



NGSOC

Next Generation Security Operations Centres

Next Generation Security Operation Centres

D5.3 Open Cybersecurity Training and Exercise Scenarios			
Report Identifier:	D5.3		
Work-package:	WP5	Task:	T5.3
Responsible Partner:	FUNITEC (FUNI)	Version Number:	1.0
Due Date	30/06/2026	Document Date:	30/06/2026
Distribution Security:	PUB	Deliverable Type:	OTHER
Keywords:			
Project website: https://ng-soc.eu/			

Document History

Version	Content & Changes	Issue Date
0.1	Document created	17/03/2026
0.2	Document sent for review	22/06/2026
0.3	Document reviewed	24/06/2026
0.4	Document reviewed	25/06/2026
0.5	Reviews are combined	29/06/2026
0.6	Sent for Quality Assurance	29/06/2026
1.0	Quality Assurance and Submission	30/06/2026

Quality Control

	Name	Organisation	Date
Editor	Jose-Maria Romero	FUNI	22/06/2026
Peer review 1	Georgios Chatzipapas	ED	24/06/2026
Peer review 2	Silvia Rull	CXB	25/06/2026
Authorised by (Technical Coordinator)	Vasileios Mavroeidis	CYEN	30/06/2026
Authorised by (Quality Manager)	Fryni Pechlidou	ED	30/06/2026
Submitted by (Project Coordinator)	Apostolos Gkletos	ED	30/06/2026

Legal Disclaimer

NG-SOC is an EU project funded by the Digital Europe Programme (DIGITAL) under grant agreement No. 101145874. The information and views set out in this deliverable are those of the author(s) and do not necessarily reflect the official opinion of the European Union. The information in this document is provided “as is”, and no guarantee or warranty is given that the information is fit for any specific purpose. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein. The NG-SOC Consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.

Copyright notice

© Copyright by the NG-SOC Consortium

This document contains information that is protected by copyright. All Rights Reserved. No part of this work covered by copyright hereon may be reproduced or used in any form or by any means without the permission of the copyright holders.

Table of Contents

Table of Contents	4
List of Figures	12
List of Tables	14
Abbreviations	15
Executive Summary.....	18
1 Introduction	19
1.1 Overview	19
1.2 Relation to other tasks and deliverables	20
1.3 Deliverable Structure	20
2 Learning Modules (LMs).....	22
2.1 LM1: Cybersecurity Laws, Regulations, and Compliance.....	23
2.1.1 Section 1: Introduction to Cybersecurity	24
2.1.2 Section 2: Cybersecurity Laws and Regulations; AI Era Legal & Ethical Issues	24
2.1.3 Section 3: Ethical Considerations in Cybersecurity.....	26
2.1.4 Section 4: Information Systems Governance.....	27
2.1.5 Section 5: Case Studies & Practical Applications	28
2.1.6 Section 6: Review & Assessment	28
2.1.7 Conclusion.....	29
2.2 LM2: Risk Management	29
2.2.1 Section 1: Introduction to Cybersecurity Risk Management.....	30
2.2.2 Section 2: Risk Appetite, Risk Evaluation and Risk Treatment	31
2.2.3 Section 3: Proposing and Managing Risk Mitigations Strategy and Options.....	33
2.2.4 Section 4: Information Security Controls.....	33
2.2.5 Section 5: Maturity Models for Cybersecurity Management	34
2.2.6 Section 6: Final Review & Assessment Quiz	35
2.2.7 Section 7: Practical Exercises and Case Studies	35
2.2.8 Conclusion.....	36
2.3 LM3: Auditing and Assessment.....	36
2.3.1 Section 1: Introduction to Auditing & Assessment.....	37
2.3.2 Section 2: Auditing Process and Techniques	38

2.3.3	Section 3: Vulnerability Assessment.....	39
2.3.4	Section 4: Reporting and Remediation.....	40
2.3.5	Section 5: Review and Assessment.....	41
2.3.6	Conclusion.....	42
2.4	LM4: Cybersecurity Policies and Frameworks	42
2.4.1	Section 1: Understanding and Developing Cybersecurity Policies and Frameworks	43
2.4.2	Section 2: Cybersecurity standards.....	44
2.4.3	Section 3: Cybersecurity policies in the Supply Chain	46
2.4.4	Section 4: Information Security Management Systems (ISMS)	47
2.4.5	Section 5: Process Improvement and Quality Management	48
2.4.6	Section 6: Final Review and Assessment	49
2.4.7	Conclusion.....	50
2.5	LM5: Technical Analysis and Security Management.....	50
2.6	LM6: Business Integration and Strategy	51
2.6.1	Section 1: Introduction to Cybersecurity Strategy.....	53
2.6.2	Section 2: Aligning Cybersecurity with Business Strategy	53
2.6.3	Section 3: Analysing Business Processes and Controls	54
2.6.4	Section 4: Technology Trend Monitoring and Threat Intelligence	55
2.6.5	Section 5: Establishing a Cybersecurity Plan.....	56
2.6.6	Section 6: Communication and Stakeholder Engagement	56
2.6.7	Section 7: Cybersecurity Culture, Privacy Awareness and Change Management.....	57
2.6.8	Section 8: Case Studies and Practical Applications.....	58
2.6.9	Final Review & Assessment	59
2.6.10	Conclusion.....	59
2.7	LM7: Privacy and Data Protection	59
2.7.1	Section 1: Introduction to Privacy and Data Protection	61
2.7.2	Section 2: Privacy and Data Protection Legal and Ethical Issues in the AI era	62
2.7.3	Section 3: Conducting Data Protection Impact Assessments (DPIAs) and Privacy Impact Assessments (PIAs).....	63
2.7.4	Section 4: Implementing Privacy Enhancing Technologies (PETs)	64
2.7.5	Section 5: Privacy preservation and Digital Forensics	65
2.7.6	Section 6: Review and Assessment.....	65

2.7.7	Conclusion.....	66
2.8	LM8: Incident Response and Forensics.....	67
2.8.1	Section 1: Introduction to Incident Response and Forensics	68
	Understanding incidents.....	68
	Standards and frameworks	69
	Section reflections	69
2.8.2	Section 2: Identifying Cybersecurity Related Issues	69
	Lesson 1: Common cyber threats	69
	Lesson 2: Detection methods and network defence mechanisms	70
	Lesson 3: Non-cyber events and human factors.....	70
	Section summary.....	70
2.8.3	Section 3: Incident Handling Standards, Methodologies and Frameworks.....	71
	Lesson 1: The incident handling lifecycle.....	71
	Lesson 2: Standards and frameworks	72
	Lesson 3: Best practices	72
	Section analysis.....	72
2.8.4	Section 4 - Operation of Computer Security Incident Response Teams (CSIRTs).....	72
	Lesson 1: CSIRT roles, responsibilities and organisational models.....	73
	Defining CSIRTs and responsibilities	73
	Lesson 2: Coordination with external entities	73
	Section synthesis.....	74
2.8.5	Section 5: Conducting Technical Analysis and Reporting	74
2.8.6	Section 6: Criminal Investigation Procedures in Cybersecurity	74
2.8.7	Section 7: Digital Forensics Best Practices.....	75
2.8.8	Section 8: Review and Assessment.....	75
2.8.9	Section 9: Practical Exercises and Case Studies.....	76
2.8.10	Conclusion.....	76
2.9	LM9: Collaboration and Communication.....	77
2.9.1	Section 1: Introduction to Cybersecurity Communication	78
2.9.2	Section 2: Information Systems Governance Communication	79
2.9.3	Section 3: Stakeholder Communication Mastery	80
2.9.4	Section 4: Teamwork and Collaboration in Cybersecurity Operations.....	81

2.9.5	Section 5: Systematic, Evidence-Based Decision-Making.....	82
2.9.6	Section 6: Comprehensive Awareness Programme Architecture.....	82
2.9.7	Section 7: Multidisciplinary Team Leadership	83
2.9.8	Section 8: Case Studies & Practical Applications	84
2.9.9	Section 9: Mastery Assessment & Professional Roadmap	85
2.9.10	Final Review & Assessment	85
2.9.11	Conclusion.....	86
3	KYPO/CRCZ cyber ranges developed	87
3.1	KYPO/CRCZ LM2 Risk Management (status: done).....	87
3.1.1	Source code	87
3.1.2	Testing.....	88
3.1.3	General context: KYPO, CyberRangeCZ and this learning module	88
3.1.4	Repository purpose and educational intent	89
3.1.5	Overall structure of the repository.....	89
3.1.6	The role of RITA.....	90
3.1.7	Training design and learner progression	92
3.1.8	Standards, frameworks and competence alignment.....	92
3.1.9	Sandbox topologies and virtual infrastructure	93
3.1.10	Provisioning approach and security implications	94
3.1.11	Deployment and operating workflow.....	94
3.1.12	Strengths of the repository.....	95
3.1.13	Assessment of suitability for training delivery	95
3.1.14	Final assessment	95
3.1.15	Scenario status and public-release readiness.....	96
3.1.16	Public-dissemination hygiene review	97
3.1.17	YAML/JSON artefact inventory	97
3.2	KYPO/CRCZ LM8 Incident Response Subcase 1a (status: done)	98
3.2.1	Source code	98
3.2.2	Testing.....	98
3.2.3	CyberRangeCZ and KYPO context	99
3.2.4	Repository identity and project status	99
3.2.5	Overall purpose of the project.....	99

3.2.6	Repository structure and content organisation.....	100
3.2.7	Training design and pedagogical flow.....	100
3.2.8	The phishing awareness scenario	101
3.2.9	Topology and virtual infrastructure	101
3.2.10	Provisioning workflow and deployment process.....	103
3.2.11	Ansible playbook architecture	103
3.2.12	REP core services	103
3.2.13	Reporting workspace and analytics	104
3.2.14	Instructor console	104
3.2.15	Trainee workstation configuration	105
3.2.16	Windows base configuration	105
3.2.17	Helper scripts and automation utilities	105
3.2.18	Validation and quality controls.....	106
3.2.19	Credential and secret management	106
3.2.20	Strengths of the repository.....	106
3.2.21	Suitability for training delivery	107
3.2.22	Final assessment	107
3.2.23	Scenario status and public-release readiness.....	108
3.2.24	Public-dissemination hygiene review	109
3.2.25	YAML/JSON artefact inventory	109
3.3	KYPO/CRCZ LM8 Incident Response Subcase 1a-3 (status: testing on execution)	110
3.3.1	Source code	110
3.3.2	Overall purpose of the project.....	111
3.3.3	Repository structure and content organisation.....	112
3.3.4	Network topology and sandbox architecture	112
3.3.5	Host roles and simulated enterprise environment.....	112
3.3.6	Provisioning workflow and Ansible design	113
3.3.7	Security tooling: SIEM, DFIR and CTI.....	113
3.3.8	Red-team and penetration-testing component	114
3.3.9	Training design and pedagogical flow.....	114
3.3.10	Practical assessed activities	115
3.3.11	Synthetic evidence and realism	115

3.3.12	Validation and quality controls	116
3.3.13	Deployment requirements and operational caveats	116
3.3.14	Strengths of the repository	116
3.3.15	Suitability for training delivery	117
3.3.16	Final assessment	117
3.3.17	Scenario status and public-release readiness	118
3.3.18	Public-dissemination hygiene review	118
3.3.19	YAML/JSON/CACAO artefact inventory	119
3.4	KYPO/CRCZ LM5 Network Vulnerability Identification Training 1b ² (status: testing on execution)	119
3.4.1	Source code	119
3.4.2	Overall purpose of the project	121
3.4.3	Repository structure and content organisation	121
3.4.4	Training design and pedagogical flow	121
3.4.5	Scenario content and target vulnerabilities	122
3.4.6	Topology and virtual infrastructure	122
3.4.7	REP, LMS and course delivery components	123
3.4.8	Pentest workstations and toolchain	123
3.4.9	Reporting, feedback and analytics	124
3.4.10	CYNET DC1 and identity-layer simulation	124
3.4.11	Provisioning workflow and deployment process	125
3.4.12	Validation and quality controls	125
3.4.13	Credential and secret management	125
3.4.14	Operational inconsistencies and caveats	126
3.4.15	Security posture and lab-only assumptions	126
3.4.16	Strengths of the repository	127
3.4.17	Suitability for training delivery	127
3.4.18	Final assessment	127
3.4.19	Scenario status and public-release readiness	128
3.4.20	Public-dissemination hygiene review	129
3.4.21	YAML/JSON artefact inventory	129

3.5	KYPO/CRCZ LM8 Phishing Attack Training Scenario Subcase 1a ² (status: testing on execution)	130
3.5.1	Source code	130
3.5.2	Overall purpose of the project.....	131
3.5.3	Repository structure and content organisation.....	132
3.5.4	Training design and pedagogical flow.....	132
3.5.5	Scenario realism and phishing content.....	133
3.5.6	Topology and virtual infrastructure	133
3.5.7	LMS course portal	134
3.5.8	GoPhish phishing simulator	134
3.5.9	Mail relay and sandboxed email delivery	134
3.5.10	Reporting workspace, scoring and feedback.....	135
3.5.11	Instructor console	135
3.5.12	Windows trainee workstations and REP collector.....	136
3.5.13	Provisioning workflow	136
3.5.14	Validation and quality controls.....	137
3.5.15	Credential management and operational caveats	137
3.5.16	Strengths of the repository.....	137
3.5.17	Suitability for training delivery	138
3.5.18	Final assessment	138
3.5.19	Scenario status and public-release readiness.....	138
3.5.20	Public-dissemination hygiene review	139
3.5.21	YAML/JSON artefact inventory	139
3.6	KYPO/CRCZ LM5 Malware Attack Detection & Response Training 1c (status: validation).....	140
3.6.1	Source code	140
3.7	KYPO/CRCZ LM8 CACAO Playbook Authoring Training (Firewall IP Block) 1d (status: validation)	141
3.7.1	Source code	141
3.7.2	CACAO and the educational theme	142
3.7.3	Repository structure and content organisation.....	142
3.7.4	Overall purpose of the project.....	142
3.7.5	Topology and virtual infrastructure	143

3.7.6	Host roles and scenario components	143
3.7.7	Provisioning workflow and Ansible design	144
3.7.8	NG-SOAR implementation	145
3.7.9	CACAO toolkit and trainee experience	145
3.7.10	Firewall action and verification model	146
3.7.11	Evaluation and reporting	146
3.7.12	Validation and quality controls	147
3.7.13	Secrets management and security posture	147
3.7.14	Strengths of the repository	148
3.7.15	Suitability for training delivery	148
3.7.16	Final assessment	149
3.7.17	Scenario status and public-release readiness	149
3.7.18	Public-dissemination hygiene review	150
3.7.19	YAML/JSON/CACAO artefact inventory	150
4	Conclusion and Future Enhancements	152
	Appendix A – Asset Specification	156
	REFERENCES	158

List of Figures

Figure 1 LM1 Section 1 on Open edX.....	24
Figure 2 LM1 Section 2 on Open edX.....	24
Figure 3 LM1 Section 3 on Open edX.....	26
Figure 4 LM1 Section 4 on Open edX.....	27
Figure 5 LM1 Section 5 on Open edX.....	28
Figure 6 LM1 Section 6 on Open edX.....	28
Figure 7 LM2 Section 1 on Open edX.....	30
Figure 8 LM2 Section 2 on Open edX.....	32
Figure 9 LM2 Section 3 on Open edX.....	33
Figure 10 LM2 Section 4 on Open edX.....	33
Figure 11 LM2 Section 5 on Open edX.....	34
Figure 12 LM2 Section 6 on Open edX.....	35
Figure 13 LM2 Section 7 on Open edX.....	35
Figure 14 LM3 Section 1 on Open edX.....	37
Figure 15 LM3 Section 2 on Open edX.....	38
Figure 16 LM3 Section 3 on Open edX.....	39
Figure 17 LM3 Section 4 on Open edX.....	40
Figure 18 LM3 Section 5 on Open edX.....	41
Figure 19 LM4 Section 1 on Open edX.....	43
Figure 20 LM4 Section 2 on Open edX.....	44
Figure 21 LM4 Section 3 on Open edX.....	46
Figure 22 LM4 Section 4 on Open edX.....	47
Figure 23 LM4 Section 5 on Open edX.....	48
Figure 24 LM4 Section 6 on Open edX.....	49
Figure 25 LM6 Section 1 on Open edX.....	53
Figure 26 LM6 Section 2 on Open edX.....	53
Figure 27 LM6 Section 3 on Open edX.....	54
Figure 28 LM6 Section 4 on Open edX.....	55
Figure 29 LM6 Section 5 on Open edX.....	56
Figure 30 LM6 Section 6 on Open edX.....	56
Figure 31 LM6 Section 7 on Open edX.....	57
Figure 32 LM6 Section 8 on Open edX.....	58
Figure 33 LM6 Final Review & Assessment on Open edX.....	59
Figure 34 LM7 Section 1 on Open edX.....	61
Figure 35 LM7 Section 2 on Open edX.....	62
Figure 36 LM7 Section 3 on Open edX.....	63
Figure 37 LM7 Section 4 on Open edX.....	64
Figure 38 LM7 Section 5 on Open edX.....	65
Figure 39 LM7 Section 6 on Open edX.....	65
Figure 40 LM8 Section 1 on Open edX.....	68

Figure 41 LM8 Section 2 on Open edX.....	69
Figure 42 LM8 Section 3 on Open edX.....	71
Figure 43 LM8 Section 4 on Open edX.....	73
Figure 44 LM8 Section 5 on Open edX.....	74
Figure 45 LM8 Section 6 on Open edX.....	74
Figure 46 LM8 Section 7 on Open edX.....	75
Figure 47 LM8 Section 8 on Open edX.....	75
Figure 48 LM8 Section 9 on Open edX.....	76
Figure 49 LM9 Section 1 on Open edX.....	78
Figure 50 LM9 Section 2 on Open edX.....	79
Figure 51 LM9 Section 3 on Open edX.....	80
Figure 52 LM9 Section 4 on Open edX.....	81
Figure 53 LM9 Section 5 on Open edX.....	82
Figure 54 LM9 Section 6 on Open edX.....	82
Figure 55 LM9 Section 7 on Open edX.....	83
Figure 56 LM9 Section 8 on Open edX.....	84
Figure 57 LM9 Section 9 on Open edX.....	85
Figure 58 LM9 Final Review & Assessment on Open edX.....	85
Figure 59 KYPO/CRCZ LM2 Risk Management source code on GitHub	88
Figure 60 Exercise 1 - Risk Assessment and Threat Modelling for a Banking System (PUC1 - Financial Sector).....	88
Figure 61 LM2 Topologies Overview.....	93
Figure 62 KYPO/CRCZ LM8 Incident Response Subcase 1a source code on GitHub.....	98
Figure 63 Level 02 - Incident briefing.....	99
Figure 64 LM8 Subcase 1a Topology Overview	103
Figure 65 LM8 Subcase 1a exercise (screenshot)	108
Figure 66 KYPO/CRCZ Incident Response Subcase 1a-3 source code on GitHub	110
Figure 67 Level 04 - Alert Analysis - the C2 IP address	111
Figure 68 KYPO/CRCZ LM5 Network Vulnerability Identification Training 1b source code on GitHub	120
Figure 69 Level 04 - Verify Lab Connectivity -- Resolve Target-Server IP	120
Figure 70 CYNET-Like Infrastructure	128
Figure 75 Scenario status and public-release readiness.....	Error! Bookmark not defined.
Figure 71 KYPO/CRCZ LM8 Phishing Attack Training Scenario Subcase 1a source code on GitHub.....	130
Figure 72 Level 09 - Module 3 — Identify a Dangerous Script Extension.....	131
Figure 73 KYPO/CRCZ LM8 CACAO Playbook Authoring Training (Firewall IP Block) 1d source code on GitHub	141
Figure 74 List of cyber ranges deployed on a moment.....	149
Figure 75 Deployment process (3 stages) in a pool with a sandbox on CyberRangeCZ	153
Figure 76 Automating the creation of CyberRangeCZ Platform scenarios (screenshot)	154

List of Tables

Table 1 Inputs from Deliverables	20
Table 2 Learning Modules list	22
Table 3 LM1 Extraction	23
Table 4 LM2 Extraction	29
Table 5 LM3 Extraction	36
Table 6 LM4 Extraction	42
Table 7 LM5 Extraction	50
Table 8 LM6 Extraction	51
Table 9 LM7 Extraction	60
Table 10 LM8 Extraction	67
Table 11 LM9 Extraction	77
Table 12 Scenario status and public-release readiness	96
Table 13 Public-dissemination hygiene review	97
Table 14 YAML/JSON artefact inventory	97
Table 15 Scenario status and public-release readiness	108
Table 16 Public-dissemination hygiene review	109
Table 17 YAML/JSON artefact inventory	109
Table 18 Scenario status and public-release readiness	118
Table 19 Public-dissemination hygiene review	118
Table 20 YAML/JSON/CACAO artefact inventory	119
Table 21 Scenario status and public-release readiness	128
Table 22 Public-dissemination hygiene review	129
Table 23 YAML/JSON artefact inventory	129
Table 24 Scenario status and public-release readiness	139
Table 25 Public-dissemination hygiene review	139
Table 26 YAML/JSON artefact inventory	139
Table 27 Scenario status and public-release readiness	149
Table 28 Public-dissemination hygiene review	150
Table 29 YAML/JSON/CACAO artefact inventory	150
Table 30 OpenEDx Asset Specification	156

Abbreviations

Acronym	Description
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
BYOD	Bring Your Own Device
C2	Command and Control
CACAO	Collaborative Automated Course of Action Operations
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CICMS	Collaborative Incident and Case Management System
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMM	Capability Maturity Model
CMMI	Capability Maturity Model Integration
CMS	Content Management System
CNIL	Commission Nationale de l'Informatique et des Libertés
CRA	Cyber Resilience Act
CRCZ	CyberRangeCZ
CSF	Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CTI-SS	Cyber Threat Intelligence Sharing Service
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DFIR	Digital Forensics and Incident Response
DFIR-IRIS	Digital Forensics and Incident Response – IRIS
DIGITAL	Digital Europe Programme

DLP	Data Loss Prevention
DMAIC	Define, Measure, Analyse, Improve and Control
DORA	Digital Operational Resilience Act
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ECSF	European Cybersecurity Skills Framework
EDPB	European Data Protection Board
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity
FIRST	Forum of Incident Response and Security Teams
GDPR	General Data Protection Regulation
GRC	Governance, Risk and Compliance
IoC	Indicator of Compromise
IRP	Incident Response Plan
IRT	Incident Response Team
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
ISMS	Information Security Management System
KRI	Key Risk Indicator
KYPO	KYPO Cyber Range Platform
LM	Learning Module
LMS	Learning Management System
MISP	Malware Information Sharing Platform
NG-SIEM	Next Generation Security Information and Event Management
NG-SOAR	Next Generation Security Orchestration, Automation and Response
OpenVAS	Open Vulnerability Assessment Scanner
OWASP	Open Worldwide Application Security Project
PUC	Pilot Use Case
QMS	Quality Management System
RDP	Remote Desktop Protocol
REP	Random Education Platform
RITA	Risk Identification and Threat Assessment

SIEM	Security Information and Event Management
SOC	Security Operations Centre
SOAR	Security Orchestration, Automation and Response
VM	Virtual Machine
VPN	Virtual Private Network
YAML	YAML Ain't Markup Language

Executive Summary

This deliverable, D5.3 Open Cybersecurity Training and Exercise Scenarios, presents the training content and practical exercise environments developed within NG-SOC Work Package 5, Task T5.3. Its purpose is to document the open cybersecurity training scenarios produced by the project, showing how the NG-SOC curriculum is translated into structured Learning Modules and practical KYPO/CRCZ cyber range exercises. The deliverable therefore contributes to the broader NG-SOC objective of strengthening the skills, readiness and operational capabilities required by next-generation Security Operation Centres.

The document covers two complementary dimensions of the training work. The first dimension is the set of Learning Modules, delivered through the NG-SOC training platform and designed to provide the conceptual, methodological and professional foundation for cybersecurity roles. These modules address cybersecurity laws and compliance, risk management, auditing and assessment, policies and frameworks, technical analysis and security management, business integration, privacy and data protection, incident response and forensics, and collaboration and communication. Together, they support a multidisciplinary training path that reflects the needs of modern SOC's, where technical expertise must be combined with governance, legal awareness, communication, risk-based decision-making and organisational coordination.

The second dimension is the set of KYPO/CyberRangeCZ cyber ranges developed to convert selected learning outcomes into practical, hands-on exercises. These cyber ranges provide realistic and isolated environments in which learners can practise risk assessment, phishing awareness, incident response, vulnerability identification, malware detection and response, CTI enrichment, SOAR-supported containment, CACAO playbook authoring and cyber range quality assurance. The scenarios use representative tools, artefacts, topologies, provisioning scripts and reporting workflows, allowing learners to move from theory to operational practice.

The major outcome of this deliverable is the creation of a reusable and extensible training foundation for NG-SOC. The Learning Modules provide the common curriculum, terminology and assessment logic, while the cyber ranges provide the practical environments for experiential learning. Several scenarios have reached completion, while others are undergoing execution testing or validation, reflecting a realistic engineering and quality assurance lifecycle. This document also identifies future enhancements, including final validation, stronger cross-referencing between modules and exercises, standardised scenario packaging, richer assessment mechanisms and further automation of cyber range deployment and testing.

1 Introduction

The NG-SOC project addresses the development of capabilities for next-generation Security Operation Centres, combining technology, processes, skills and operational readiness. Within this context, Work Package 5 focuses on training, exercises and competence development. Task T5.3 contributes to this effort by producing open cybersecurity training and exercise scenarios that can be used to support learning, assessment and capability verification.

This deliverable documents the results of that work. It brings together the Learning Modules developed for the NG-SOC training programme and the KYPO/CyberRangeCZ cyber range scenarios implemented to provide practical, hands-on exercises. The document therefore connects curriculum design with technical scenario engineering. It does not only describe what learners should know, but also how selected learning outcomes are operationalised through realistic cyber range environments.

The deliverable is positioned as a bridge between theoretical training and applied practice. The Learning Modules provide structured educational content, including lessons, case studies, review sections and assessments. The KYPO/CyberRangeCZ scenarios complement this by providing sandboxed environments where learners can interact with simulated systems, tools, vulnerabilities, alerts, reports and response workflows. This combination supports a progressive learning model in which trainees first acquire the relevant concepts and then apply them in controlled operational settings.

1.1 Overview

The scope of this deliverable is to present the open cybersecurity training and exercise scenarios developed under NG-SOC Task T5.3. It includes the description of the Learning Modules, their topics, learning outcomes and relationship to cybersecurity roles, as well as the practical cyber ranges developed for deployment and execution through CyberRangeCZ/KYPO-compatible environments.

The document demonstrates that the training work has produced both educational and technical outputs. On the educational side, it describes nine Learning Modules covering legal, governance, risk, technical, strategic, privacy, incident response and communication aspects of cybersecurity. On the practical side, it documents a set of cyber range scenarios aligned with selected modules and use cases, including risk management, incident response, phishing, vulnerability assessment, malware detection and response, and security automation.

The objectives related to this deliverable have been achieved in full and as scheduled. The document provides the required overview of the Learning Modules and the cyber range scenarios developed so far. Some individual cyber range repositories are still marked as being in execution testing or validation, but this reflects the normal technical refinement process of practical training assets and does not prevent the deliverable from achieving its reporting objective.

1.2 Relation to other tasks and deliverables

This deliverable is related to the wider NG-SOC work on training, capability development, requirements definition and technical validation. It receives input from the project's curriculum design, competence mapping, platform preparation and cyber range implementation activities. It also provides input to future piloting, evaluation, exploitation and quality assurance activities by documenting which training assets have been produced, how they are structured and how they can be further validated or reused.

The Learning Modules described in Chapter 2 provide the educational foundation for the training programme. The cyber range scenarios described in Chapter 3 operationalise selected learning objectives in practical environments. The conclusions and future enhancements in Chapter 4 identify how these outputs can be consolidated, standardised and aligned with the NG-SOC roadmap.

Receives inputs from:

Table 1 Inputs from Deliverables

Deliverable	Description
Description of Work / Grant Agreement	Defines the overall NG-SOC objectives, the role of WP5, and the expected contribution of training and exercise scenarios to the project.
D2.3 Requirements and Traceability Inputs	Provides requirements and traceability elements to be reflected in the implemented training features and cyber range scenarios.
WP5 Learning Module development activities	Provides the educational content, learning outcomes, assessment logic and Open edX-based module structure documented in Chapter 2.
WP5 cyber range development activities	Provides the KYPO/CyberRangeCZ repositories, topology definitions, provisioning artefacts, validation notes and scenario descriptions documented in Chapter 3.
Piloting, validation and quality assurance activities	Provides feedback on scenario execution, deployment maturity, learner-facing instructions and future improvements.

1.3 Deliverable Structure

The deliverable is structured in four chapters:

- Chapter 1 introduces the document, explains its scope, and summarizes its relationship with other NG-SOC tasks, inputs and deliverables.
- Chapter 2 presents the Learning Modules. It describes the educational content developed for the NG-SOC training programme, including module objectives, topics, learning outcomes, assessment components and links to relevant cybersecurity roles and competences.
- Chapter 3 presents the KYPO/CyberRangeCZ cyber ranges developed. It describes the practical training scenarios, their source code repositories, educational purpose, technical architecture, topology, provisioning approach, validation status, strengths, caveats and suitability for training delivery.

- Chapter 4 provides the conclusions and future enhancements of the document. It summarises the main achievements, explains the contribution of the Learning Modules and cyber ranges to NG-SOC objectives, and identifies future work related to validation, standardisation, automation, assessment and integration between theory and practice.

2 Learning Modules (LMs)

The Learning Modules constitute the educational backbone of the NG-SOC training programme. They provide structured content for the development of cybersecurity knowledge, professional judgement and practical readiness across a broad range of SOC-relevant domains. The modules are designed to support different learner profiles, including technical analysts, risk managers, auditors, incident responders, privacy specialists, governance professionals and decision-makers.

Each module combines subject content, learning outcomes and assessment elements. The modules introduce key concepts, develop them through lessons and examples, and reinforce them through quizzes, review sections, case studies or practical activities. This approach supports progressive learning: learners first acquire a common vocabulary and methodological foundation and then apply that knowledge in more practical or scenario-based contexts.

The Learning Modules also support alignment with recognised cybersecurity roles and competence frameworks. They address not only technical knowledge, but also legal, ethical, organisational, strategic and communication dimensions of cybersecurity. This is essential for next-generation SOC's, where effective performance depends on the ability to combine technology, process, governance, coordination and evidence-based decision-making.

Table 2 Learning Modules list

Learning Module (LM)	Description
LM1	Cybersecurity Laws, Regulations & Compliance
LM2	Risk Management
LM3	Auditing & Assessment
LM4	Cybersecurity Policies and Frameworks
LM5	Technical Analysis and Security Management
LM6	Business Integration and Strategy
LM7	Privacy & Data Protection
LM8	Incident Response & Forensics
LM9	Collaboration and Communication

The following sections describe the individual Learning Modules included in the NG-SOC training programme. They cover cybersecurity laws, regulations and compliance; risk management; auditing and assessment; cybersecurity policies and frameworks; technical analysis and security management; business integration and strategy; privacy and data protection; incident response and forensics; and collaboration and communication.

2.1 LM1: Cybersecurity Laws, Regulations, and Compliance

Table 3 LM1 Extraction

Competence Level: Basic / Intermediate	
This module introduces the legal and regulatory frameworks governing cybersecurity, including international and EU-specific regulations. It examines ethical considerations, especially in emerging areas like AI, and provides an overview of governance and compliance standards. Through case studies, learners will understand the practical application of these laws, their ethical implications, and how to maintain compliant information systems.	
Subject contents and topics	Learning outcomes (competences)
> Introduction to Cybersecurity > Cybersecurity Laws and Regulations, Legal and Ethical issues in the Artificial Intelligence era > Ethical Considerations in Cybersecurity Information Systems Governance > Case Studies and Practical Applications Review and Assessment	The student is able to: - Understand foundational cybersecurity laws and regulations at global and EU levels. - Identify key legal and ethical issues in cybersecurity, including those arising from AI technologies. - Apply principles of governance and compliance in information security management. - Evaluate case studies to understand the real-world implications of legal and ethical standards. - Develop a baseline ability to incorporate compliance measures into organizational cybersecurity practices.
	Mapping with ENISA ECSF
	Cyber Legal, Policy & Compliance Officer, Cybersecurity Risk Manager, Cybersecurity Auditor.

The **Cybersecurity Laws, Regulations & Compliance** module (NG-SOC LM1) introduces learners to the legal and regulatory environment in which cybersecurity teams operate. It begins with fundamental cybersecurity concepts, then examines European and global regulations, explores ethical issues - especially around artificial intelligence (AI) - and shows how governance frameworks help organisations align controls with strategic objectives. Later sections provide case studies to practise applying the legal, ethical and governance concepts. Throughout the module the authors emphasise ENISA's European Cybersecurity Skills Framework (ECSF) and map learning activities to roles such as Cybersecurity Auditor, Risk Manager and Policy & Compliance Officer.

The module uses narrative scenarios, external readings and concept tests, allowing learners to practise analysing incidents through a compliance lens.

Link to Open edX: https://apps.ngsoc-training-platform.eurodyn.com/learning/course/course-v1:NG-SOC+LM1+2025_Q1/home

2.1.1 Section 1: Introduction to Cybersecurity

- ✓ SECTION 1: Introduction to Cybersecurity
 - ✓ Section Introduction
 - ✓ Lesson 1 - Cybersecurity Fundamentals
 - ✓ Section 1 Concept Test

Figure 1 LM1 Section 1 on Open edX

The first section establishes a shared understanding of **cybersecurity** and its relationship with information-security disciplines. The objectives invite learners to **define cybersecurity**, explain its importance, describe the CIA triad and identify threat actors and attack lifecycles. In the main **Cybersecurity Fundamentals** lesson, a junior security analyst briefs leadership on key concepts - confidentiality, integrity and availability, the **Cyber Kill Chain** and the **NIST Cybersecurity Framework (NIST CSF)** [19] - and links them to day-to-day decisions. A separate page notes that the term “cybersecurity” emerged from “cyber space” and has often been used synonymously with IT or ICT security. Another page summarises definitions from standards bodies: the Oxford English Dictionary¹ defines cybersecurity as protection of systems from theft or damage, while international standards bodies broaden it to include **availability, integrity and confidentiality** and to consider physical, legal and social risks. Learners are encouraged to read ENISA’s “Definition of Cybersecurity”² and identify stakeholders, scope and relevance.

The module introduces **Lockheed Martin’s Cyber Kill Chain**, describing its seven stages - reconnaissance, weaponisation, delivery, exploitation, installation, command & control and actions on objectives - and highlighting that early detection and controls can disrupt adversaries. Scenario-based questions ask learners to apply the kill chain; for example, a system administrator discovers privacy breaches and service outages and must determine control gaps. Section 1 also contains a reading list with an ENISA report on cyber-security definition gaps, a video primer on the CIA triad and guidance on reading risk assessments; these resources provide a deeper context but are not summarised here due to space constraints.

2.1.2 Section 2: Cybersecurity Laws and Regulations; AI Era Legal & Ethical Issues

- ✓ SECTION 2: Cybersecurity Laws and Regulations, Legal and Ethical issues in the AI era
 - ✓ Section Introduction
 - ✓ Lesson 1 – Understanding Cybersecurity Laws, Regulations & Compliance in the AI Era
 - ✓ Section 2 Concept Test

Figure 2 LM1 Section 2 on Open edX

¹ Oxford English Dictionary Context: [Public and Private Governance of Cybersecurity](#) & [Oxford Learner's Dictionary](#).

² ENISA Official Report: Definition of Cybersecurity - Gaps and Overlaps in Standardisation.

Section 2 introduces the **EU cybersecurity rulebook**, explaining why legal compliance matters and how to translate regulatory obligations into security controls. The introduction page lists general objectives: identify **EU instruments** shaping cybersecurity (including **NIS2 [20]**, **GDPR [21]**, **DORA [22]**, the **Cyber Resilience Act (CRA) [23]** and the proposed **EU AI Act [24]**), explore organisational obligations (risk management measures, incident reporting, supply-chain security, security-by-design and data protection), and explain how AI introduces new security, legal and ethical risks.

- **Lesson 1 - Understanding Cybersecurity Laws, Regulations & Compliance in the AI Era** presents an overview of the EU rulebook. Learners examine a chatbot scenario where an AI system answers questions about an organisation's security policy; they must assess whether the chatbot inadvertently exposes confidential information and whether its training data complied with GDPR. The lesson emphasises that NIS2's **Article 21** requires essential and important entities to implement risk management measures, secure supply chains, incident reporting and business continuity; Article 23 obliges notification of incidents to a national CSIRT within 24 hours. The chapter also highlights the CRA - adopted in **October 2024** - which introduces mandatory cybersecurity requirements for digital products and sets **five-year certification validity**, and notes that the **Cyber Solidarity Act**³ (expected early **2025**) will strengthen EU-level capacities and include a European cyber-defence network. Learners compare the obligations of large enterprises and SMEs: Eurostat statistics show that **83 %** of large enterprises apply at least one ICT security measure, but only **17 %** apply all core measures; for SMEs the figures are **36 %** and **4 %**, respectively. This contrast reinforces the need for regulatory compliance and investment across organisational sizes.
- **Common Objectives in National Cybersecurity Strategies** are presented via a radial infographic. Countries typically aim to establish **incident reporting mechanisms**, combat cybercrime, raise public awareness, foster research & development, organise cyber exercises, strengthen training, enhance cooperation between public and private actors, protect essential and important entities, implement baseline security measures and build public-private partnerships. Learners reflect on how these objectives underpin regulations like NIS2.
- **Annexes** supply supporting material. *Annex C* provides a **glossary of technical terms** such as **Advanced Persistent Threat (APT)** and **Cyber Threat Intelligence (CTI)**. *Annex I* and *Annex II* list sectors of high criticality and other critical sectors covered by NIS2, while the **Map of EU landscape** links to ENISA's **2024 Report on the State of Cybersecurity in the Union** (a 71-page report summarising threat trends and policy recommendations).

Section 2 therefore equips learners with knowledge of the evolving EU legislative landscape and encourages them to map legal requirements to organisational controls, especially when deploying AI-enabled systems.

³ <https://eur-lex.europa.eu/eli/reg/2025/38/oj>

2.1.3 Section 3: Ethical Considerations in Cybersecurity

✓ SECTION 3: Ethical Considerations in Cybersecurity

- ✓ Section Introduction
- ✓ Lesson 1 – Principles of Cybersecurity Ethics
- ✓ Section 3 Concept Test

Figure 3 LM1 Section 3 on Open edX

Ethics in cybersecurity goes beyond legal compliance; it encompasses professional values and societal implications. Section 3's introduction encourages students to recognise key ethical principles, differentiate between ethics and law, apply ethics to real-world scenarios (including AI use cases), and identify appropriate escalation paths and professional duties.

- **Principles of Cybersecurity Ethics.** The lesson describes core ethical principles - **privacy, integrity, accountability, fairness and harm minimisation** - and introduces a narrative scenario: a product security team investigating unusual access patterns after enabling an AI feature must decide whether to stop the service and how to communicate with stakeholders. Learners are instructed to read a primer on cybersecurity ethics focusing on definitions and differences between ethics, law and policy. One page emphasises that ethics aims to protect confidentiality, integrity and availability, and lists seven guiding principles: **accountability, transparency, confidentiality, integrity, availability, resilience and continuous learning**.
- **Common Ethical Issues** include privacy intrusion, misallocation of security resources, the possibility of disinformation, lack of transparency and accountability, and failure to comply with regulations. Learners analyse these issues and propose measures such as privacy-by-design, risk-based prioritisation, truthful communications and regular audits.
- **Principle list Framework for Cybersecurity Ethics.** The module directs students to a paper that outlines five principles - **privacy, harm minimisation, fairness, accountability and integrity** - and suggests translating them into controls like least privilege, access reviews, logging and disclosure practices. Another page summarises a related set of principles: **beneficence, non-maleficence, autonomy, justice and explicability** (transparency and intelligibility). These frameworks help security professionals navigate dilemmas where legal compliance alone is insufficient.
- **Ethics in AI.** The lesson highlights challenges unique to AI, such as bias, adversarial manipulation and misuse of personal data. It urges practitioners to adopt fairness metrics, secure model training pipelines and robust audit trails. A concluding page underscores that cultivating an ethical culture reduces security incidents and enhances trust.

2.1.4 Section 4: Information Systems Governance

✓ SECTION 4: Information Systems Governance

✓ Section Introduction

✓ Lesson 1 – Introduction to Cybersecurity Governance: Clarity, Coordination and Commitment

✓ Section 4 Concept Test

Figure 4 LM1 Section 4 on Open edX

This section explains how governance structures enable effective cybersecurity by clarifying roles, coordinating information sharing and ensuring resource commitment. The section introduction advises learners to consult the presentation file and lists objectives: define information systems governance, explain its role in aligning cybersecurity with organisational mission, risk appetite and legal obligations, and describe how policies, roles, decision rights and processes distribute accountability and enable oversight.

- **Lesson 1 - Introduction to Cybersecurity Governance: Clarity, Coordination and Commitment** presents a narrative scenario: a cross-functional team in an EU Member State revises a National Cyber Security Strategy but lacks clear roles, coordination and dedicated budget; leadership asks what good governance looks like. The lesson explains that governance sets direction and accountability, management executes, and auditors verify. It introduces **governance artefacts** (policies, charters, role descriptions, decision matrices such as RACI, escalation and reporting lines) and discusses why governance matters for SOC - it prioritises what to measure, what to monitor, what to remediate and who is accountable - and how governance steers SOC priorities and links to auditing, vulnerability assessment and remediation.
- Subsequent pages define **information systems governance** as “exercise of power and authority”; within the security sector it encompasses formal and informal decisions, processes and actors that influence the provision of public goods like security. Learners study the **security sector**, defined as all structures, institutions and personnel responsible for security provision, management and oversight at national and local levels, and learn that communities can self-organise to provide security (neighbourhood watches, women’s groups). **Security sector reform** is described as a political and technical process aimed at making security provisions more effective and accountable within democratic, rule-of-law frameworks.
- Later pages expand on **cyber governance**. With the growth of cyberspace and cyber threats, cyber governance is defined as the operation of decision-making processes that increase participation, transparency and accountability in measures related to cyberspace. The section differentiates **strategic, operational and technical governance**, analyses key challenges when deploying governance models, and encourages learners to apply ENISA good practices to a national cyber security strategy scenario. A concept test at the end assesses understanding of governance artefacts and their role in SOC operations.

2.1.5 Section 5: Case Studies & Practical Applications

- ✓ SECTION 5: Case Studies & Practical Applications
 - ✓ Section Introduction
 - ✓ Lesson 1 – Analyzing Cybersecurity Compliance Cases

Figure 5 LM1 Section 5 on Open edX

Section 5 applies the module’s theoretical material to real incidents. The introduction outlines objectives: analyse real cyber incidents and relate them to governance, compliance and SOC practices; map observed actions to controls and responsibilities (using ECSF roles/competences); distil prevention, detection, response and recovery lessons; and practise converting narrative cases into checklists, runbooks and audit-ready evidence.

- **Lesson 1 - Analysing Cybersecurity Compliance Cases** explains that students examine real-world incidents to understand how organisations identify threats, coordinate responses and embed best practice. A narrative case involves a cross-functional team preparing for a compliance review; leadership asks what real incidents teach about controls. Learners use ECSF use-cases and readings to extract what went right or wrong, determine who owned which actions, and identify controls that could have prevented or shortened the incident. The lesson teaches students to read case studies through a **controls and accountability lens** (policy, roles, procedures, evidence), map actions to ECSF roles/competences and control frameworks, identify quick wins (prevention/containment), and understand audit-evidence requirements. Activities include a small-business ransomware scenario where learners practise immediate response versus long-term fixes. By the end, students can produce short, audit-ready artefacts from narratives, such as checklist entries, runbook updates and evidence pointers.
- Additional units summarise ECSF design principles, benefits and applications, describe the ECSF modular approach in practice, and guide learners to connect good governance to case execution. A survey of cyber-threat history and a real-world incident provide context, while an interactive ransomware scenario allows learners to apply theoretical controls in a simulated crisis.

2.1.6 Section 6: Review & Assessment

- ✓ SECTION 6 - Review & Assessment
 - ✓ Final Review and Assessment (1 Question)
Final Review & Assessment

Figure 6 LM1 Section 6 on Open edX

The final section synthesises the module and evaluates comprehension. It typically includes a **review of key concepts**, practise quizzes and a final assessment. Learners revisit definitions of cybersecurity, the CIA triad and the Cyber Kill Chain; summarise regulatory obligations under NIS2, GDPR, DORA, CRA and the AI Act; reflect on ethical principles and frameworks; and recall governance artefacts and their importance in SOC operations. Concept tests may present multiple-choice questions, matching exercises or scenario-based prompts. The assessments encourage learners to apply their knowledge to new situations and identify gaps for further study.

Although the content of Section 6 is not quoted directly due to limited access, it likely emphasises consolidation of learning outcomes, encourages self-reflection and directs learners to additional resources or training modules.

2.1.7 Conclusion

Learning Module 1 provides a comprehensive introduction to cybersecurity regulation and compliance, blending foundational technical concepts with legal, ethical and governance perspectives. Early sections clarify terminology, emphasise the CIA triad and attack lifecycles, and introduce frameworks like the NIST CSF and the Cyber Kill Chain. The module then delves into EU cybersecurity laws, explaining the obligations imposed by NIS2, GDPR, DORA, the Cyber Resilience Act and upcoming AI legislation, and emphasises the importance of risk-management measures, incident reporting and supply-chain security. Ethical considerations are interwoven throughout, with discussions of privacy, fairness, accountability, harm minimisation and explicability - principles that are essential when deploying AI and other emerging technologies. The governance section teaches learners how clear roles, coordination and commitment enable effective security management, while the final case-study section provides hands-on practice in analysing incidents and producing audit-ready artefacts. Collectively, the module equips learners to navigate the complex intersection of technology, law and ethics in the evolving cybersecurity landscape.

2.2 LM2: Risk Management

Table 4 LM2 Extraction

Competence Level: Intermediate / Advanced	
This module focuses on the principles and practices of cybersecurity risk management. It covers fundamental concepts of identifying and assessing risks, understanding risk appetite, and implementing effective risk treatment strategies. Students will learn to propose and manage mitigation options, select and apply relevant information security controls, and leverage maturity models to enhance cybersecurity management. Through practical exercises and case studies, learners will gain hands-on experience in evaluating and improving risk management frameworks.	
Subject contents and topics	Learning outcomes (competences)
> Introduction to Risk Management > Risk Appetite, Risk Assessment, and Risk Treatment > Proposing and Managing Risk Mitigations Strategy and Options > Information Security Controls > Maturity Models for Cybersecurity Management > Practical Exercises and Case Studies > Review and Assessment	The student is able to: - Identify and categorize cybersecurity risks and their potential impacts on organizational assets. - Assess risk appetite, conduct risk assessments, and develop risk treatment plans aligned with business objectives. - Propose effective mitigation strategies and select appropriate security controls to reduce identified risks. - Apply maturity models to evaluate and enhance the organization's cybersecurity posture. - Analyze case studies to refine practical risk management decision-making skills.
Mapping with ENISA ECSF	

	Cybersecurity Risk Manager, Cybersecurity Auditor.
--	--

Link to Open edX: https://apps.ngsoc-training-platform.eurodyn.com/learning/course/course-v1:NG-SOC+LM2+2025_Q1/home

The Risk Management module is designed to give learners a structured understanding of how cybersecurity risks are identified, assessed, evaluated and treated within an organisation. The module begins by establishing a common vocabulary of risk, threat, vulnerability, asset and impact, then progresses through risk appetite, evaluation, treatment planning, control selection, mitigation strategies, maturity models and assessment. A recurring theme is the need to translate high-level policies and appetite statements into measurable tolerances, thresholds and controls that support governance and decision-making. To reinforce the concepts, the module uses a running narrative centred on *TechNova Logistics* and later *BlueLine Energy*, where learners apply the theory to IoT sensor malfunctions, cloud/API exposures and privileged-access misuse. Reading materials (including ISO/IEC 27005 clauses, IRM practitioner guides and industry papers) and open-response exercises encourage reflection and critical thinking.

TechNova Logistics is used as a running case study in the Risk Management module. *BlueLine Energy* appears later as another scenario organisation, most likely representing an energy or critical-infrastructure operator. Their relation to the **NG-SOC EU project** is therefore **pedagogical**. They function as realistic teaching cases inside the NG-SOC training platform, helping learners practise the skills targeted by the project: risk analysis, governance, control selection, mitigation planning, stakeholder communication and alignment with ENISA ECSF roles such as Cybersecurity Risk Manager and Cybersecurity Auditor.

2.2.1 Section 1: Introduction to Cybersecurity Risk Management

✓ SECTION 1: Introduction to Cybersecurity Risk Management

✓ Introduction 1 min

✓ Lesson 1: Understanding Cybersecurity Risk 3 min + 5 activities

Figure 7 LM2 Section 1 on Open edX

The first section establishes foundational terminology and explains why risk management is central to cybersecurity governance. Learners are asked to define **risk**, **threat**, **vulnerability**, **asset**, **consequence** and **impact**, and to explain how risk criteria guide decision-making. The introduction notes that risk management supports organisational governance because it provides a structured mechanism for aligning security decisions with objectives, regulatory obligations and tolerance for uncertainty. Another objective is to distinguish internal sources of risk (e.g., misconfigurations, insider threats) from external ones (e.g., supply-chain vulnerabilities, geopolitical factors) and to summarise the stages of the information-security risk management process—from establishing context to identification, analysis, evaluation, treatment and monitoring. Learners are then asked

to apply the terminology to an IoT scenario involving irregular sensor readings at *TechNova Logistics*; they consider whether the problem represents a cybersecurity risk and what information is needed to assess it.

Lesson 1: Understanding Cybersecurity Risk

This lesson explains the logic connecting assets, threats and vulnerabilities. Risk arises when a threat exploits a vulnerability affecting an asset, creating a measurable likelihood and consequence. Learners compare **risk assessment** (estimating likelihood and impact) with **risk evaluation** (comparing results to risk criteria to decide on treatment) and **risk analysis** (systematically examining components to derive estimates). They are reminded that risk ownership must be defined because a risk without an owner cannot be managed. The lesson also highlights the difference between risk and routine technical malfunctions: a malfunction becomes a risk only when it has adverse effects on confidentiality, integrity or availability. A scenario asks learners to interpret early warning signals, differentiate between technical failures and genuine risks, and decide what additional data (e.g., event logs, asset information) is needed. To deepen understanding, a reading assignment directs learners to ISO/IEC 27005 clause 3 (Terms & Definitions), urging them to focus on definitions of **risk**, **threat**, **vulnerability**, **likelihood**, **consequence** and **risk criteria**, and to note the distinction between risk assessment, analysis and evaluation. Another reading explores the evolution and purpose of risk management, emphasising that structured risk management provides organisations with a disciplined way of making decisions under uncertainty and supports governance frameworks such as NIST CSF. The section closes with an ungraded concept test that asks learners to differentiate risk analysis (estimating likelihood and consequence) from risk evaluation (comparing those estimates to risk criteria), reinforcing the conceptual distinction.

Risk Categories and Sources

A final reading invites learners to consider how enterprises categorise risks. Using the *Introduction to Risk Management* text, the page distinguishes **strategic**, **operational**, **reporting** and **compliance** risk categories and reminds learners that tools like risk registers and checklists can aid in identification. Internal sources of risk include human error, system misconfiguration and outdated controls, while external sources may involve market volatility, vendor vulnerabilities or regulatory changes. The reading stresses the importance of cause-and-effect thinking—for example, how a misconfigured IoT sensor (cause) could lead to unauthorised data exposure (effect) and degrade service quality. Learners are asked to describe three categories of risks in their own words, encouraging articulation of the distinctions among them.

2.2.2 Section 2: Risk Appetite, Risk Evaluation and Risk Treatment

✓ SECTION 2: Risk Appetite, Risk Evaluation and Risk Treatment

- ✓ Introduction 1 min
- ✓ Lesson 1: Risk Appetite and Risk Evaluation 3 min + 5 activities
- ✓ Lesson 2: Risk Treatment Planning 1 min + 5 activities
- ✓ Concept Test 1 min + 1 activity

Figure 8 LM2 Section 2 on Open edX

This section bridges policy-level risk appetite with operational risk treatment. The introduction lists objectives such as explaining the difference between **risk appetite**, **risk tolerance** and **limits**; drafting risk-appetite statements with measurable thresholds; proposing key risk indicators (KRIs) to monitor risk; evaluating risks against criteria and deciding whether to accept, monitor or treat; and selecting appropriate treatment options such as avoidance, modification, sharing or retention. Learners also learn to produce concise treatment-plan entries specifying actions, owners, timelines and residual risk notes.

Lesson 1: Risk Appetite and Risk Evaluation

Learners explore how organisations make risk appetite actionable. Risk appetite expresses the amount and type of risk an organisation is willing to pursue or retain to achieve its objectives, whereas **risk tolerance** defines acceptable variation around that appetite. The narrative scenario introduces *BlueLine Energy*, an electricity-distribution operator that has expanded its IoT infrastructure and outsourced analytics; the newly appointed risk manager must convert high-level appetite statements into measurable tolerances, define threshold zones (within, watch, outside appetite), and set escalation triggers. Students practice drafting risk appetite statements by reading *Risk Appetite Explained Guide* and related papers. They learn to convert qualitative statements into thresholds and define KRIs that provide early warning when risk is approaching or exceeding tolerance. An exercise requires drafting a risk appetite statement for BlueLine Energy covering service continuity, privileged-access misuse and supplier risk, with measurable thresholds and escalation triggers.

A subsequent reading focuses on **risk evaluation**. Based on ISO/IEC 27005 clause 7.4⁴, risk evaluation compares analysed risks against risk criteria, identifies whether risks fall within appetite or tolerance, prioritises them, and determines what actions are required. Learners are asked to articulate the purpose of evaluation and to propose criteria for evaluating BlueLine Energy's top risk. Another activity has them classify the risks identified earlier (e.g., privileged-access misuse, IoT vulnerabilities, cloud/API exposure, monitoring/logging gaps) according to whether they sit within or outside appetite, and to justify the decision using the tolerance categories.

Lesson 2: Risk Treatment Planning

The second lesson covers treatment planning and residual-risk governance. Students learn to choose among four treatment options—**avoid**, **modify/mitigate**, **share/transfer** and **retain**—and to appreciate that transferring risk may reduce impact but rarely affects likelihood. They study ISO/IEC 27005 clause 8.2 & 8.3 and consider how to select controls that reduce likelihood and/or impact. The lesson emphasises that treatment plans should be concise yet actionable, detailing the control mechanism, scope, owner, timeline and evidence required to show completion. Learners practice drafting treatment entries, defining residual-risk governance (how and when to review residual risk) and setting monitoring triggers for re-evaluation.

⁴ <https://www.iso.org/standard/80585.html>

2.2.3 Section 3: Proposing and Managing Risk Mitigations Strategy and Options

- ✓ **SECTION 3: Proposing and Managing Risk Mitigations Strategy and Options**
 - ✓ Introduction 1 min
 - ✓ Lesson 1: From “Treat” Decisions to a Mitigation Strategy 2 min + 3 activities
 - ✓ Lesson 2: Planning, Tracking and Governing Mitigations 1 min + 4 activities
 - ✓ Concept Test 1 min + 1 activity

Figure 9 LM2 Section 3 on Open edX

This section teaches learners to translate treatment decisions into an overarching mitigation strategy. The introduction explains that learners will prioritise out-of-appetite risks, align mitigations with risk drivers, and justify sequencing based on risk reduction potential and constraints. They must define control objectives for each risk, propose layered mitigations (prevent, detect, respond, recover), plan quick wins versus structural fixes, design compensating controls when primary mitigations are delayed, and document evidence and monitoring signals. The narrative scenario continues: as a new member of BlueLine Energy’s risk team, learners must deliver a prioritised mitigation strategy, a 90-day plan with milestones and owners, and KRIs showing whether risk is trending back within tolerance. Exercises ask them to select control catalogue entries, build a small “control package” for one risk, and craft Plan of Action & Milestones (POA&M) entries.

2.2.4 Section 4: Information Security Controls

- ✓ **SECTION 4: Information Security Controls**
 - ✓ Introduction 1 min
 - ✓ Lesson 1: Control Fundamentals and Control Taxonomy 2 min + 2 activities
 - ✓ Lesson 2: Using Control Catalogs and Writing Implementable Controls 2 min + 3 activities
 - ✓ Concept Test 1 min + 1 activity

Figure 10 LM2 Section 4 on Open edX

Information security controls implement the treatment choices identified earlier. The section’s general objectives are to explain what a control is and how controls support risk reduction, distinguish control intent (preventive, detective, corrective, directive) from control form (procedural/people, physical/environmental, technical/logical), navigate major control catalogues such as ISO/IEC 27002, NIST SP 800-53 and CIS Controls, and draft concise implementation statements with mechanism, scope, owner and evidence. Learners first study control fundamentals, comparing control intent versus form and practising how to design balanced control sets that remain resilient if individual controls fail. A reading assignment summarises Appendix D of *Information Risk Management: A practitioner’s guide*, highlighting distinctions between strategic, tactical and operational

controls; preventive, detective, directive and corrective types; and procedural/people, physical/environmental and technical/logical forms.

Subsequent pages teach learners how to interpret control catalogue language. They compare the structure of ISO/IEC 27002, NIST SP 800-53 and CIS Controls and learn to “parameterise” controls by specifying scope, values, ownership and implementation approach. The lesson emphasises writing implementable control statements that specify intent, coverage, review period and evidence. Exercises ask learners to propose controls for a cloud/API exposure risk and classify each control by intent and form, including evidence that demonstrates operation.

2.2.5 Section 5: Maturity Models for Cybersecurity Management

- ✔ **SECTION 5: Maturity Models for Cybersecurity Management**
 - ✔ Introduction 1 min
 - ✔ Lesson 1: Understanding Cybersecurity Maturity Models 1 min + 2 activities
 - ✔ Lesson 2: Applying Maturity Models in Cybersecurity Governance 1 min + 4 activities
 - ✔ Concept Test 1 min + 1 activity

Figure 11 LM2 Section 5 on Open edX

The penultimate section introduces maturity models as tools for planning improvement. The introduction instructs learners to use a presentation to understand maturity concepts and then complete study-guide activities. Its general objectives include explaining what a maturity model is and why organisations use maturity assessments, describing maturity levels and differentiating ad-hoc performance from defined and continuously improved processes, conducting a lightweight maturity assessment for domains like logging or access management using evidence-based reasoning, translating a target maturity level into an improvement roadmap, and explaining how maturity relates to but is distinct from compliance or risk acceptance decisions.

Lesson 1: Understanding Cybersecurity Maturity Models

This lesson defines maturity as a measure of consistency and effectiveness of cybersecurity activities. Learners explore what maturity models measure - process consistency, governance, measurement discipline and continuous improvement - and examine the five levels of the Capability Maturity Model (CMM): Initial/Ad hoc, Managed, Defined, Quantitatively Managed and Optimising. They identify practical indicators distinguishing each level for cybersecurity activities, such as existence of documented processes, role clarity, metrics and continual learning. The lesson emphasises evidence-based assessments: maturity ratings should be supported by artefacts and records that demonstrate how processes are performed and improved. Short exercises ask learners to read about the CMM and apply maturity levels to logging and monitoring.

Lesson 2: Applying Maturity Models in Cybersecurity Governance

The second lesson operationalises maturity by linking levels to evidence and improvement planning. Learners perform a lightweight maturity assessment, defend their rating using observable evidence, and set a realistic target maturity level aligned to risk exposure, operational needs and organisational capacity. They design a staged roadmap with people, process and technology milestones and clear accountability. Additional guidance helps them choose maturity metrics that reveal both capabilities build-out (coverage and discipline) and outcome improvement (performance), and to use maturity reporting to support governance decisions such as assurance, prioritisation and exception handling. Short activities include mini-assessments for logging and monitoring, building a six-month maturity roadmap and reflecting on differences between maturity, compliance and risk acceptance.

2.2.6 Section 6: Final Review & Assessment Quiz

✓ SECTION 6: Final Review & Assessment Quiz

✓ Final Review & Assessment Quiz (20 Questions) 1 min + 1 activity
 Final Review & Assessment

Figure 12 LM2 Section 6 on Open edX

The sixth section consists of a comprehensive assessment, typically a 20-question quiz covering all prior sections. It allows learners to review key concepts - terminology, risk appetite and evaluation, treatment options, control types, mitigation strategies and maturity models - and to test their understanding before completing the module. Completing the assessment contributes to course completion and ensures learners can apply the material.

2.2.7 Section 7: Practical Exercises and Case Studies

✓ SECTION 7: Practical Exercises and Case Studies

✓ Practical Exercises and Case Studies 1 min

Figure 13 LM2 Section 7 on Open edX

The final section (not fully accessible in the instructor view but noted in the course outline) contains practical exercises and case studies. Based on preceding narrative scenarios (TechNova Logistics and BlueLine Energy), learners work through realistic risk-management challenges. Tasks likely include identifying additional risks in an IoT-heavy environment, drafting appetite statements and treatment plans for new scenarios, selecting controls from catalogues, designing mitigation strategies with sequencing, and performing maturity assessments. These exercises aim to reinforce skills by moving from guided instruction to independent application and encourage learners to provide structured responses, often requiring open-response text. The section may also include peer discussion or instructor feedback, helping learners refine their reasoning and decision-making.

2.2.8 Conclusion

Learning Module 2 equips learners with the knowledge and tools necessary to manage cybersecurity risk systematically. Beginning with a clear lexicon and conceptual distinctions between assessment, evaluation and treatment, the module guides learners through the steps of determining risk appetite, measuring and prioritising risks, selecting treatment options, designing layered controls and mitigation strategies, and assessing organisational maturity. Throughout, case studies and scenario-based questions ground the theory in realistic contexts, ensuring that participants can translate high-level concepts into actionable plans. By the end of the module, learners should be able to articulate and justify risk decisions, design balanced control packages, develop evidence-based maturity roadmaps, and communicate effectively with stakeholders about cybersecurity risk and governance.

2.3 LM3: Auditing and Assessment

Table 5 LM3 Extraction

Competence Level: Intermediate / Advanced	
This module provides a comprehensive understanding of cybersecurity auditing and assessment processes. It begins with fundamental auditing concepts and the evaluation of auditor competence, then explores recognized standards, frameworks, and methodologies. Learners will gain knowledge on managing audit programs, conducting thorough audits, performing data protection and privacy impact assessments, and working toward relevant certifications. Practical exercises and case studies will help translate theoretical knowledge into applied auditing skills.	
Subject contents and topics	Learning outcomes (competences)
> Introduction to Auditing > Principles of Auditing, Competence and Evaluation of Auditors > Auditing Standards, Methodologies, Frameworks, and Tools > Managing an Audit Programme > Conducting an Audit > Conducting Data Protection Impact Assessments / Privacy Impact Assessments > Auditing-Related Certification > Practical Exercises and Case Studies > Assessment	The student is able to - Understand fundamental principles and standards of cybersecurity auditing. - Evaluate auditor competence and apply recognized methodologies, frameworks, and tools. - Manage an audit program, from planning and resource allocation to reporting findings. - Conduct data protection and privacy impact assessments to ensure compliance and safeguard personal information. - Prepare for audit-related certifications to enhance professional credibility.
	Mapping with ENISA ECSF

Cyber Legal, Policy & Compliance Officer, Cybersecurity Risk Manager, Cybersecurity Auditor.

Link to Open edX: <https://apps.ngsoc-training-platform.eurodyn.com/learning/course/course-v1:NG-SOC+LM3+2025Q1/home>

Learning Module 3 on the NG-SOC Training Platform introduces cybersecurity auditing and assessment as complementary activities within a security programme. It emphasises that **auditing** provides structured verification of controls and compliance, while **assessment** takes a broader, risk-oriented view to identify weaknesses and drive improvement. Throughout the module, learners progress from conceptual foundations and regulatory frameworks (Section 1), through hands-on auditing procedures and adversary emulation (Section 2), into vulnerability assessments (Section 3), report writing and remediation (Section 4), and a final review (Section 5). The course uses scenarios, external readings and lab exercises to illustrate key points, and it stresses ethical practice, independence and continuous improvement.

2.3.1 Section 1: Introduction to Auditing & Assessment

- ✔ **SECTION 1 – Introduction to Auditing and Assessment**
 - ✔ Section Introduction
 - ✔ Lesson 1 - Understanding the Foundations of Auditing & Assessment
 - ✔ Lesson 2 – Standards and Frameworks: Choosing the Right Map for the Terrain

Figure 14 LM3 Section 1 on Open edX

The opening section defines the scope of auditing and assessment and positions them within security governance. The **section objectives** instruct learners to distinguish between audits (structured verification) and assessments (broader evaluations), explain their roles in compliance and continuous improvement, introduce widely used standards (NIST CSF, ISO/IEC 27001, NIST SP 800-53 and CIS Controls v8) and consider auditor qualifications.

Lesson 1: Understanding the Foundations of Auditing & Assessment

A scenario casts learners as advisers preparing an organisation for its first cybersecurity audit. It explains that *internal* audits verify controls while *external* audits provide independent assurance, whereas assessments such as risk reviews or vulnerability scans support ongoing governance. A video underscores that regular evaluations are important for organisations of all sizes. Sub-lessons then explore the difference between risk assessment and control verification via UK NCSC materials and summarise the NIST Cybersecurity Framework: six core functions (Govern, Identify, Protect, Detect, Respond and Recover) that guide the integration of audits and assessments across the cyber-security lifecycle. Learners are reminded that although external providers can assist, organisations remain accountable for understanding risk and remediating findings.

Lesson 2: Standards and Frameworks: Choosing the Right Map

This lesson helps learners match organisational needs to appropriate frameworks.

- **ISO/IEC 27001** - described as a systematic management framework for information security using a Plan-Do-Check-Act cycle. Adopting the standard embeds security into business processes and allows organisations to demonstrate maturity and credibility.
- **NIST SP 800-53 (Rev. 5)** - offers a catalogue of controls organised by families (Access Control, Incident Response, etc.). It suits organisations requiring rigorous, customisable controls and is often mandated for US Federal and critical-infrastructure sectors.
- **CIS Controls v8** - provides 18 prioritised controls grouped into implementation groups IG1-IG3, offering a practical starting point for small and medium-sized businesses or early-maturity programmes. The lesson encourages learners to consider risk appetite, sector obligations and resource availability when choosing frameworks, and ends with a quiz on certification requirements and control prioritisation.

2.3.2 Section 2: Auditing Process and Techniques

✓ SECTION 2 – Auditing Process and Techniques

- ✓ Section Introduction
- ✓ Lesson 1 – Planning and Conducting Audits: Setting the Groundwork for Trust
- ✓ Lesson 2 – Automated Auditing Tools: Let the Machines Do Their Work

Figure 15 LM3 Section 2 on Open edX

This section moves from theory to practice. Its objectives are to describe each stage of the audit lifecycle (planning through reporting), tailor methodologies to context, apply manual and automated tools, evaluate auditor competence (ISO 19011) and manage the audit programme end-to-end.

Lesson 1: Planning and Conducting Audits: Setting the Groundwork for Trust

Learners join a fintech audit team and must define the audit's scope, identify interviewees and review documentation while maintaining independence. Sub-lessons emphasise risk-based planning, the need to state clear objectives and scope, and the use of checklists and templates from organisations like ISACA to ensure consistent evidence collection. Readings outline typical audit steps from pre-engagement through reporting, highlighting limitations such as scope and timing and reinforcing that competent, independent auditors are essential. A quiz tests understanding of audit limitations, planning tools and the role of independence.

Lesson 2: Automated Auditing Tools: Let the Machines Do Their Work

The second lesson introduces **MITRE Caldera** and **Wazuh** as tools for adversary emulation and log monitoring. Students act as junior auditors in a managed security services provider, simulating attacks in a sandbox and analysing detection. A video explains Caldera's modular architecture and its mapping to the MITRE ATT&CK framework, while another sub-lesson explores the Caldera GitHub repository and encourages customising operations. Learners then study Wazuh dashboards to see how SIEM systems collect and correlate logs, tune detection rules and visualise anomalies.

A live lab on the **KYPO Cyber Range** has students deploy Caldera on a Kali Linux VM and simulate adversarial campaigns (e.g., credential dumping or lateral movement). They monitor Wazuh alerts, compare detected versus

undetected events and analyse logs. The scenario “Operation RedTrace” describes a virtual enterprise with machines such as Audit-Control-01 (Kali/Caldera), WebServer-01 (Ubuntu with Apache2 and an outdated CMS), FileServer-01 (Windows with SMB and RDP), DomainController (Active Directory) and a SIEM Node running Wazuh. The lab workflow instructs learners to launch the environment, deploy agents, run campaigns, analyse outputs and manually review logs to identify missed detections. Guiding questions encourage reflection on which tactics were detected or missed, how quickly alerts were generated and how rules might be tuned. Deliverables include a campaign summary, detection matrix, mini-audit report and reflection on automation vs. manual analysis. The exercise aims to build hands-on skills with red-team automation, SIEM monitoring and evidence-based reporting.

2.3.3 Section 3: Vulnerability Assessment

✓ SECTION 3 – Vulnerability Assessment

- ✓ Section Introduction
- ✓ Lesson 1 – Principles of Vulnerability Assessment: What Lies Beneath
- ✓ Lesson 2 – Advanced Analysis Techniques: Thinking Like an Attacker, Reporting Like a Professional

Figure 16 LM3 Section 3 on Open edX

Section 3 introduces vulnerability assessment as a proactive counterpart to audits. The **section introduction** highlights core concepts and testing strategies, helping learners prioritise vulnerabilities by severity and business impact, practise tools such as KYPO, Nessus and OpenVAS, and emphasise continuous mitigation.

Lesson 1: Principles of Vulnerability Assessment

A scenario describes a cloud services company that narrowly avoided a breach due to an exposed API. Learners must understand what vulnerabilities are, how they emerge and why some matter more. The lesson covers types of vulnerabilities (injection flaws, misconfigurations, weak credentials) and shows how attack chains exploit multiple weaknesses. An article included from Rapid7 stresses that vulnerability assessments are required by compliance regimes and enable targeted penetration tests; turning raw scan data into actionable intelligence is essential, and effective communication helps engage non-technical stakeholders. Rapid7’s tools illustrate risk-based scoring, dynamic filters and dashboards. Learners also review the CISA Cyber Resilience Review to understand capabilities that support vulnerability management and incident detection. A hands-on challenge using CVE entries has students classify vulnerabilities, estimate CVSS v3 scores and select mitigation strategies.

Lesson 2: Advanced Analysis Techniques: Thinking Like an Attacker, Reporting Like a Professional

The second lesson frames learners as red-team analysts performing an advanced assessment. It involves scanning systems with multiple tools, comparing results, mapping attacker paths and producing remediation roadmaps. Sub-lessons instruct learners to log into CyberRangeCZ, verify access to Linux and Windows targets and use the network topology to plan lateral movement; to consult documentation on launching, pausing and

snapshotting scenarios and on log generation; and to read a tool-comparison study that discusses detection accuracy, false positives, scan depth, and when active or passive scanning is appropriate.

The “Red Team Debrief Challenge” is a capstone exercise executed in teams. Phase 1 (Discovery and Enumeration) requires scanning targets with OpenVAS or Nessus and documenting critical vulnerabilities. Phase 2 (Threat Mapping) involves using the MITRE ATT&CK framework to simulate attacker paths and identify chokepoints. Phase 3 (Risk-Based Remediation Planning) asks teams to prioritise vulnerabilities by CVSS score and business impact, propose mitigation (patching, segmentation, access control) and prepare a remediation matrix with urgency and responsible teams. Phase 4 (Executive and Technical Debrief) requires drafting two reports: a concise executive summary and a detailed annex for SOC and IT teams, explaining trade-offs and feasibility. After completion, learners should be able to simulate and analyse vulnerabilities in a real-world scenario, compare scanning tools, create priority-driven remediation plans and communicate risk to non-technical audiences.

2.3.4 Section 4: Reporting and Remediation

✓ SECTION 4 – Reporting and Remediation

- ✓ Section Introduction
- ✓ Lesson 1 – Audit and Assessment Reporting: One Truth, Two Voices
- ✓ Lesson 2 – Remediation and Continuous Improvement: From Findings to Fixes
- ✓ Lesson 3 – Data Protection and Privacy Impact Assessments (DPIA/PIA): Seeing Privacy Before the Risk Becomes Real

Figure 17 LM3 Section 4 on Open edX

The fourth section focuses on translating technical findings into actionable reports and remediation plans. Its objectives are to craft professional reports for multiple audiences, structure findings effectively, develop remediation plans with short- and long-term goals and use feedback loops to improve audit programmes.

Lesson 1: Audit and Assessment Reporting: One Truth, Two Voices

This lesson highlights the need to tailor reports to both technical and executive readers. Learners study the **UpGuard Cyber Incident Reporting Guide**, noting the core components of a report, the importance of timeliness and clarity, and how technical evidence must support business decisions. Next, they review **CYNET’s Incident Response Template**, examining how risks are framed differently for technical vs. non-technical audiences, the inclusion of sections on threat intelligence, timelines and remediation status, and the use of visual cues such as colour-coded severity indicators.

The third sub-lesson introduces **AuditScripts** templates, encouraging learners to explore formats for executive summaries, detailed findings and audit closure. It emphasises language differences between stakeholder reports and the value of evidence referencing and traceability tables. An interactive concept test reinforces lessons on tailoring content to audiences and using severity matrices in reports.

Lesson 2: Remediation and Continuous Improvement: From Findings to Fixes

Learners transition into the role of remediation strategists. Having presented an audit report, they must turn findings into a roadmap: prioritise actions, assign owners, define key performance indicators (KPIs), align remediation with policies and track success. They explore the **CICMS** tool— a collaborative platform for documenting incidents and remediation — and learn how incidents are categorised, remediation actions assigned and progress tracked with dashboards. Reviewing the CICMS documentation teaches how to open cases, assign stakeholders, track status and support long-term improvement cycles. Another sub-lesson directs learners to **CISA’s Free Cybersecurity Services and Tools**, focusing on resources for vulnerability mitigation, patch management, system hardening, endpoint detection, configuration checks, phishing simulations and public-private collaboration. The section ends with a concept test covering remediation planning, KPIs and remediation tracking tools.

Lesson 3: Data Protection and Privacy Impact Assessments (DPIA/PIA): Seeing Privacy Before the Risk Becomes Real

The final lesson of Section 4 introduces privacy impact assessments. Learners join a cross-functional team building a healthcare app that collects geolocation and health data; before development continues, they must decide whether a DPIA is required under GDPR. The lesson emphasises **proactive privacy risk management**— understanding when a DPIA or PIA is legally or ethically required (e.g., under GDPR Articles 35-36 or ISO/IEC 27701), defining the scope, assessing necessity and proportionality, identifying risks to individuals’ rights and freedoms and proposing mitigation. The curriculum explains legal triggers and operational triggers for DPIAs, types of personal data, documentation structure and aligning privacy assessments with standards and audit readiness.

Learners then read **EDPB guidelines** to determine when DPIAs are required, the risk-based approach to personal data protection and examples of high-risk processing. They examine the **ISO/IEC 27701** privacy management standard, learning how it extends ISO/IEC 27001, how DPIA documentation can align with ISO control categories and why consistent terminology aids audit readiness. A presentation on Data Protection Impact Assessment highlights the CNIL methodology, legal triggers under GDPR, and the distinction between information security risk assessments and data protection impact assessments. The concept test at the end asks learners about the three “feared events” in the CNIL methodology (illegitimate access, unwanted change and disappearance of personal data), roles such as the Data Protection Officer and factors used to evaluate risk.

2.3.5 Section 5: Review and Assessment



SECTION 5: Review and Assessment



Review & Assessment (21 Questions)

Final Review & Assessment

Figure 18 LM3 Section 5 on Open edX

The final section provides a comprehensive review. Learners answer **21 multiple-choice questions** covering all previous sections — auditing vs assessment, standards and frameworks, audit processes, vulnerability assessment methods, reporting techniques, remediation planning and privacy impact assessments. The assessment allows learners to confirm their understanding and identify topics requiring further study.

2.3.6 Conclusion

Learning Module 3 offers a structured journey through cybersecurity auditing and assessment. It begins by clarifying foundational concepts and frameworks, then builds practical auditing skills through planning, execution and automation. It extends into vulnerability assessment, emphasising both foundational scanning and red-team analysis, and it teaches learners to translate findings into clear, audience-appropriate reports and actionable remediation plans. The module closes with privacy impact assessments and a final review, encouraging learners to integrate privacy considerations into audits and to self-evaluate their grasp of the material. Through scenarios, external readings, labs and quizzes, the module fosters the independence, ethical conduct and continuous improvement expected of modern cybersecurity auditors and assessors.

2.4 LM4: Cybersecurity Policies and Frameworks

Table 6 LM4 Extraction

Competence Level: Intermediate / Advanced	
This module focuses on the creation, implementation, and maintenance of effective cybersecurity policies and frameworks. It covers international and industry standards, supply chain security policies, and the application of Information Security Management Systems (ISMS). Learners will explore strategies for process improvement and quality management, ensuring that cybersecurity measures align with organizational objectives and compliance requirements.	
Subject contents and topics	Learning outcomes (competences)
> Understanding and Developing Cybersecurity Policies and Frameworks > Cybersecurity standards > Cybersecurity Policies in the Supply chain > Information Security Management Systems (ISMS) > Process Improvement and Quality Management > Review and Assessment	The student is able to - Understand key cybersecurity standards and frameworks (e.g., ISO/IEC 27001). - Develop and implement tailored cybersecurity policies, including those governing supply chain activities. - Establish and maintain an effective ISMS aligned with organizational goals and regulatory requirements. - Apply principles of process improvement and quality management to enhance the cybersecurity posture. - Critically review and assess existing policies to ensure their relevance, effectiveness, and continuous improvement.
	Mapping with ENISA ECSF
	Cyber Legal, Policy & Compliance Officer, Cybersecurity Risk Manager, Cybersecurity Auditor, Cybersecurity Implementer.

Link to Open edX: <https://apps.ngsoc-training-platform.eurodyn.com/learning/course/course-v1:NG-SOC+LM4+2025Q1/home>

Learning Module 4 in the NG-SOC training platform provides a comprehensive exploration of governance, risk and compliance (GRC) in cyber-security. It guides learners through the policy development lifecycle, global and sector-specific standards, supply chain security, information security management systems and quality-management frameworks. The module is structured into six sections with scenario-based exercises that challenge learners to apply theoretical knowledge in realistic contexts. This document summarises the content and key takeaways from each section, supplementing the brief guidelines provided on the platform with additional research from reputable sources.

2.4.1 Section 1: Understanding and Developing Cybersecurity Policies and Frameworks

✓ SECTION 1: Understanding and Developing Cybersecurity Policies and Frameworks

✓ Lesson 1 - The Policy Playbook 21 min + 1 activity

✓ Section 01 Concept Test 1 min + 1 activity

Figure 19 LM4 Section 1 on Open edX

The first section introduces the policy playbook. Learners are told that they are applying for a role in a security operations centre (SOC) and must articulate the purpose of an information security policy (ISP) and its essential components. The introduction emphasises balancing organisational security with user privacy and compliance requirements. Key objectives include recognising a standard ISP structure, understanding the relationship between technical controls and mandatory policies, and appreciating how high-level mandates translate into SOC tasks.

Policy development lifecycle

The tasks direct learners to study an article on information security policies and a chapter from *Safeguarding Your Technology*⁵. From general research, an ISP should outline an organisation's strategy for protecting information assets. Policies describe roles and responsibilities, define acceptable use, identify technical and administrative safeguards, and state consequences for non-compliance. Effective policies should be concise, free of jargon, and aligned with business objectives. When drafting policies, stakeholders must identify sensitive data, classify it according to confidentiality and integrity requirements, and select appropriate controls (e.g., encryption, access control) to mitigate risks.

A well-structured ISP typically includes:

- **Purpose and scope** - explains why the policy exists and the information systems it covers.
- **Information classification and ownership** - categorises data and assigns owners to ensure accountability.
- **Roles and responsibilities** - outlines duties of employees, managers, IT staff and security teams.
- **Acceptable use rules** - defines permitted and prohibited activities on corporate systems.

⁵ <https://nces.ed.gov/pubs98/98297.pdf>

- **Security controls** - lists mandatory technical measures such as authentication, encryption and network segmentation.
- **Incident response and reporting** - describes procedures for reporting breaches or security incidents.
- **Compliance and enforcement** - cites relevant laws and standards and details consequences for violations.

The platform encourages learners to identify the relationship between an ISP and standards such as ISO/IEC 27001 and NIST SP 800-53. Since policies are high-level statements, they should reference controls from recognised frameworks to ensure completeness and alignment with best practice. Finally, policies must be periodically reviewed and updated to remain relevant in the face of evolving threats.

Scenario-based Q&A and concept test

This section includes scenario-based questions where learners are asked to propose policy components for a hypothetical organisation. The concept test assesses whether learners understand that policies must be clear, consistent and free from conflicting statements. The tasks emphasise the importance of not including vague, aspirational language in an ISP, as this undermines enforceability.

2.4.2 Section 2: Cybersecurity standards

✓ SECTION 2: Cybersecurity standards

✓ Lesson 1: The Global Cybersecurity Blueprint 2 min + 1 activity

✓ Section 02 Concept Test 1 min + 1 activity

Figure 20 LM4 Section 2 on Open edX

The second section provides an overview of international and regional standards. Learners should recognise the purpose of frameworks such as ISO/IEC, NIST and regional regulations (e.g., the GDPR) and understand how governance, risk management and compliance are interrelated. The narrative scenario places learners in a SOC at a cloud service provider confronted with a potential data leak affecting a medical application; management asks which ISO standard applies to cloud-hosted personal data, which national data-protection act applies to the company's branch in Singapore, and what US healthcare regulation applies if American data are involved. The scenario illustrates the complexity of complying with multiple jurisdictions when operating internationally.

Global standards: ISO/IEC 27000 series and ISO/IEC 27001

The ISO/IEC 27000 family of standards provides a comprehensive set of guidelines for information security management. ISO/IEC 27001:2022 is the core standard that specifies requirements for establishing, implementing and improving an information security management system (ISMS). It requires organisations to identify information security risks, implement appropriate controls and undertake continual improvement. A 2024 amendment (ISO/IEC 27001:2022+A1:2024) requires organisations to consider climate change as an external issue when determining their context and interested parties. Achieving ISO 27001 certification involves defining the ISMS scope, performing a risk assessment, selecting controls from Annex A, and undergoing internal and external audits. Certification is typically valid for three years, with surveillance audits annually.

The broader 27000 series include standards like ISO/IEC 27002:2022, which provides a code of practice and guidance on selecting and implementing information security controls. It reorganises controls into four themes - organisational, people, physical and technological - with 93 controls in total. Each control is mapped against attributes such as its type (preventive, detective, corrective), information security properties (confidentiality, integrity, availability), cybersecurity concepts (identify, protect, detect, respond, recover) and security domains. Other parts of the 27000 series provide additional guidance, such as risk management (ISO/IEC 27005), cloud security (ISO/IEC 27017), and privacy information management (ISO/IEC 27701).

NIST frameworks and US regulations

NIST publishes frameworks that complement ISO standards. The NIST Cybersecurity Framework (CSF) outlines five functions - identify, protect, detect, respond and recover - that form the basis for a risk-based cyber-security programme. The framework is voluntary but widely adopted. NIST SP 800-53 provides a catalogue of security controls for federal systems, while the NIST Privacy Framework helps organisations integrate privacy considerations into their risk management.

In the healthcare sector, the United States Health Insurance Portability and Accountability Act (HIPAA) includes the Security Rule, which establishes national standards for protecting electronic protected health information (ePHI). The rule requires regulated entities to ensure the confidentiality, integrity and availability of ePHI, to protect against anticipated threats, and to ensure workforce compliance. It is technology-neutral and designed to be scalable for entities of different sizes.

Regional and sector-specific frameworks

- **European Union (EU) - GDPR:** The General Data Protection Regulation regulates the processing of personal data of EU residents, imposing strict requirements on data controllers and processors. It includes obligations such as lawful processing, data subject rights, data protection impact assessments and mandatory breach notification.
- **Payment Card Industry Data Security Standard (PCI DSS):** The PCI Security Standards Council oversees PCI DSS, which aims to protect payment card data throughout the payment lifecycle. It sets technical and operational requirements for merchants, service providers and financial institutions to secure cardholder data. The standard covers security management, policies, network architecture and software design.
- **Industrial and energy sectors (NERC CIP, ISO 27019):** The North American Electric Reliability Corporation's Critical Infrastructure Protection (CIP) standards apply to power transmission systems, requiring utilities to implement cyber-security measures for critical infrastructure. ISO/IEC 27019 provides guidelines for information security management in energy utility organisations.
- **Telecommunications sector:** National regulators may require compliance with standards such as ETSI EN 303 645 for consumer IoT devices and the Telecommunications Security Act in the UK, which mandates baseline security requirements for telecom operators.

The platform instructs learners to examine diagrams showing how different frameworks fit together, emphasising the central role of ISO 27001 and the interrelationships among sector-specific standards.

2.4.3 Section 3: Cybersecurity policies in the Supply Chain

✔ Section 3: Cybersecurity policies in the Supply Chain

✔ Lesson 1: The Strategic importance of the Supply Chain Security 2 min + 1 activity

✔ Section 03 Concept Test 1 min + 1 activity

Figure 21 LM4 Section 3 on Open edX

The third section focuses on security risks arising from complex ICT supply chains. Organisations increasingly rely on third-party suppliers for hardware, software and services; vulnerabilities at any point in the chain can result in data breaches or operational disruption. Task 01 asks learners to research the ISO/IEC 27036 standard series. These standards provide guidance for managing information security in supplier relationships. ISO/IEC 27036 is designed to be integrated with ISO/IEC 27001, 27002, 27005, 28000, 27017 and 27701. The series comprises four parts: (1) overview and concepts; (2) requirements for supplier and acquirer relationships; (3) guidelines for hardware, software and services supply chain security; and (4) cloud services. It emphasises transparency and traceability across supplier relationships and aims to protect information and information systems throughout the supplier lifecycle.

The tasks highlight specific points to examine: understanding the purpose and structure of Part 1; recognising the supplier-acquirer relationship and termination process in Part 2; identifying management activities and the importance of transparency in Part 3; and recognising the need for technical solutions to maintain supply chain integrity. Students are encouraged to think about real-world practices such as supplier risk assessments, contractual clauses on information security, secure development and acquisition, and monitoring of supplier performance.

NIST SP 800-161 Rev. 1 - Cyber-Security Supply Chain Risk Management (C-SCRM)

Task 02 introduces NIST SP 800-161 Revision 1, published in 2021, which provides guidance on identifying, assessing and mitigating supply chain risks. The publication emphasises integrating cyber-security supply chain risk management (C-SCRM) into organisational risk management activities. A multi-level risk management approach is proposed: an **enterprise/executive tier** sets the strategic direction and policy; a **mission/business process tier** translates strategy into processes; and an **operational tier** implements risk management and monitoring. The standard suggests developing C-SCRM strategies and plans, establishing processes to identify and evaluate suppliers, and implementing controls to mitigate risks. An article summarising the document notes that over 60 % of data breaches result from third-party exposure and that 90 % of organisations experienced an incident due to a third-party failure, underscoring the urgency of robust supply chain security programmes.

Key practices and guidelines

Both ISO/IEC 27036 and NIST SP 800-161 advocate the following practices:

1. **Risk assessment and due diligence** - evaluate suppliers' security posture, financial stability and compliance history before engagement.
2. **Contractual controls** - include clauses on information security requirements, right to audit and incident reporting.

3. **Transparency and traceability** - maintain visibility into supplier sub-tiers and require suppliers to cascade security requirements down their supply chains.
4. **Continuous monitoring** - monitor supplier performance, conduct periodic audits and adjust risk assessments when threats or business relationships change.
5. **Incident response coordination** - ensure that suppliers and the organisation coordinate responses to incidents to minimise impact.

By instilling these practices, organisations can mitigate supply chain risks and ensure that third-party dependencies do not undermine overall security.

2.4.4 Section 4: Information Security Management Systems (ISMS)

✓ SECTION 4: Information Security Management Systems (ISMS)

✓ Lesson 1: Navigating ISO/IEC 27001 2 min + 1 activity

✓ Section 04 Concept Test 1 min + 1 activity

Figure 22 LM4 Section 4 on Open edX

This section deepens the discussion of ISMS frameworks, focusing on ISO/IEC 27001 and its supporting standards. Building on the earlier overview, learners are expected to understand the structure of an ISMS and its stages: planning, implementing, monitoring and continual improvement. The platform may provide the official ISO 27001 document for reference, though accessibility may be limited.

Structure of an ISMS

An ISMS is a systematic approach to managing sensitive information to ensure confidentiality, integrity and availability. It involves:

1. **Context and scope definition** - identify internal and external issues (including legal, regulatory and environmental factors) and determine the scope of the ISMS.
2. **Leadership and planning** - obtain commitment from top management, define information security objectives, and plan actions to address risks and opportunities.
3. **Support and operation** - establish resources, competencies and awareness, document processes, and implement controls to manage risks.
4. **Performance evaluation** - monitor, measure and evaluate the effectiveness of the ISMS through audits, performance metrics and management reviews.
5. **Improvement** - address nonconformities, apply corrective actions and seek continual improvement. The 2022 update emphasises iterative learning and adaptation.

Control selection and implementation (ISO/IEC 27002)

Annex A of ISO 27001 references controls described in ISO/IEC 27002. The four themes and 93 controls described earlier should be tailored to the organisation's needs. For example:

- **Organisational controls** include information security policies, roles and responsibilities, business continuity management, supplier relationships and compliance.
- **People controls** cover background checks, confidentiality agreements, security awareness training, disciplinary processes and remote working.
- **Physical controls** involve secure areas, entry controls, equipment security and protection against environmental threats.
- **Technological controls** address network security, data protection, access management, secure development, vulnerability management and logging.

Implementing these controls requires integration with existing processes and coordination across departments. The new attribute taxonomy helps organisations prioritise controls according to risk, business objectives and resource availability.

Certification and benefits

Certification to ISO 27001 signals that an organisation follows internationally recognised best practices. Benefits include improved risk management, competitive advantage, potential safe-harbour under certain data-protection laws and increased customer trust. However, achieving and maintaining certification requires ongoing commitment, investment in training and periodic audits.

2.4.5 Section 5: Process Improvement and Quality Management

- ✓ **SECTION 5: Process Improvement and Quality Management**
 - ✓ **Lesson 1: Measuring Process Excellence** 2 min + 1 activity
 - ✓ **Section 05 Concept Test** 1 min + 1 activity

Figure 23 LM4 Section 5 on Open edX

This section introduces process improvement frameworks that complement cyber-security standards by promoting quality, efficiency and maturity.

Capability Maturity Model Integration (CMMI)

CMMI is a process improvement framework that helps organisations develop high-quality products and services. It evolved from the Capability Maturity Model (CMM) and integrates best practices from multiple disciplines. CMMI emphasises process standardisation, measurement-based improvement and organisational alignment. Two representations exist:

- **Staged representation:** organisations progress through five maturity levels-Initial, Managed, Defined, Quantitatively Managed and Optimising. Each level builds upon the previous one, introducing standardised processes, quantitative management and continuous improvement.
- **Continuous representation:** organisations focus on specific process areas and can achieve capability levels individually, allowing more flexibility.

CMMI's structured approach helps organisations reduce risk, improve predictability and deliver consistent quality. For cyber-security, a higher maturity level indicates that security is embedded into development and operational processes.

ISO 9001 - Quality Management Systems

ISO 9001 is an internationally recognised standard that sets out criteria for a quality management system (QMS). It provides a framework for establishing, implementing, maintaining and improving quality processes. ISO 9001 is applicable to any organisation, regardless of size or sector. Core principles include customer focus, leadership commitment, engagement of people, process approach, improvement, evidence-based decision making and relationship management.

Organisations use ISO 9001 to build a QMS by documenting processes, setting quality objectives, identifying non-conformities and implementing corrective actions. Certification demonstrates the ability to consistently deliver products and services that meet customer and regulatory requirements. It can enhance reputation, facilitate international trade and provide a framework for continuous improvement. Integrating ISO 9001 with cyber-security practices ensures that security controls are aligned with broader quality and business objectives.

HIPAA Security Rule and sector-specific standards

While not primarily a process improvement framework, the HIPAA Security Rule exemplifies how sector-specific regulations incorporate quality and risk management. It mandates administrative, physical and technical safeguards to protect ePHI. Ensuring confidentiality, integrity and availability of ePHI requires systematic processes, workforce training and continuous evaluation, aligning with the principles of quality management. Other industry frameworks, such as NERC CIP for energy utilities and the Payment Card Industry Data Security Standard, similarly require structured processes to maintain compliance and improve security.

Relationship among frameworks

Learning Module 4 emphasises that process improvement and quality-management frameworks like CMMI and ISO 9001 complement cyber-security standards. Implementing ISO 27001 without a strong QMS may lead to inconsistent procedures and poor documentation, while achieving high CMMI maturity requires robust security controls to protect intellectual property and customer data. Integrating these frameworks fosters a holistic culture of security and quality.

2.4.6 Section 6: Final Review and Assessment



Section 06: Final Review and Assessment



Final Review and Assessment (20 Questions) 1 min + 1 activity

Final Review & Assessment

Figure 24 LM4 Section 6 on Open edX

The final section of Learning Module 4 consists of a timed assessment with twenty multiple-choice questions. It is designed to verify understanding of the topics covered in Sections 1-5, including policy development, global and sector-specific standards, supply chain security, ISMS frameworks and process improvement. The

instructions encourage learners to use the assessment as a tool for reinforcement and to identify subjects that may need additional study. No new technical content is introduced; rather, the assessment summarises key points and challenges learners to apply their knowledge to realistic scenarios.

2.4.7 Conclusion

Learning Module 4 provides a holistic overview of the governance, risk and compliance landscape in cyber-security. The module starts by emphasising the importance of clear, enforceable policies that define roles, responsibilities and technical requirements. It then explores global and sector-specific standards, highlighting the central role of ISO 27001 and the need to integrate multiple frameworks when operating in different jurisdictions. Supply chain security emerges as a critical area, with ISO/IEC 27036 and NIST SP 800-161 offering practical guidance for managing third-party risks. The module also delves into information security management systems, underlining the iterative nature of improvement and the value of certification, and introduces process improvement and quality-management frameworks. It concludes with a final review and assessment to consolidate learning and highlight areas for further improvement.

For SOC analysts and security professionals, understanding this ecosystem of policies, standards and frameworks is essential. Implementing these frameworks requires organisational commitment, cross-departmental collaboration and ongoing monitoring. When combined, they provide a strong foundation for protecting assets, complying with regulations and achieving operational excellence.

2.5 LM5: Technical Analysis and Security Management

Table 7 LM5 Extraction

Competence Level: Intermediate / Advanced	
This module delves into the technical aspects of cybersecurity, covering a broad range of topics including network and system security, secure programming, malware analysis, vulnerability management, and security architecture. Learners will gain hands-on experience with tools and techniques for analyzing threats, implementing secure software development practices, managing logs, and configuring secure infrastructures (including cloud environments). Through practical exercises and case studies, they will learn to identify threat actors, apply security best practices, and assess the effectiveness of cybersecurity controls.	
Subject contents and topics	Learning outcomes (competences)

> Introduction to Technical Analysis and Security Management > Computer and Communication Network Security > Computer Programming for Security Professionals > Computer Systems Vulnerabilities > Malware Analysis Tools > Secure Software Development and Best Practices > Security Architecture Reference Models - Identifying Threat Actors, Vulnerabilities management and TTPs > Log File Management and Analysis > Working with Operating Systems, Servers, and Cloud Infrastructures > Implementing Cybersecurity Recommendations and Best Practices > Assessing Cybersecurity Controls > Practical Exercises and Case Studies > Assessment	The student is able to - Understand fundamental and advanced principles of computer and communication network security. - Apply secure programming and software development best practices to mitigate vulnerabilities. - Identify and analyze computer system vulnerabilities, malware, threat actors, and their Tactics, Techniques, and Procedures (TTPs). - Implement security architecture models and deploy effective security controls across operating systems, servers, and cloud infrastructures. - Use log management and analysis techniques to detect, respond to, and prevent security incidents. - Assess and validate cybersecurity controls to ensure robust protection and compliance with best practices.
	Mapping with ENISA ECSF
	Cybersecurity Implementer, Digital Forensics Investigator, Cyber Incident Responder, Cybersecurity Architect.

This Learning Module 5 does not contain an Open edX module, as it consists of KYPO/CRCZ cyber ranges:

- LM5 Network Vulnerability Identification Training 1b (section 3.4 of this document).
- LM5 Malware Attack Detection & Response Training 1c (section 3.6 of this document).

In addition, the D5.2 is a technical deliverable, and it describes the KYPO/CRCZ platform.

2.6 LM6: Business Integration and Strategy

Table 8 LM6 Extraction

Competence Level: Intermediate / Advanced
--

This module bridges the gap between cybersecurity and organizational objectives. It guides learners on how to align cybersecurity strategies with broader business goals, analyze processes to identify and implement appropriate security controls, and stay abreast of evolving technological and cybersecurity trends. Additionally, it covers effective communication with stakeholders, methods to influence cybersecurity culture, and approaches to integrating cybersecurity awareness and privacy considerations into business decision-making.

Subject contents and topics	Learning outcomes (competences)
> Aligning Cybersecurity with Business Strategy > Analyzing Business Processes and Security Controls > Technology Trend Monitoring and Cybersecurity Trends > Establishing a Cybersecurity Plan > Communication and Stakeholder Engagement > Cybersecurity and Privacy Awareness, Influencing Cybersecurity Culture and Managing Change > Review and Assessment	The student is able to - Align cybersecurity strategies, plans, and controls with organizational business objectives. - Evaluate and integrate cybersecurity considerations into business processes and workflows. - Monitor emerging technology and cybersecurity trends to inform strategic decision-making. - Develop and maintain a comprehensive cybersecurity plan that includes communication strategies and stakeholder engagement. - Foster a strong cybersecurity culture within the organization, influencing behaviour and managing change effectively.
	Mapping with ENISA ECSF
	Cyber Legal, Policy & Compliance Officer, Cybersecurity Risk Manager, Cybersecurity Architect.

Link to Open edX: <https://apps.ngsoc-training-platform.eurodyn.com/learning/course/course-v1:NG-SOC+LM6+2025Q1/home>

The module addresses how cybersecurity has evolved from a reactive technical function into a proactive business enabler and offers learners a structured approach for aligning security with organisational objectives. Each section builds on the last: the early lessons introduce strategic concepts and alignment frameworks, the middle sections provide analytical and planning methodologies, and the later lessons focus on communication, culture and practical case studies. The final assessment synthesises these themes into an integrated review.

2.6.1 Section 1: Introduction to Cybersecurity Strategy

- ✓ **Section 1: INTRODUCTION TO CYBERSECURITY STRATEGY**
- ✓ Lesson 1: Introduction to Cybersecurity Strategy 3 min
- ✓ Section 1 Concept Test (5 Questions) 1 activity
Section Concept Tests

Figure 25 LM6 Section 1 on Open edX

The module begins by explaining how the security function has shifted from patching systems and installing firewalls to influencing investment decisions, product launches and mergers. Modern CISOs report to boards, quantify risks in business terms and coordinate with legal, HR and finance. A key message is that security has become a strategic enabler: a breach or successful attack can derail market expansion, while a well-designed security posture can unlock opportunities.

To professionalise this discipline, the module introduces roles defined by ENISA's European Cybersecurity Skills Framework. A cyber legal, policy and compliance officer translates regulation into policy and ensures audit readiness; a cybersecurity risk manager quantifies and prioritises risks based on asset value and business impact; and a cybersecurity architect designs reference architectures and integrates controls across initiatives. The section also presents the ALIGN-ANALYSE-ANTICIPATE-ARCHITECT-ADVOCATE framework: alignment of security with business goals; analysis of processes and controls; anticipation of emerging technologies and threats; architecture of comprehensive programmes and communication strategies; and advocacy to build a security-minded culture. Fundamental definitions of risk, threat, vulnerability and impact set the stage for later quantitative models.

2.6.2 Section 2: Aligning Cybersecurity with Business Strategy

- ✓ **Section 2: ALIGNING CYBERSECURITY WITH BUSINESS STRATEGY**
- ✓ Lesson 1: Aligning Cybersecurity with Business Strategy 4 min
- ✓ Section 2 Concept Test (5 Questions) 1 activity
Section Concept Tests

Figure 26 LM6 Section 2 on Open edX

Strategic alignment means translating business goals into security requirements rather than bolting on controls after the fact. Learners are taught to map a business strategy (e.g., geographic expansion) to critical assets (customer databases, payment systems), identify key risks (data breaches, fraud, vendor compromise) and derive appropriate controls (encryption, compliance with PCI-DSS, vendor assessments). This translation is formalised in the Cyber-SAFE framework: Strategy translation links board directives to security objectives; Asset mapping inventories the assets that support those objectives; Forecast risk identifies threats and vulnerabilities affecting each asset; and Execute controls involves choosing and prioritising mitigations such as multi-factor authentication or rate-limiting.

Justifying investment is essential to win support from executives. The module presents several ROI models. Risk-reduction value compares the expected cost of incidents before and after implementing controls. For example, reducing the likelihood of a \$5 million breach from 20 % to 5 % lowers the expected loss from \$1 million to \$250 000; if controls cost \$200 000, the first-year ROI is 375 %. Compliance value measures fines avoided and insurance reductions; an example shows that avoiding a \$1.5 million fine and reducing premiums by \$100 000 produces a 640 % ROI on a \$250 000 investment. Business enablement evaluates revenue unlocked by a security initiative, such as a new digital service generating \$2 million for a \$300 000 investment (667 % ROI). Cost-avoidance assesses how controls lower the probability of costly incidents; reducing breach likelihood from 5 % to 2 % saves enough to justify a \$40 000 investment. A case study illustrates these calculations: implementing an enterprise data-loss prevention system costing \$500 000 reduced a \$2.5 million risk and delivered payback in six months.

2.6.3 Section 3: Analysing Business Processes and Controls

- ✓ **Section 3: ANALYSING BUSINESS PROCESSES AND SECURITY CONTROLS**
- ✓ Lesson 1: Analysing Business Processes and Security Controls 5 min
- ✓ Section 3 Concept Test (5 Questions) 1 activity
Section Concept Tests

Figure 27 LM6 Section 3 on Open edX

To move from strategy to operations, the module adapts the DMAIC [25] methodology for security. In the Define step, learners map end-to-end processes and stakeholders; Measure identifies data flows, storage points and existing controls; Analyse models threats, vulnerabilities and impacts; Improve designs layered controls; and Control institutes monitoring and continuous improvement. A layered approach is reinforced by the P-A-T-D framework: Preventive measures (encryption, authentication, secure coding), Administrative controls (policies, training, change management), Technical tools (data-loss prevention, endpoint detection, SIEM, multi-factor authentication) and Detective measures (audit logging, anomaly detection, security audits). Combining these layers, for example to defend against ransomware, ensures attacks are blocked, detected quickly and contained.

The section also introduces a business process security maturity model that describes progression from ad-hoc, reactive practices through standardised, measured and optimised stages. Higher maturity levels feature consistently implemented controls, metrics and predictive analytics. Learners apply these concepts through a detailed risk treatment plan. A high-risk data-breach scenario identifies a 30 % annual likelihood and \$10 million impact; mitigation controls (encryption, access control, DLP, monitoring and testing) reduce the annual risk value from \$3 million to \$500 000. With an implementation cost of \$500 000, the project yields a 500 % ROI.

2.6.4 Section 4: Technology Trend Monitoring and Threat Intelligence



Figure 28 LM6 Section 4 on Open edX

Strategic planning must anticipate disruptive technologies and evolving threats. The module highlights several trends:

- AI and machine learning offer enhanced threat detection and fraud prevention but introduce risks such as adversarial attacks, model poisoning and algorithmic bias. Learners are advised to test AI tools for adversarial robustness, establish governance frameworks and build intelligence on AI-specific attack techniques.
- Quantum computing threatens current cryptography; a “harvest now, decrypt later” scenario could expose long-lived secrets. Organisations should inventory cryptographic assets, classify data by sensitivity, monitor NIST standards and plan migration to post-quantum algorithms.
- Zero-Trust architecture replaces perimeter-centric security with continuous verification. Benefits include reduced breach impact and better remote-work security, but challenges include complexity and operational overhead. Strategic actions involve piloting zero-trust in non-critical areas, redesigning identity management and training teams.
- IoT and OT convergence brings remote monitoring and efficiency but expands the attack surface. Many industrial devices are hard to patch; critical risks include supply-chain compromise and physical safety impacts. Mitigation requires inventories, network segmentation, encryption, device monitoring and adoption of sector-specific standards like IEC 62443.

The section then examines threat intelligence maturity. Early stages involve ad-hoc monitoring of vendor reports; intermediate stages incorporate vendor feeds and participation in information-sharing communities; advanced stages involve custom indicator correlation and predictive analytics with deception technologies. An associated Threat Intelligence Action Cycle guides organisations to collect and normalise data from internal and external sources, analyse patterns and trends, disseminate tailored reports to technical and executive stakeholders, and feed lessons into threat hunting and control improvement. A complementary horizon scanning process groups risks into short-term (0-12 months) known threats, medium-term (12-36 months) emerging issues like AI-driven social engineering, and long-term (36+ months) transformational risks such as quantum computing. It emphasises data collection (e.g., technology research, regulatory proposals), interpreting signals, analysing strategic implications and producing foresight reports for executives

2.6.5 Section 5: Establishing a Cybersecurity Plan

- ✓ **Section 5: ESTABLISHING A CYBERSECURITY PLAN**
 - ✓ Lesson 1: Establishing Aa Cybersecurity Plan 3 min
 - ✓ Section 5 Concept Test (5 Questions) 1 activity
Section Concept Tests

Figure 29 LM6 Section 5 on Open edX

A cybersecurity plan turns strategy into an operational roadmap. The module recommends including an executive summary (business case, risk landscape, high-level objectives), risk management strategy (current assessment, risk appetite and treatment priorities), technology and architecture strategy (current state, target architecture and roadmap), operating model (roles, structure and governance forums), people and culture strategy (awareness programme, recruitment and culture transformation), third-party management (vendor requirements and assessment processes), metrics and measurement (key performance indicators and reporting cadence) and review and continuous improvement mechanisms.

Plan development follows phased steps: (1) Current state assessment using frameworks like NIST CSF to inventory technology and capacity and review compliance; (2) Target state definition aligned with business strategy and risk appetite; (3) Gap analysis and prioritisation across people, process and technology to quantify gaps and sequence initiatives; (4) Roadmap and investment cases with multi-year sequencing and ROI calculations; and (5) Governance and execution model that defines operating structures, communication plans and review cycles. A worked example of a risk treatment plan for a data-breach scenario shows how controls like encryption, access management, DLP and monitoring can reduce both the likelihood and impact of an incident and generate a high return on investment.

2.6.6 Section 6: Communication and Stakeholder Engagement

- ✓ **Section 6: COMMUNICATION AND STAKEHOLDER ENGAGEMENT**
 - ✓ Lesson 1: Communication and Stakeholder Engagement 4 min
 - ✓ Section 6 Concept Test (5 Questions) 1 activity
Section Concept Tests

Figure 30 LM6 Section 6 on Open edX

Effective execution depends on communicating the right information to the right audience at the right time. A stakeholder communication framework identifies stakeholders (board, executive committee, business unit leaders, IT leadership, security team, compliance and risk functions, employees) and tailors messages. Boards care about strategic risk, regulatory exposure and investment returns; they should receive quarterly dashboards and risk heatmaps summarising incident history and compliance. Business unit leaders need monthly updates on programme progress, incidents and upcoming audits, while the security team requires weekly operational

briefings. Employees are engaged through awareness campaigns and training, with metrics such as phishing-simulation performance and e-learning completion rates to measure progress.

The module emphasises presenting risk in business language. A risk heatmap plots severity against likelihood to highlight critical and manageable risks. A business-impact scenario demonstrates that a database breach involving two million records could incur \$10-50 million in fines and cause revenue loss through customer churn. Proposed investments, such as adopting parameterised queries and automated threat detection, can reduce risk by 90 % and save more than \$1.6 million. Another example shows that implementing an endpoint detection and response solution that reduces detection time from eight hours to 20 minutes and incident impact by 40 % yields a 900 % ROI and pays for itself within a month.

For incident communication, the module defines three tiers: the security operations centre escalates incidents to security leadership (Tier 1) with an initial summary and recommended containment; the executive leadership and legal teams (Tier 2) receive details on scope and business impact within an hour; and external stakeholders (Tier 3), including regulators and customers, are informed in non-technical terms, describing data affected, containment actions, guidance for customers and any compensation offered. Four escalation levels—green (normal), amber (elevated), red (major) and black (existential)—dictate communication frequency and urgency. For example, in a red incident, internal briefings occur every hour, external communication within 24 hours and board briefings daily.

2.6.7 Section 7: Cybersecurity Culture, Privacy Awareness and Change Management

- ✓ **Section 7: CYBERSECURITY CULTURE, PRIVACY AWARENESS, AND CHANGE MANAGEMENT**
- ✓ Lesson 1: Cybersecurity Culture, Privacy Awareness, and Change Management 6 min
 - ✓ Section 7 Concept Test (5 Questions) 1 activity
Section Concept Tests

Figure 31 LM6 Section 7 on Open edX

Building and sustaining a security-conscious culture is essential for long-term success. While the available course materials offer only a high-level overview, they suggest using behavioural models such as COM-B (Capability, Opportunity, Motivation → Behaviour) to design interventions. Capability is built through training and skills development; opportunity is created by embedding security into processes and tools; motivation arises from leadership communication, incentives and peer influence. Privacy-by-design principles require that data protection considerations are embedded into system design rather than bolted on later, and change management frameworks emphasise early stakeholder engagement, clear communication of benefits and continuous feedback to reduce resistance. Although detailed examples are scarce in the source materials, Section 7 underscores that technical controls and plans will fail unless people understand, accept and adopt secure practices.

2.6.8 Section 8: Case Studies and Practical Applications

- ✔ **Section 8: CASE STUDIES AND PRACTICAL APPLICATIONS**
- ✔ Lesson 1: Case Studio and Practical Applications 1 min
- ✔ Lesson 2: Real-World Case Studies 3 min
- ✔ Lesson 3: Sector-Specific Strategies 2 min
- ✔ Section 8 Concept Test (5 Questions) 1 activity
Section Concept Tests

Figure 32 LM6 Section 8 on Open edX

The penultimate section applies strategic concepts to real incidents and sector-specific scenarios. Learners are provided with a structured case-study framework comprising six elements: organisational context (industry, size, regulatory environment and security posture), event description (what happened and how it was discovered), root-cause analysis (vulnerabilities, control failures, organisational factors), response effectiveness (time to containment, coordination and communication), strategic implications (regulatory and business impact, industry-wide risks) and lessons and improvements (what could be done differently, lessons for the organisation and adjustments to strategy).

Three notable case studies illustrate this framework. *SolarWinds supply chain compromise (2020)*: attackers inserted malware into SolarWinds' Orion updates, allowing lateral movement and credential theft across approximately 18 000 customers. Root causes included weak access controls in the build system, inadequate monitoring and slow detection; the company suffered significant reputational damage and costs exceeding \$300 million. Lessons emphasised the criticality of supply-chain risk management, continuous monitoring of build pipelines, extending zero-trust principles to vendors and the need for industry-wide software-signing improvements.

Colonial Pipeline ransomware attack (2021) [27]: the DarkSide group exploited an old VPN account with a default password to deploy ransomware. Weaknesses included inadequate network segmentation between IT and operational technology (OT), poor password hygiene and lack of multifactor authentication. The attack led to a multi-day shutdown of fuel distribution across the US East Coast, requiring ransom payment and emergency declarations. The case highlighted the critical importance of OT security, defence-in-depth for legacy systems, rigorous access controls and clear policies on ransom payments.

Financial services data breach: a disgruntled employee at a mid-sized investment firm exfiltrated a customer database and proprietary trading algorithms via personal cloud storage. Inadequate insider-threat controls, permissive BYOD policies and insufficient data classification allowed the breach to go undetected for three weeks. The organisation faced lawsuits, fines and damage estimated at \$20 million. Lessons include the need for strong data classification, continuous monitoring of privileged users, separation of duties and robust offboarding processes.

The section ends by examining sector-specific strategies. In the **healthcare** sector, patient safety, legacy devices and privacy regulations necessitate inventorying medical devices, segmenting networks, adopting NIST/IEC 62443 controls for operational technology, embedding privacy by design and building incident response

capability. **Financial services** require API security, real-time fraud detection, redundant systems for business continuity, granular audit trails and rigorous third-party risk management. **Manufacturing and industrial** organisations must protect operational technology through network segmentation, supply-chain risk management for industrial components, layered defences and OT-specific anomaly detection, balancing safety and productivity

2.6.9 Final Review & Assessment

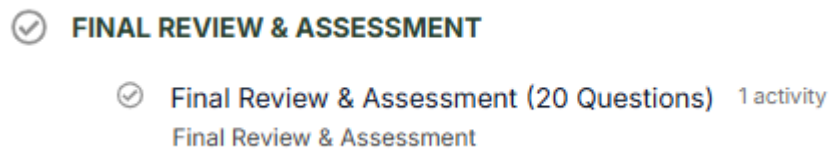


Figure 33 LM6 Final Review & Assessment on Open edX

The module concludes with a **final review and assessment** comprising twenty questions that span all sections. The assessment reinforces key concepts such as the correct timing for notifying internal leadership in incident communications (e.g., within one hour for Tier 2 leadership), the importance of change management and stakeholder engagement for major security initiatives, and other core topics like risk frameworks, threat intelligence maturity, cybersecurity planning and culture. This summative exercise tests learners' ability to integrate strategic alignment, process analysis, emerging-threat monitoring, planning, communication, cultural change and sector-specific lessons. While the review is interactive, its underlying purpose is to ensure that participants can apply the frameworks and principles in realistic scenarios; sample questions challenge learners to recall how incident communication tiers operate and why technological deployments fail when change management is neglected.

2.6.10 Conclusion

Learning Module 6 takes students on a journey from understanding why cybersecurity matters strategically to developing comprehensive plans and engaging people to execute them. It blends conceptual frameworks with quantitative models, hands-on analysis and real-world case studies. By the end of the module learners understand how to align security with business goals, justify investments, analyse processes, anticipate technological disruption, plan comprehensively, communicate effectively and cultivate a security-centric culture. The final case studies and assessment tie the lessons together, demonstrating that cybersecurity strategy is not only about technical controls but about integrating people, processes and technology to support business objectives in a rapidly evolving threat landscape.

2.7 LM7: Privacy and Data Protection

Table 9 LM7 Extraction

Competence Level: Intermediate / Advanced	
This module provides a comprehensive understanding of privacy and data protection principles, focusing on the legal, ethical, and regulatory frameworks that govern personal data in the digital era. It addresses challenges introduced by Artificial Intelligence (AI), emphasizes conducting Data Protection Impact Assessments (DPIAs) and Privacy Impact Assessments (PIAs), and explores the use of Privacy-Enhancing Technologies (PET). Learners will also understand how privacy considerations intersect with digital forensics, ensuring data protection obligations are met throughout the investigative process.	
Subject contents and topics	Learning outcomes (competences)
> Introduction to Privacy and Data Protection > Privacy and Data Protection Legal and Ethical issues in the Artificial Intelligence era > Conducting Data Protection Impact Assessments / Privacy Impact Assessments > Implementing Privacy-Enhancing Technologies (PET) > Privacy-preservation and Digital Forensics > Review and Assessment	The student is able to - Understand global and EU data protection laws, regulations, and ethical considerations, including those related to AI. - Conduct DPIAs/PIAs to identify, evaluate, and mitigate privacy risks. - Apply Privacy-Enhancing Technologies (PET) to protect personal data throughout its lifecycle. - Integrate privacy considerations into digital forensic procedures, ensuring evidence handling does not infringe on individual rights. - Embed privacy and data protection best practices into organizational policies, ensuring compliance and trustworthiness.
	Mapping with ENISA ECSF
	Cyber Legal, Policy & Compliance Officer, Cybersecurity Risk Manager.

Link to Open edX: <https://apps.ngsoc-training-platform.eurodyn.com/learning/course/course-v1:NG-SOC+LM7+2025Q1/home>

Learning Module 7 of the NG-SOC training curriculum examines privacy and data-protection principles and their interplay with cybersecurity in modern digital ecosystems. It is designed for security and compliance professionals who need to understand legal obligations under the European Union's General Data Protection Regulation (GDPR) and related standards, and to apply them in contexts ranging from everyday data handling to artificial-intelligence (AI) services, data-protection impact assessments (DPIAs), privacy-enhancing technologies (PETs) and digital forensics. The module consists of five sections—each with lessons, case studies and concept tests—and concludes with a final review. Throughout the module, narrative scenarios place the learner in

realistic roles (e.g., junior compliance analyst, data-protection officer) to illustrate how legal principles translate into operational decisions.

The following sections provide a detailed summary of each part, highlighting the key lessons, scenarios and practical guidance. Citations point to the NG-SOC course materials accessed during this research.

2.7.1 Section 1: Introduction to Privacy and Data Protection

✓ SECTION 1: Introduction to Privacy and Data Protection

✓ Introduction

✓ Lesson 1: Understanding the Fundamentals of Privacy and Data Protection

Figure 34 LM7 Section 1 on Open edX

The first section sets the foundation by explaining *why personal data requires enhanced protection*. Learners explore the distinction between **privacy**—concerned with who can access personal data—and **data protection**, which refers to the policies, technical controls and legal frameworks that govern and secure that data. The lesson introduces **GDPR's seven key principles**—lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity/confidentiality; and accountability—and links them to classic information-security goals (confidentiality, integrity, availability). It emphasises that organisations processing personal data must implement appropriate safeguards throughout the data life cycle.

The section's general objectives summarise the above goals: learners should explain why personal data needs special protection; *distinguish privacy from data protection* (with examples); describe/apply the main GDPR principles; demonstrate how privacy, data protection and security interrelate; and list the key GDPR rights of data subjects—access, rectification, erasure (the “right to be forgotten”), data portability, restriction and objection.

Narrative scenario: healthcare start-up

The course introduces a **scenario** set at a healthcare start-up building a mobile app that records exercise habits, heart-rate trends and location data. As a junior compliance analyst, the learner must advise senior management on the difference between privacy and data protection under EU law; explain why these concepts matter for a consumer-facing digital service; and suggest how GDPR principles can guide design decisions. The scenario highlights the tension between collecting valuable data for personalised services and respecting individuals' rights.

Distinguishing privacy and data protection

A complementary reading from Cloudian [26] clarifies that **data privacy** determines who is authorised to view personal data, while **data protection** focuses on the technical measures and policies that restrict access. Compliance with regulations (GDPR, HIPAA, PCI) ensures user privacy rights and requires companies to employ measures such as data-loss prevention, encryption, tokenisation and identity-access management. The module also references academic literature on the *legal construction of privacy and data protection*, asking learners to identify substantive differences between these rights and to apply them in a multinational mobile-app scenario. A concept test assesses understanding of when a DPIA is mandatory, with the correct answer being when processing is likely to **result in a high risk to the rights and freedoms of natural persons**.

2.7.2 Section 2: Privacy and Data Protection Legal and Ethical Issues in the AI era

✓ SECTION 2: Privacy and Data Protection Legal and Ethical issues in the Artificial Intelligence era

✓ Introduction

✓ Lesson 1: Legal and Ethical Challenges of AI in Privacy and Data Protection

Figure 35 LM7 Section 2 on Open edX

This section examines how **artificial intelligence** reshapes privacy and data-protection obligations. The general objectives highlight that AI systems can introduce new risk-bias, opaque decision-making, inference attack-and that GDPR principles must be applied throughout the AI lifecycle. Learners are expected to describe *fairness*, *transparency* and *accountability*; identify organisational measures such as records of processing, data-protection impact assessments, privacy notices and technical safeguards; and evaluate real AI scenarios.

Lesson 1: Legal and ethical challenges of AI

The lesson's introduction frames the discussion: AI is transforming business but raises complex legal and ethical questions. Learners revisit GDPR fundamentals and consider new regulatory instruments like the **EU AI Act**. They are given a narrative scenario: acting as a **data-protection officer** at an online retailer deploying an AI-driven recommendation engine that analyses browsing history, purchase records and location data. Management asks how GDPR principles of lawfulness, fairness and transparency apply; when a DPIA is required; what to do if customers request access or object to profiling; and which technical and organisational safeguards (e.g., model-governance logs, consent capture, human-in-the-loop reviews) can demonstrate compliance.

Refresher on GDPR basics

Before delving into AI specifics, learners revisit the **scope and lawful bases of GDPR**. A referenced article notes that GDPR has applied since 25 May 2018 and affects organisations worldwide that collect data from EU residents; compliance is daunting, especially for small enterprises, but penalties for violations are severe. A **compliance checklist** lists practical steps: conduct an information audit to map all data and legal bases; provide clear information in privacy policies; maintain an up-to-date register of processing activities (including data types, recipients, protection measures and deletion schedules); and ensure data-protection impact assessments and *privacy by design* are embedded into projects.

AI-specific guidance

Several resources extend the discussion to AI. Learners must read an excerpt from a **Training curriculum on AI and data protection** to understand how AI workflows interact with GDPR principles and identify risk points throughout the AI lifecycle. Another video segment, "10 Key Challenges for AI within the EU Data Protection Framework," explores how the proposed **EU AI Act** complements GDPR, describes overlapping obligations and challenges such as ensuring transparency for machine-learning models, documenting algorithmic decision-making, and managing bias. The module also includes case studies describing AI applications (e.g., facial-recognition, credit-scoring) and challenges learners to map legal principles to technical safeguards and derive lessons. A scenario-based exercise invites learners, acting as a DPO at a firm using machine-learning models, to identify three basic measures to ensure transparency and fairness when collecting personal data.

Ethical and legal dilemmas

Through these materials, the section emphasises that **AI projects require careful management of legal and ethical risks**: ensuring lawful processing (e.g., consent, legitimate interest), maintaining fairness and avoiding discriminatory outcomes, providing meaningful transparency about automated decisions, enabling human oversight, and documenting accountability. The narrative scenario, checklists and case studies encourage learners to adopt a holistic perspective, balancing innovation with compliance.

2.7.3 Section 3: Conducting Data Protection Impact Assessments (DPIAs) and Privacy Impact Assessments (PIAs)

- ✔ **SECTION 3: Conducting Data Protection Impact Assessments (DPIAs) and Privacy Impact Assessments (PIAs)**
 - ✔ Section Introduction
 - ✔ Lesson 1: Performing Data Protection and Privacy Impact Assessments (DPIAs /PIAs)

Figure 36 LM7 Section 3 on Open edX

Section overview and objectives

Section 3 guides learners through the **legal basis**, **triggers** and **practical steps** for DPIAs and PIAs. The introduction notes that DPIAs/PIAs are vital tools for embedding privacy by design and demonstrating compliance with GDPR's accountability requirements. The general objectives state that learners should explain the legal basis for DPIAs/PIAs; identify scenarios where a DPIA is mandatory; describe key stages in a DPIA (scoping, risk analysis, mitigation, documentation); map GDPR principles to each step; evaluate proposed processing activities and recommend safeguards; and prepare documentation that supports regulatory engagement.

Lesson 1: Performing DPIAs/PIAs

The lesson's introduction emphasises that DPIAs and PIAs help organisations systematically assess risks to data subjects and integrate privacy by design. Learners adopt the role of a DPO at a **smart voice assistant** project that stores voice commands and user data in the cloud. Management asks them to perform a DPIA to assess compliance. The course underscores that failing to conduct a DPIA when required can lead to regulatory penalties and reputational harm.

Understanding DPIA basics

A video segment summarises the **definition of a DPIA**, its legal basis under GDPR Article 35 and circumstances requiring one. A DPIA is required when processing is likely to result in **high risk** to individuals' rights and freedoms (e.g., large-scale profiling, systematic monitoring, processing of sensitive data). The module highlights that PIAs (more common outside the EU) share similar goals but may be voluntary or mandated by other laws.

Practical steps and templates

Learners review a detailed article outlining a **seven-step DPIA process**:

1. **Identify the need for a DPIA** (e.g., new technology, large-scale sensitive data).

2. **Describe the processing** (purpose, data flows, stakeholders, technical/organisational measures).
3. **Consider consultation** with stakeholders and data subjects.
4. **Assess necessity and proportionality** relative to the stated purpose.
5. **Identify and assess risks** to individuals' rights and freedoms.
6. **Identify mitigating measures** that reduce risk to an acceptable level (e.g., encryption, access controls, anonymisation).
7. **Sign off and record outcomes**, ensuring accountability.

The article explains who should conduct the DPIA and the DPO's role: while project managers may complete the assessment, the DPO advises on methodology and reviews results. Learners also watch a video demonstrating how to complete each section of a DPIA template and emphasising the link between identified risks and mitigation measures.

Scenario-based activity and concept test

A practice exercise asks learners, acting as a DPO at a health-tech start-up launching a mobile fitness app, to decide whether a DPIA is required, outline the assessment's key content and recommend mitigation measures such as minimising data collection and implementing robust encryption. The concept test checks comprehension by asking which element is *not* typically included in a DPIA; the correct answer is a **record of employee salaries**. This reinforces the focus on describing processing operations, assessing necessity and proportionality, identifying risks and measures to address them.

2.7.4 Section 4: Implementing Privacy Enhancing Technologies (PETs)

- ✓ **SECTION 4: Implementing Privacy-Enhancing Technologies (PETs)**
 - ✓ Section Introduction
 - ✓ Lesson 1: Using Privacy-Enhancing Technologies to Protect Personal Data

Figure 37 LM7 Section 4 on Open edX

The fourth section uses **PDF resources** (OECD Digital Economy Papers and an ENISA report) to introduce **privacy-enhancing technologies**. The material emphasises that PETs are a set of tools and techniques designed to protect personal data while enabling its analysis and use. Although the course does not provide interactive lessons for this section, the provided documents outline the **regulatory and policy landscape** for PETs and summarise technologies such as:

- **Homomorphic encryption** and secure multi-party computation, which allow computations on encrypted data without revealing raw inputs.
- **Differential privacy**, providing strong mathematical guarantees that individual contributions cannot be inferred from aggregate data.
- **Federated learning**, enabling machine-learning models to be trained across decentralised devices without transferring raw data.

- **Data anonymisation and pseudonymisation** techniques, along with privacy-preserving query systems.

The OECD paper—*Emerging Privacy Enhancing Technologies - Current Regulatory and Policy Approaches*—highlights that policymakers see PETs as crucial for reconciling data-intensive innovation with fundamental rights. The report argues that PET adoption should be encouraged through regulatory clarity, standards, incentives and cross-sector collaboration. The accompanying **ENISA report on Data Protection Engineering** emphasises integrating PETs into systems through privacy-by-design principles, risk-based requirements, and security engineering practices. Together, these resources urge organisations to evaluate PETs when designing AI and big-data projects, and to remain informed about evolving standards and best practices.

2.7.5 Section 5: Privacy preservation and Digital Forensics

✓ SECTION 5: Privacy-preservation and Digital Forensics

✓ Section Introduction

✓ Lesson 1: Privacy and Data Protection in Digital Forensics

Figure 38 LM7 Section 5 on Open edX

The final substantive section explores the tension between **digital forensic investigations** and the obligation to protect personal data. A PDF titled *Digital Forensic Framework for Protecting Data Privacy during Investigation* introduces a framework that leverages machine-learning techniques to filter relevant evidence and preserve privacy. Key points include:

- Digital forensics can inadvertently expose sensitive personal data; investigators must abide by legal frameworks (GDPR, national laws) governing data privacy.
- The proposed framework aims to collect and analyse evidence while minimising the intrusion into unrelated personal data.
- Machine-learning models can help automatically identify relevant evidence and flag data requiring additional anonymisation or protection.
- Combining privacy-preserving methods with forensic tools supports accountability and ensures evidence integrity.

The report emphasises that **cybersecurity professionals should collaborate with legal and privacy teams** when conducting investigations to balance the competing demands of evidence collection and data-subject rights. This section broadens the learner's perspective, showing that privacy considerations apply even in post-incident contexts.

2.7.6 Section 6: Review and Assessment

✓ SECTION 6: Review and Assessment

✓ Review and Assessment (22 Questions) Final Review & Assessment

Figure 39 LM7 Section 6 on Open edX

The module concludes with a **Review and Assessment** section designed to consolidate learning across all previous parts. This final part presents **22 multiple-choice questions** that test the learner's understanding of key concepts and practical applications. The introduction encourages participants to use the assessment to confirm comprehension of **GDPR principles, data-subject rights, legal and ethical AI challenges, DPIA/PIA processes, privacy-enhancing technologies, and privacy-preserving digital-forensics frameworks**. The questions cover diverse scenarios—for example, identifying when a DPIA is mandatory, distinguishing privacy from security, recognising AI-specific risks and selecting appropriate PETs. By summarising and testing the material, the assessment helps learners identify any areas that may require further study and reinforces the holistic, risk-based approach advocated throughout the module.

Final Review and Takeaways

The final portion of the module, summarised above under Section 6, consists of a **review and assessment** that tests comprehension across all topics through multiple-choice questions. This assessment encourages learners to revisit core concepts—such as distinctions between privacy and data protection, application of GDPR principles and data-subject rights, legal and ethical AI issues, DPIA/PIA processes, PETs and privacy-preserving digital forensics—and to identify areas requiring further study.

Cross-sectional themes

Several overarching themes emerge:

1. **Interdependence of privacy, data protection and security** - While privacy focuses on the right to control personal information and data protection provides mechanisms to enforce that right, both depend on sound security practices. GDPR principles integrate these domains and emphasise accountability.
2. **Risk-based approach and proactive measures** - DPIAs/PIAs and PETs exemplify proactive tools for identifying and mitigating risks before harm occurs. Organisations must integrate privacy by design throughout project lifecycles rather than rely on retroactive compliance.
3. **Challenges of emerging technologies** - AI introduces new risks such as bias, opacity and inference attacks. Regulatory frameworks like the EU AI Act aim to address these issues, but operationalising fairness and transparency requires careful design, documentation and human oversight.
4. **Balancing innovation with rights** - Whether deploying AI systems, performing vulnerability assessments, or conducting digital forensics, organisations must balance innovation and efficiency with individual rights and ethical considerations. Transparency, consent and purpose limitation are crucial tools in maintaining this balance.
5. **Continuous learning and adaptation** - The regulatory landscape is evolving, and privacy professionals must remain informed about new rules, guidance and technologies. Cross-disciplinary collaboration between legal, technical and organisational teams is essential for effective data protection.

2.7.7 Conclusion

Learning Module 7 provides a comprehensive exploration of privacy and data protection within a cybersecurity context. By combining legal frameworks, technical measures, ethical considerations and practical exercises, the module equips learners to navigate the complex challenges facing modern organisations. Through case studies and scenario-based activities, participants learn to translate abstract principles into actionable strategies for

compliance and risk management. Mastery of the topics covered—GDPR principles, AI legal issues, DPIA/PIA processes, PETs and privacy-preserving forensic frameworks—will enable cybersecurity professionals to design and audit systems that uphold individual rights while supporting organisational innovation.

2.8 LM8: Incident Response and Forensics

Table 10 LM8 Extraction

Competence Level: Intermediate / Advanced	
This module focuses on the skills and knowledge needed to effectively prepare for, detect, respond to, and recover from cybersecurity incidents. It covers established incident handling standards, methodologies, and frameworks, as well as the roles and operations of Computer Security Incident Response Teams (CSIRTs). Learners will gain experience in conducting technical analysis, documenting findings, and working within criminal investigation procedures, while adhering to digital forensics best practices. Through practical exercises and case studies, participants will develop the competencies necessary to manage incidents and support forensic investigations.	
Subject contents and topics	Learning outcomes (competences)
> Introduction to Incident Response and Forensics > Identifying Cybersecurity-Related Issues > Incident Handling Standards, Methodologies, and Frameworks > Operation of Computer Security Incident Response Teams (CSIRTs) > Conducting Technical Analysis and Reporting > Criminal Investigation Procedures in Cybersecurity > Digital Forensics Best Practices > Practical Exercises and Case Studies > Review and Assessment	The student is able to - Understand the incident response lifecycle, including preparation, detection, analysis, containment, eradication, and recovery. - Apply recognized standards, methodologies, and frameworks to structure and guide incident handling efforts. - Operate effectively as part of or in collaboration with CSIRTs, coordinating tasks and sharing critical information. - Conduct technical analyses to identify root causes, impacted systems, and nature of incidents, ensuring proper documentation and reporting. - Follow criminal investigation procedures and digital forensics best practices to preserve evidence integrity and support potential legal actions.
	Mapping with ENISA ECSF
	Cyber Threat Intelligence Specialist, Cyber Incident Responder, Digital Forensics Investigator, Cyber Legal, Policy & Compliance Officer.

Link to Open edX: <https://apps.ngsoc-training-platform.eurodyn.com/learning/course/course-v1:NG-SOC+LM8+2025Q1/home>

The eighth module of the **NG-SOC** curriculum introduces learners to the end-to-end processes required to detect, respond to, recover from and investigate cybersecurity incidents. The module emphasises the skills needed to prepare for incidents, identify and classify suspicious activity, apply standards-based response frameworks, operate a computer security incident response team (CSIRT), conduct technical analysis and forensics, and understand the legal and investigative dimensions of cyber-crime. The course begins with a high-level overview of what constitutes an incident, then moves through threat identification, detection methods, non-cyber factors, the incident handling lifecycle, standards and best practices, CSIRT organisation, technical analysis and reporting, criminal investigation procedures, digital forensics, and a final assessment. It uses case-based scenarios, reading assignments and presentations to reinforce the importance of both technical proficiency and procedural rigour.

2.8.1 Section 1: Introduction to Incident Response and Forensics

- ✓ **Section 1: Introduction to Incident Response and Forensics**
 - ✓ Introduction
 - ✓ Lesson 1: Introduction to Incident Response and Forensics
 - ✓ Concept Test

Figure 40 LM8 Section 1 on Open edX

The opening section establishes why incident response and forensics matter. The course introduction notes that the module teaches students how to **prepare for, detect, respond to and recover from cybersecurity incidents**. It situates these skills within established standards, highlights the role of CSIRTs, and stresses that practical exercises help learners develop competence in handling incidents and conducting digital forensics investigations. Key objectives include distinguishing routine events from incidents, understanding classification terminology and appreciating the need for timely and appropriate response.

Understanding incidents

Lesson 1 begins by defining a **cybersecurity incident**. Students examine the difference between an **event** (any observable occurrence) and an **incident** (a violation or imminent threat to policies) using NIST's definitions. The lesson emphasises that not every log entry or unusual behaviour constitutes an incident; indicators must be analysed before escalation. A narrative scenario places learners within a SOC where unusual outbound traffic is detected on a payment server. Management asks whether this constitutes an event, incident or breach, why timely response matters and what immediate steps should be taken. Such scenarios encourage reflection on the severity of flagged activities and reinforce that classification affects containment, investigation and disclosure obligations.

Standards and frameworks

The module draws on international standards. Students read sections of the **NIST Computer Security Incident Handling Guide (SP 800-61)** to understand formal definitions and the importance of monitoring. They also study the introduction to **ISO/IEC 27035**, which outlines the incident management lifecycle (preparation, detection, analysis, response and recovery) and stresses the need for timely escalation and documentation. A video highlights how quickly minor events can become incidents if not properly handled, and a concept test asks learners to distinguish between an event (e.g., user plugging in a USB drive) and a true incident (e.g., malware executing on a server).

Section reflections

Throughout Section 1, learners are reminded that effective incident response begins with **precise terminology and process discipline**. Understanding the differences between alerts, events and incidents informs the appropriate response and ensures that legal obligations are met. Using internationally recognised guidance such as NIST SP 800-61 and ISO/IEC 27035 anchors practices in accepted standards and facilitates alignment across organisations.

2.8.2 Section 2: Identifying Cybersecurity Related Issues

- ☑ **Section 2: Identifying Cybersecurity-Related Issues**
 - ☑ Introduction
 - ☑ Lesson 1: Common Cyber Threats
 - ☑ Lesson 2: Detection Methods & Network Defense Mechanisms
 - ☑ Lesson 3: Non-Cyber Events Impacting Cybersecurity
 - ☑ Concept Test

Figure 41 LM8 Section 2 on Open edX

The second section extends incident classification into the wider threat landscape. Its introduction states that learners will **recognise common categories of cyber threats**, explain detection tools and indicators of compromise (IoCs), and analyse how non-cyber events and human factors affect cybersecurity. Learners use an accompanying presentation for structured learning and then explore narrative scenarios and concept tests.

Lesson 1: Common cyber threats

Lesson 1 introduces major threat categories. A narrative scenario involves a junior SOC analyst facing suspicious emails, intermittent website slow-downs and IDS alerts; management asks whether these events are related and how to prioritise them. The lesson covers definitions and characteristics of **malware, phishing, distributed**

denial-of-service (DDoS) attacks and **insider threats**, exploring how attackers combine vectors to create blended attacks. A video highlights the behaviours of malware and phishing campaigns and explains how DDoS attacks overwhelm services. Learners then study an in-depth article on **threat actors and motives**. The article explains that **cyber-criminals** pursue financial gain, **nation-state actors** engage in espionage and disruption, **hacktivists** pursue social or political goals, **thrill-seekers** hack for fun, **insider threats** exploit access from within, and **cyber-terrorists** use digital attacks to spread fear. It also surveys attacker tactics such as ransomware, phishing and DDoS, and recommends defences: security awareness training, multifactor authentication, endpoint security and regular assessments. Through these readings learners grasp how diverse actors operate and how multi-layered controls help mitigate them.

Lesson 2: Detection methods and network defence mechanisms

Lesson 2 focuses on detection workflows. The introduction describes a scenario where multiple failed logins followed by a successful login from an unfamiliar IP address are observed; the workstation then connects to a strange domain. Learners are asked which monitoring sources (SIEM, endpoint logs, firewalls) and IoCs to examine, and what steps to take to verify or contain the incident. The lesson explains the roles of **system, application, network and authentication logs**, defines **indicators of compromise** (e.g., suspicious hashes, unexpected outbound connections), and shows how threat-intelligence feeds enrich IoCs. An article comparing **Security Information and Event Management (SIEM) systems** with **Intrusion Detection Systems (IDS)** notes that SIEMs aggregate, correlate and analyse logs for anomalies, often using machine learning; IDS monitor network traffic in real time but do not prevent intrusions. The article stresses that modern security operations use both to achieve comprehensive visibility and that next-generation SIEMs integrate with SOAR platforms and EDR solutions.

Lesson 3: Non-cyber events and human factors

Lesson 3 examines how **physical events and human vulnerabilities** influence cybersecurity. The introduction explains that natural disasters, utility failures and human manipulation can expose systems to compromise. A scenario describes a logistics company hit by a severe storm that causes a power outage; amid the confusion an employee receives a phone call from someone claiming to be IT support and divulges credentials. Learners are asked how physical disruptions increase vulnerability and why stressed employees are susceptible. An article on **physical security risks** lists examples such as vehicle ramming attacks on buildings and emphasises the need for emergency plans, perimeter security and scenario planning. It also notes that cyber-physical risks are rising and that incidents like the 2024 Change Healthcare ransomware attack illustrate how cyber risk can spill into critical infrastructure. A follow-up page explains that **social engineering** succeeds because it exploits psychology and uses pretexting and persuasion; videos demonstrate typical techniques. A concept test asks which statement best characterises a DDoS attack; the correct answer is that it overwhelms a system with massive traffic from many sources. These pages underscore the interplay between technical and human aspects of security.

Section summary

Section 2 exposes learners to the complexity of modern threat landscapes. By exploring both technical threats and non-technical factors, the module emphasises that successful incident response requires not only

monitoring and detection tools but also awareness of human behaviour and physical contingencies. Real-world examples of nation-state espionage, ransomware attacks and physical attacks on facilities illustrate the breadth of risks and the importance of layered defence.

2.8.3 Section 3: Incident Handling Standards, Methodologies and Frameworks

- ✓ **SECTION 3: Incident Handling Standards, Methodologies, and Frameworks**
 - ✓ Introduction
 - ✓ Lesson 1: The Incident Handling Lifecycle
 - ✓ Lesson 2: Standards and Frameworks
 - ✓ Lesson 3: Best Practices
 - ✓ Concept Test

Figure 42 LM8 Section 3 on Open edX

Section 3 moves from threat identification to structured incident handling. The introduction states that students will describe the phases of the incident handling lifecycle, explain how international standards support response operations, highlight the role of preparation and planning, and evaluate response workflows. The section includes three lessons: the incident handling lifecycle, standards and frameworks, and best practices.

Lesson 1: The incident handling lifecycle

Lesson 1 presents a **structured lifecycle** that guides response activities from readiness through restoration. Its introduction emphasises that detecting an incident is only the first step; a structured lifecycle ensures that subsequent actions are coordinated and documented. A scenario features a financial reporting organisation where auditors detect unexpected modifications to logs; learners must decide which immediate activities to prioritise, what information is needed to assess impact and how restoration differs from containment. The lesson instructs students to watch the video *Incident Response Lifecycle Explained* and read an article on incident management for high-velocity teams. The article notes that incident management is cyclical—not linear—and includes steps such as detection, setting up communication channels, assessing severity, communicating with customers, escalating to the right responders, delegating roles and resolving incidents. Preparation activities (defining roles, building contact lists, practising escalation) are highlighted as critical to efficiency. A subsequent task directs learners to read guidance on planning and executing incident response actions. The guidance emphasises detailed sequencing—preparation, detection, analysis, containment, eradication, recovery and lessons learned—and notes benefits such as mitigating impact, enabling good decisions under pressure, building trust through clear communication and using lessons learned to improve capabilities. Another task introduces a CISA cybersecurity incident response playbook video that illustrates a high-level flow-chart of steps and emphasises differences between phases. Finally, a scenario-based question asks which response activities should be prioritised once the lifecycle is activated.

Lesson 2: Standards and frameworks

Lesson 2 examines internationally recognised frameworks. The introduction notes that organisations often adopt **ISO/IEC 27035** and **NIST SP 800-61** to establish repeatable processes and ensure compliance. A scenario describes a cross-department file-sharing environment with unauthorised edits; management asks how to respond using a standards-based approach. Learners watch two videos on interpreting ISO/IEC 27035 and NIST SP 800-61, and then read a comparative article. The article explains that ISO/IEC 27035 uses a **two-tier assessment approach**: a point of contact performs an initial event assessment following standard procedures to determine whether the event is an incident; the **incident response team (IRT)** re-assesses the event, prioritises and plans activities, assigns actions, logs all steps, and gathers electronic evidence to ensure that false positives are eliminated and response is proportional. This structured process reduces false alarms, encourages documentation, and ensures that evidence is preserved for potential legal proceedings.

Lesson 3: Best practices

Lesson 3 focuses on developing and testing incident response plans (IRPs). The introduction presents a scenario where a security review reveals inconsistent incident reporting across departments; management asks which IRP component requires improvement, why cross-departmental consistency matters, how to verify adherence and how to address communication channels. The lesson discusses core elements of an IRP—defined roles and responsibilities, procedural steps for each phase, communication paths, escalation criteria, evidence preservation requirements and post-incident reviews. It underscores the importance of **tabletop exercises** and **after-action reviews** to test and refine plans. Videos and reading materials instruct learners on developing IRPs tailored to organisational contexts and ensuring that procedures remain effective as technology and threat landscapes evolve.

Section analysis

Section 3 stresses that effective incident response requires **formal processes grounded in standards**. By studying ISO/IEC 27035, NIST SP 800-61 and other frameworks, students learn to align their organisation's procedures with global best practices. Scenario-based questions reinforce that preparedness, documentation and continuous improvement are indispensable when facing incidents of varying complexity.

2.8.4 Section 4 - Operation of Computer Security Incident Response Teams (CSIRTs)

✓ SECTION 4: Operation of Computer Security Incident Response Teams (CSIRTs)

- ✓ Introduction
- ✓ Lesson 1: CSIRT Roles, Responsibilities, and Organizational Models
- ✓ Lesson 2: Coordination with External Entities
- ✓ Concept Test

Figure 43 LM8 Section 4 on Open edX

Section 4 shifts focus to the organisational structures that deliver response capabilities. Its introduction states that learners will **identify core CSIRT roles and responsibilities**, compare centralised, distributed and coordinated models, explain the importance of collaboration with law enforcement and peer CSIRTs, assess how organisational structure influences communication and decision-making, and recognise the value of external coordination.

Lesson 1: CSIRT roles, responsibilities and organisational models

Lesson 1 opens with a scenario where an international organisation wants to establish a CSIRT across three regions; leadership is unsure how to structure the team. Management asks which skills and roles are essential, how responsibilities like triage, forensics and communication align across structures, and how centralisation versus distribution affects response time and visibility. The lesson introduces **key CSIRT roles**—incident handlers, forensic analysts, threat intelligence analysts, communications coordinators and management liaisons—and describes required **technical and non-technical skills** (malware analysis, network forensics, case management, teamwork and clear communication). Students examine **organisational models**. A **centralised CSIRT** offers strong coordination and consistent processes but may struggle with regional nuances; a **distributed CSIRT** places response capability close to business units but may suffer from inconsistent practices; a **co-ordinated model** combines elements of both. Learners discuss the strengths and weaknesses of each relative to organisation size, geography and risk appetite.

Defining CSIRTs and responsibilities

A detailed article defines a **CSIRT** as a team providing services and support for the assessment, management and prevention of cybersecurity incidents. Its goals include responding quickly and efficiently to incidents and helping organisations improve resilience. The article outlines the **NIST incident handling phases**—preparation, detection and analysis, containment/eradication/recovery, and post-incident activity—and associates CSIRT responsibilities with each. These responsibilities include creating and updating IRPs, maintaining communication with internal and external stakeholders, identifying and analysing incidents, coordinating response efforts, remediating incidents, reporting, managing audits, and reviewing policies to recommend changes. It emphasises that a CSIRT must have a defined mission, structure and roles, and references the **Forum of Incident Response and Security Teams (FIRST)** framework, which describes service areas such as event management and vulnerability management. Another task requires learners to read a document on CSIRT staffing, highlighting that staff composition depends on mission, services, available expertise, constituency size, anticipated incident load and budget; teams may have core members for fundamental services and specialists for deep analysis and training.

Lesson 2: Coordination with external entities

Although we could not fully explore Lesson 2, its objectives suggest that learners examine **coordination with external entities**, including national CERTs, law enforcement, peer CSIRTs and industry bodies. Effective collaboration ensures timely information sharing, helps contain large-scale incidents and supports legal investigations.

Section synthesis

Section 4 underscores that incident response is a **team sport**. Building an effective CSIRT requires careful consideration of roles, structures and skill sets. Integrating with external networks enhances situational awareness and ensures that incident response efforts contribute to broader cybersecurity ecosystems.

2.8.5 Section 5: Conducting Technical Analysis and Reporting

✔ Section 5: Conducting Technical Analysis and Reporting

- ✔ Introduction
- ✔ Lesson 1: Technical Analysis Techniques
- ✔ Lesson 2: Reporting Procedures
- ✔ Concept Test

Figure 44 LM8 Section 5 on Open edX

This section, not fully explored due to time constraints, aims to train learners in the **technical investigation of incidents** and the development of clear reports for technical and non-technical audiences. The section likely covers memory and disk forensics, network traffic analysis, malware analysis, documentation of findings, and communicating results in a structured incident report. Lessons may emphasise the importance of capturing volatile evidence, reconstructing timelines, using specialised forensic tools and producing documentation that supports remediation and legal proceedings.

2.8.6 Section 6: Criminal Investigation Procedures in Cybersecurity

✔ SECTION 6: Criminal Investigation Procedures in Cybersecurity

- ✔ Introduction
- ✔ Lesson 1: Legal Considerations & Evidence Preservation
- ✔ Concept Test

Figure 45 LM8 Section 6 on Open edX

Section 6 introduces the **legal and investigative aspects** of cyber incidents. The course outline indicates that learners will study **legal considerations, evidence preservation and chain of custody**, and evaluate how criminal procedures govern the collection and analysis of digital evidence. Although the detailed lessons were not explored, typical topics would include understanding relevant laws and regulations (e.g., data protection, computer misuse), working with law enforcement agencies, maintaining a documented chain of custody for

evidence, and recognising the role of cyber forensics in supporting prosecutions. A concept test may assess knowledge of evidence handling and legal thresholds.

2.8.7 Section 7: Digital Forensics Best Practices

- ✓ **SECTION 7: Digital Forensics Best Practices**
 - ✓ Introduction
 - ✓ Lesson 1: Introduction to Digital Forensics
 - ✓ Lesson 2: Forensic Process
 - ✓ Lesson 3: Tools and Techniques
 - ✓ Concept Test

Figure 46 LM8 Section 7 on Open edX

This section focuses on **digital forensic techniques** for identifying, acquiring, preserving, analysing and presenting digital evidence. Learners are likely to explore the stages of a forensic investigation, including planning, evidence collection (disk images, memory captures, network logs), examination (file system analysis, malware dissection), analysis (timeline reconstruction, correlation), and reporting. Best practices emphasise maintaining integrity of evidence (hashing, write-blocking), using validated tools, documenting procedures, and understanding admissibility requirements. Links to widely used frameworks—such as the **Digital Forensic Process Model**—and case examples would illustrate these principles. A concept test could evaluate understanding of evidence preservation, forensic tool capabilities and common pitfalls.

2.8.8 Section 8: Review and Assessment

- ✓ **SECTION 8: Review and Assessment**
 - ✓ Review and Assessment (22 Questions)
Final Review & Assessment

Figure 47 LM8 Section 8 on Open edX

The final section provides a **comprehensive assessment** covering topics across the module. It likely includes multiple-choice questions and scenario-based exercises that ask learners to apply knowledge of incident classification, threat identification, detection workflows, incident handling processes, CSIRT operations, forensics and legal considerations. The assessment ensures that students understand the theoretical foundations and can apply them in realistic contexts.

2.8.9 Section 9: Practical Exercises and Case Studies

✔ Section 9: Practical Exercises and Case Studies

✔ Practical Exercises and Case Studies

Figure 48 LM8 Section 9 on Open edX

The last instructional section offers an **applied capstone** for the module. Rather than introducing new theory, Section 9 presents a set of **practical exercises and case studies** designed to consolidate the knowledge gained throughout the course. The guidance page explains that these exercises simulate realistic incidents in a financial-sector environment and emphasise **manual incident response processes, cross-team coordination, threat analysis and secure recovery**. Learners are provided with a downloadable guide that outlines five distinct scenarios, each aligned with roles in the European Cybersecurity Skills Framework. The roles include **SOC analyst, incident responder, cyber-threat intelligence analyst, penetration tester** and **incident response coordinator**, allowing participants to experience different perspectives during an incident.

According to the module's description, the exercises require learners to solve problems under constrained conditions, make decisions about escalation and communication, and perform hands-on analysis without relying on automated workflows. By working through these cases, students practise investigating suspicious activity, coordinating with team members, analysing threats and implementing recovery strategies. The tasks build on earlier sections by requiring participants to apply standards-based processes (ISO/IEC 27035, NIST SP 800-61), use threat-identification techniques and evidence-preservation practices, and develop concise reports for different stakeholders. The exercises also feed into broader NG-SOC research objectives by providing data for piloting and evaluation phases. Overall, Section 9 transforms the theoretical and procedural knowledge from the module into **experiential learning** that prepares learners for real-world incident response and forensic investigations.

2.8.10 Conclusion

Learning Module 8 provides an in-depth exploration of incident response and forensics. Beginning with foundational definitions and standards, it guides learners through the spectrum of threats, detection techniques, incident handling frameworks, organisational structures and investigative procedures. Scenario-based activities and concept tests emphasise application and critical thinking. By integrating technical knowledge with procedural and organisational considerations, the module prepares students to respond to cybersecurity incidents effectively, coordinate teams, navigate legal requirements and conduct thorough forensic analyses. The emphasis on internationally recognised standards such as NIST SP 800-61 and ISO/IEC 27035, as well as frameworks like FIRST for CSIRTs, ensures that learners can align their practices with globally accepted best practices. Overall, the module underscores that incident response is not simply about technical expertise but requires preparation, coordination, communication and continuous improvement across people, processes and technology.

2.9 LM9: Collaboration and Communication

Table 11 LM9 Extraction

Competence Level: Basic / Intermediate	
This module emphasizes the importance of effective communication, teamwork, and interdisciplinary collaboration in cybersecurity contexts. It covers strategies for clear stakeholder communication, evidence-based decision-making, and the development of cybersecurity awareness programs. By integrating soft skills with technical competencies, learners will be prepared to navigate complex organizational environments, engage diverse teams, and foster a culture of cybersecurity readiness.	
Subject contents and topics	Learning outcomes (competences)
> Roles and responsibilities within cybersecurity teams > Strategies for improving coordination in incident response and security operations > Identifying and addressing the communication needs of different stakeholders (executives, technical teams, end-users) > Writing clear and concise security reports and documentation > Presenting cybersecurity risks and mitigation strategies effectively > Crisis communication and handling security incidents transparently > Implementing systematic approaches for risk assessment and threat management > Utilizing data and analytics to support cybersecurity policies and strategies > Designing cybersecurity training and awareness initiatives > Measuring the impact of awareness programs and improving security culture > The role of policy, regulation, and compliance in cybersecurity collaboration > Review and Assessment	The student is able to - Develop effective communication strategies tailored to various stakeholders and organizational levels. - Enhance teamwork, problem-solving, and interpersonal skills for collaboration in cybersecurity operations and projects. - Implement systematic, evidence-based work practices to inform decision-making and improve cybersecurity outcomes. - Design and deliver cybersecurity awareness programs that promote a positive security culture. - Recognize and navigate the multidisciplinary aspects of cybersecurity to engage diverse expertise and perspectives.
	Mapping with ENISA ECSF
	Cyber Legal, Policy & Compliance Officer, Cybersecurity Risk Manager,

Cybersecurity Architect, Cybersecurity Educator.

Link to Open edX: <https://apps.ngsoc-training-platform.eurodyn.com/learning/course/course-v1:NG-SOC+LM9+2025Q1/home>

Learning Module 9 focuses on the strategic importance of collaboration and communication within cybersecurity operations. Rather than viewing security as a solely technical discipline, the module emphasises that poor communication is responsible for the majority of cyber-security failures. The module progresses through nine sections, illustrating how effective communication and collaboration underpin organisational resilience, from governance and stakeholder messaging to incident response, evidence-based decision-making and awareness programmes. It equips professionals with frameworks, matrices and case studies to transform technical findings into compelling business narratives and to coordinate cross-functional teams.

2.9.1 Section 1: Introduction to Cybersecurity Communication

- ✓ **Section 1: INTRODUCTION TO CYBERSECURITY COMMUNICATION (EXPANDED)**
 - ✓ Lesson 1: Introduction to Cybersecurity Communication (Expanded) 3 min
 - ✓ Section 1 Concept Test (5 Questions) 1 activity
Section Concept Tests

Figure 49 LM9 Section 1 on Open edX

The opening section identifies a communication crisis: roughly 75 % of cyber-security failures stem from communication breakdowns rather than technical flaws. Technical failures (e.g., unpatched systems, misconfigured firewalls) can be remedied with technology, but communication failures (ignoring risk warnings, failing to coordinate during incidents or neglecting user awareness) often undermine otherwise sound security controls. The section lists typical failure examples and explains why communication dominates cyber-security success: executives control budgets yet often do not understand technical risks, employees implement controls yet need clear guidance, incidents require coordination across many teams, regulators demand rapid evidence and customers judge organisations based on crisis communication. Four common communication failure modes are analysed: jargon overload, siloed reporting, employee resistance and regulatory communication gaps. Solutions include translating technical issues into business impact, notifying all stakeholders simultaneously and offering empathetic value propositions to employees.

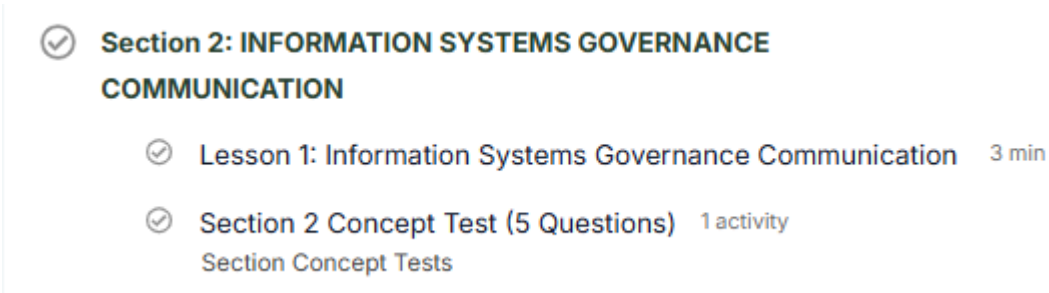
The section introduces the ENISA European Cybersecurity Skills Framework (ECSF) roles and their communication demands. A Cyber Legal Officer must manage regulatory notifications (e.g., NIS2 24-hour and GDPR 72-hour deadlines), oversee policy roll-out and present audit evidence. The Cybersecurity Risk Manager spends about 60 % of their time translating risk metrics into business impact for executives and boards, presenting investment

cases and incident impact reports. The Cybersecurity Architect allocates half of their time to translating technical requirements into business requirements and briefing executives on architecture trade-offs. The Cybersecurity Educator largely communicates through awareness programmes and behaviour metrics dashboards.

To address communication deficiencies, the section proposes the 5C Communication Mastery Framework. This model consists of:

- **Collaborate** - establishing team alignment with defined roles, cadences, shared language and mutual respect. Without clear collaboration protocols, security teams drift into siloed behaviour.
- **Communicate** - mastering stakeholder-specific messaging. Boards need risk dashboards; executives require return-on-investment (ROI) calculations; business units need operational impact; technical teams need actionable instructions; employees require simple behaviour guidance; and regulators require compliance evidence.
- **Coordinate** - implementing systematic processes such as incident response protocols, daily stand-ups, cross-functional forums and evidence-based decision registers.
- **Create** - building awareness programmes through onboarding training, campaigns and role-specific education with measurement and continuous improvement.
- **Connect** - promoting multidisciplinary leadership linking legal, finance, human resources (HR), public relations (PR), operations and executives to align evidence collection, investment justification and culture transformation

2.9.2 Section 2: Information Systems Governance Communication



✓ **Section 2: INFORMATION SYSTEMS GOVERNANCE COMMUNICATION**

- ✓ Lesson 1: Information Systems Governance Communication 3 min
- ✓ Section 2 Concept Test (5 Questions) 1 activity
- Section Concept Tests

Figure 50 LM9 Section 2 on Open edX

Section 2 focuses on communication within governance structures. The **Three Lines Model** communication flows highlight that the first line (business units) implements controls and reports daily on suspicious activities and metrics; the second line (risk/compliance) provides oversight with monthly executive reports and quarterly audit preparation; and the third line (internal audit) delivers quarterly board updates and annual reports on control effectiveness. Each line's communications have specific frequencies and metrics to avoid gaps.

A **Governance Role Communication Protocols** framework provides templates for dashboards and briefings. It shows how a cybersecurity executive dashboard can summarise risk status (e.g., amber risk due to elevated incidents), incident counts, compliance scores, budget utilisation and decisions needed (e.g., approval of a \$200 000 endpoint detection and response (EDR) upgrade). Monthly executive briefings report on incident

statistics, project progress (e.g., MFA rollout, SIEM deployment), key metrics (mean time to detect (MTTD), phishing click rates) and investment requests. Daily security stand-ups provide real-time updates on alerts, urgent tasks, blockers and upcoming activities. These structured communications ensure the right people receive the right information at the right time.

The **Policy Communication Master Framework** demonstrates how to roll out a new multi-factor authentication (MFA) policy. A six-week plan begins with an executive announcement and department briefings, proceeds to role-specific training, technical testing and helpdesk support, then enforces compliance (system lock without MFA) and finally sustains reinforcement through monthly dashboards and success stories. A RACI (Responsible, Accountable, Consulted, Informed) matrix clarifies responsibilities for each stage of the policy rollout.

2.9.3 Section 3: Stakeholder Communication Mastery

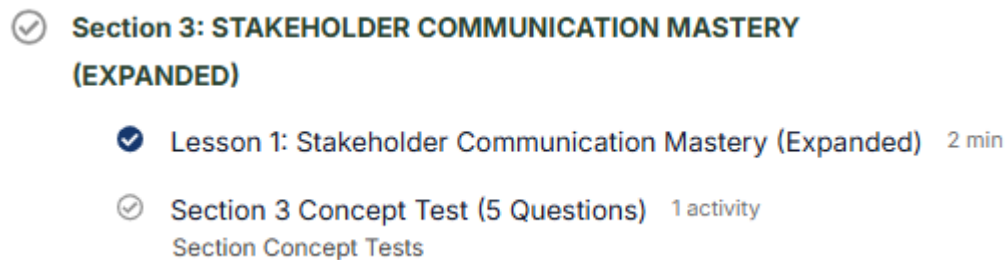


Figure 51 LM9 Section 3 on Open edX

This section develops tools for tailoring messages to stakeholders. A **Complete Stakeholder Communication Matrix** maps each stakeholder group to their concerns, ideal communication format, frequency and metrics. For example, the board focuses on risk and reputation; they receive one-page dashboards quarterly and success is measured by decisions influenced. CEOs/CFOs care about budget and business impact, receiving executive summaries monthly; business units need monthly briefings with Q&A; technical teams rely on daily stand-ups; employees receive continuous campaigns; regulators get formal reports as required; customers are contacted only during incidents; and vendors receive updates during project phases.

The **Message Translation Mastery Framework** teaches how to convert technical jargon into business language. A high-risk vulnerability (e.g., “SQL injection CVE-2026-1234”) should be translated into a business impact (“attackers could steal customer data”) and then quantified (£10 M fine, 20 % customer loss). MFA implementation can be framed as preventing 99 % of account compromises, with a 30-fold ROI compared with breach costs. The framework provides reverse translations where executive directives (“security budget must show ROI”) are broken down into technical tasks (building three-year financial models, dashboards, board presentations). Such translations ensure alignment between leadership and technical teams.

The **Communication Channel Optimisation Matrix** recommends primary and backup channels for different purposes: urgent issues use phone or Slack with email backup; strategic updates use dashboards and executive briefings with version control; operational issues use stand-ups and project tools; awareness campaigns use email and intranet, measured by open/click rates; training uses learning management systems or workshops;

regulatory communications use certified mail or portals to provide an audit trail; customer updates rely on the website and hotline; and project communication uses tools like Jira and Slack. A decision tree helps choose channels based on urgency, need for audit evidence and audience technical level.

2.9.4 Section 4: Teamwork and Collaboration in Cybersecurity Operations

- ✓ **Section 4: TEAMWORK AND COLLABORATION IN CYBERSECURITY OPERATIONS (EXPANDED)**
 - ✓ **Lesson 1: Teamwork and Collaboration in Cybersecurity Operations (Expanded)** 3 min
 - ✓ **Section 4 Concept Test (5 Questions)** 1 activity
Section Concept Tests

Figure 52 LM9 Section 4 on Open edX

Section 4 examines **team structures and collaboration mechanisms**. A **cybersecurity team structure** table defines roles. The SOC Lead coordinates threat detection, team huddles and executive reports. SOC Analysts triage alerts and perform shift handovers; Security Engineers deploy controls; Incident Responders handle containment and recovery; Threat Hunters conduct proactive hunting; and a Compliance Officer manages audit readiness. A supporting teams matrix lists IT operations (system uptime, patch schedules), developers (secure coding), business owners, legal, HR and compliance. Clear responsibilities and escalation paths minimise confusion during incidents.

The **Incident Response Communication Playbook** describes a six-phase timeline: detection (0-15 min), notification (15-60 min), assessment (1-4 hrs), containment (4-24 hrs), eradication/recovery (Day 2-7) and lessons learned (Week 2). During the early minutes, SOC analysts triage and notify the SOC lead; the incident commander informs the CISO; the CISO updates executives and legal; and communications prepare a holding statement. Escalation matrices specify when to notify executives, regulators, customers and the board depending on severity. Such playbooks ensure that communication keeps pace with technical response and regulatory obligations.

A **Daily/Weekly Team Collaboration Cadence** prescribes short morning huddles, weekly cross-functional forums and monthly executive reviews. The huddle covers overnight incidents, priorities, blockers and metrics (e.g., alerts, MTTD). The weekly forum brings security, IT, legal, business and compliance together to review major incidents, project security gates and metrics trends. Shift handover templates document active incidents, open vulnerabilities, scheduled tasks and metrics to maintain continuity across shifts.

2.9.5 Section 5: Systematic, Evidence-Based Decision-Making

✓ Section 5: SYSTEMATIC, EVIDENCE-BASED DECISION MAKING (EXPANDED)

- ✓ Lesson 1: Systematic, Evidence-Based Decision Making (Expanded) 2 min
- ✓ Section 5 Concept Test (5 Questions) 1 activity
Section Concept Tests

Figure 53 LM9 Section 5 on Open edX

Cyber-security decisions must be grounded in evidence, not anecdotes. The **Evidence Hierarchy** ranks sources from least to most valuable: anecdotes/opinion at the bottom, vendor claims (to be verified), industry benchmarks (e.g., Gartner or Verizon reports), peer-reviewed studies (academic research demonstrating MFA effectiveness or zero-trust benefits) and, at the top, an organisation's own data (incident history, control effectiveness, employee behaviour). Professionals are encouraged to prioritise higher-level evidence whenever possible.

A **Five-Step Decision Framework** provides templates for evidence-based decision-making: 1) define the problem precisely; 2) gather evidence from at least three sources (internal data, industry data, vendor proof of concept); 3) quantify alternatives by estimating cost and risk reduction; 4) document and communicate the decision, including ROI calculations and success metrics; 5) monitor results and adjust accordingly. For example, deciding whether to deploy an internal EDR solution or outsource to a managed service provider involves comparing expected risk reduction and investment to determine the best ROI. Documenting the rationale ensures transparency and facilitates board approval.

A forthcoming subpage (not visited during the summary) included an **essential metrics dashboard** for live tracking; typical metrics might include MTTD, mean time to respond (MTTR), phishing click rates, patch compliance and training completion rates. By continuously monitoring these metrics, organisations can make informed adjustments and demonstrate ROI to leadership.

2.9.6 Section 6: Comprehensive Awareness Programme Architecture

✓ Section 6: COMPREHENSIVE AWARENESS PROGRAMME ARCHITECTURE (EXPANDED)

- ✓ Lesson 1: Comprehensive Awareness Programme Architecture (Expanded) 2 min
- ✓ Section 6 Concept Test (5 Questions) 1 activity
Section Concept Tests

Figure 54 LM9 Section 6 on Open edX

Section 6 provides a 12-month awareness roadmap. Each quarter addresses a thematic focus:

- **Q1 - Phishing mastery:** baseline phishing test, training on recognition, simulated phishing campaign and feedback, plus targeted micro-trainings.
- **Q2 - Identity protection:** password hygiene assessment, passphrase training, MFA rollout support, compliance campaign and continuous weak password alerts.
- **Q3 - Physical & social:** physical security assessment, social engineering training (vishing/pretexting), clean desk campaign and USB drop test.
- **Q4 - Data protection:** data classification training, DLP policy rollout, public Wi-Fi & VPN training and year-end certification.

A **Role-Specific Training Content** library tailors training to different functions. Executives receive 30-minute briefings on ransomware cost, board reporting and investment decisions. Finance teams learn about payment fraud patterns, wire transfer verification and macro malware. Developers undertake 90-minute sessions on secure coding, dependency scanning, secrets management and vulnerability disclosure. HR teams learn about PII protection, off-boarding security and secure recruitment. A campaign library includes phishing simulations (e.g., CEO fraud) and password hygiene materials that demonstrate good passphrases and advocate the use of password managers.

The **Success Measurement Framework** assigns weightings to performance indicators: behavioural metrics (70 %) such as phishing click rate (<5 %), phishing report rate (>50 %), reduced helpdesk calls and high MFA adoption; training metrics (20 %) such as completion and pass rates; and business metrics (10 %) like reduction in human-error incidents and improved security culture survey scores. This weighting underscores that behaviour change, not mere completion of training, determines success.

2.9.7 Section 7: Multidisciplinary Team Leadership

Section 7: MULTIDISCIPLINARY TEAM LEADERSHIP (EXPANDED)

 **Lesson 1: Multidisciplinary Team Leadership (Expanded)** 3 min

 **Section 7 Concept Test (5 Questions)** 1 activity
 Section Concept Tests

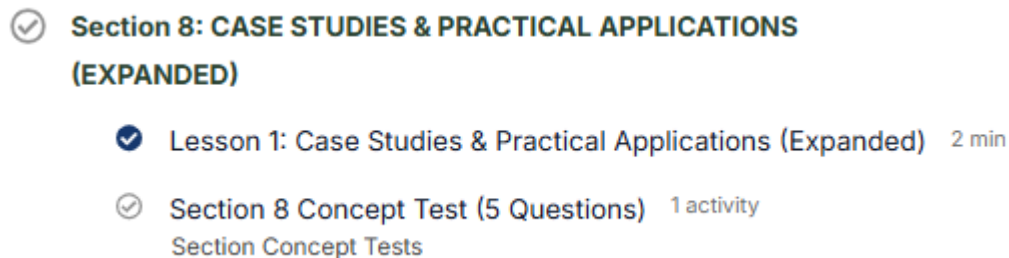
Figure 55 LM9 Section 7 on Open edX

Cyber-security requires input from a range of disciplines. A **Discipline Integration Matrix** defines how legal, finance, HR, PR, operations, compliance and business functions contribute to security, the topics they discuss and their collaboration frequency. For example, legal provides liability protection and manages notification deadlines; finance allocates budgets and calculates ROI; HR enforces policies and oversees training compliance; PR manages reputation and crisis communications; operations ensures process continuity; compliance addresses audit readiness; and business leaders evaluate risk tolerance and impact.

Section 7 introduces cross-functional forums and governance. A **Weekly Security Council** (Thursday, 10:00) convenes up to ten stakeholders (CISO, IT Director, legal counsel, compliance officer, business leads, security lead, HR and finance). Agenda items include incident reviews, project security gates (e.g., passing or failing architecture reviews), compliance status and metrics such as phishing click rates and MTDD. A **RACI matrix** details who is responsible, accountable, consulted and informed for each decision, ranging from strategy and budget approval to incident response, policy approval, vendor selection and audit findings. Clear accountability prevents decisions from stalling.

The **Collaboration Success Factors** page lists four actionable factors: establishing a shared language that translates technical to business concepts; maintaining regular cadences (daily coordination, weekly cross-functional alignment, monthly executive updates and quarterly strategic roadmaps); enforcing escalations within 48 hours (from issue owners up to executives); and celebrating joint wins (e.g., recognition when security and developers identify a zero-day vulnerability saving the company millions). This fosters trust and reinforces positive behaviour.

2.9.8 Section 8: Case Studies & Practical Applications



✓ **Section 8: CASE STUDIES & PRACTICAL APPLICATIONS (EXPANDED)**

- ✓ Lesson 1: Case Studies & Practical Applications (Expanded) 2 min
- ✓ Section 8 Concept Test (5 Questions) 1 activity
Section Concept Tests

Figure 56 LM9 Section 8 on Open edX

Practical case studies illustrate how communication makes or breaks cyber-security outcomes:

1. **Phishing Communication Failure:** A retailer with 8 000 employees experienced a phishing campaign. Although technical controls blocked 97 % of phishing emails, communications faltered: security alerted business units without explaining financial impact, business units failed to prioritise, employees ignored technical instructions and executives questioned training ROI. Consequently 28 % of employees clicked (2 240 accounts compromised), causing \$1.2 M in fraud and reputational damage. Lessons: always translate risk to dollar impact, instruct employees to forward suspicious emails, quantify training ROI (e.g., \$1.2 M avoided for \$50 k investment) and continuously measure and report progress.
2. **Ransomware Communication Success:** A manufacturing firm detected ransomware encrypting five production servers. Within minutes the SOC updated the CISO with business impact; the CISO informed executives; executives reassured employees; legal notified regulators; and communications reassured stakeholders. The event resulted in only four hours of downtime (\$50 k cost) and no customer impact. Rapid escalation, tiered messaging and proactive regulator engagement reduced losses and improved executive confidence (leading to a 35 % budget increase).

3. **Awareness ROI Transformation:** A financial services firm had baseline metrics of 32 % phishing clicks, 185 helpdesk calls and 28 incidents per month. After launching monthly phishing simulations, executive video messages linking security to bonuses, role-specific training and positive incentives (e.g., vouchers), phishing clicks fell to 2.8 %, helpdesk calls to 38/week and incidents to seven per month. Executives estimated \$2.1 M savings for a \$180 k investment. Key communication elements: publicised baseline metrics, monthly progress dashboards, executive testimonials and supportive individual feedback.

These case studies demonstrate that **effective communication aligns stakeholders around risk and ROI** and that poor communication negates technical controls.

2.9.9 Section 9: Mastery Assessment & Professional Roadmap

- ✓ **Section 9: MASTERY ASSESSMENT & PROFESSIONAL ROADMAP (FINAL)**
 - ✓ Lesson 1: Mastery Assessment & Professional Roadmap (Final) 1 min

Figure 57 LM9 Section 9 on Open edX

The final section prepares learners to apply the module's frameworks in their careers. A **5C Framework Mastery Checklist** summarises achievements: collaborating via RACI matrices and weekly forums, communicating tailored messages for five stakeholder groups, coordinating incident timelines and evidence-based decisions, creating a 12-month awareness roadmap and connecting disciplines such as legal, finance, HR and PR. It notes ENISA ECSF competences gained for each role.

A **Professional Communication Roadmap** suggests 90-day milestones: in weeks 1-2 practise stakeholder translations, document a team RACI matrix and build personal incident communication templates; in weeks 3-6 propose a weekly security forum, launch a phishing simulation and develop an executive dashboard; in weeks 7-12 present an ROI case to management, lead a cross-functional security review and measure training results. A **Self-Assessment Scorecard** encourages learners to evaluate their proficiency across communication, collaboration, evidence, awareness and regulatory compliance, scoring themselves from 1 (foundational) to 5 (ENISA-ready).

2.9.10 Final Review & Assessment

- ✓ **FINAL REVIEW & ASSESSMENT**
 - ✓ Final Review & Assessment (20 Questions) 1 activity
 - Final Review & Assessment

Figure 58 LM9 Final Review & Assessment on Open edX

To consolidate learning, the module finishes with a **Final Review & Assessment**. Students complete a 20-question multiple-choice test that revisits every major framework introduced. Example items require identifying which quarter of the awareness roadmap addresses password hygiene, mapping responsibilities in a Three Lines Model scenario, selecting the correct RACI role for approving a security policy, matching case study lessons to communication principles, and interpreting metrics such as mean time to detect or phishing click rate. Other questions probe the 5C framework, translation techniques and communication channel choices. The assessment ensures that learners can apply knowledge across varied contexts - from board communication to incident response - and serves as a summative check of collaboration and communication mastery.

2.9.11 Conclusion

Learning Module 9 underscores that **cyber-security is fundamentally a people and communication challenge**. Technical controls and frameworks are necessary, but they fail without clear communication, cross-functional collaboration and disciplined decision-making. The module offers practical tools—the 5C framework, stakeholder matrices, translation techniques, channel optimisation, incident playbooks, evidence hierarchies, awareness programmes and case studies—that professionals can immediately apply. By aligning language across disciplines, adopting regular cadences, documenting responsibilities and quantifying business impact, organisations can turn communication from a liability into a force multiplier for security effectiveness.

3 KYPO/CRCZ cyber ranges developed

The projects belong to the broader world of cyber range-based training. CyberRangeCZ is described in its own documentation as a fork of the KYPO Cyber Range Platform, building on Masaryk University's earlier work in cybersecurity education, cyber defence exercises and training. The platform is based on modern approaches such as containers, infrastructure as code, microservices and open-source software, with support for OpenStack and AWS cloud provider technology. Its documentation emphasises repeatability, scalability, automation and interoperability, which are precisely the qualities expected from a training module such as this one.

KYPO Cyber Range Platform itself was released as open-source software in 2020, and although active development of the original KYPO CRP has concluded, its legacy continues through CyberRangeCZ. The KYPO site describes the platform as a flexible and scalable virtual environment used for university education, professional training and community building around reusable cybersecurity scenarios. This is important context because the repository is not trying to provide a general-purpose risk platform; it is a training asset designed to be imported into a cyber range environment.

All KYPO/CRCZ projects go through the design, programming, **validation**, and **testing** phases.

For more details about the KYPO/CRCZ platform there are in the relevant deliverable D5.2.

3.1 KYPO/CRCZ LM2 Risk Management (status: **done**)

3.1.1 Source code

The KYPO/CRCZ project is imported from a public GitHub repository maintained by the NG-SOC consortium:

Link to GitHub: <https://github.com/NG-SOC-eu/lm2>

README: <https://github.com/NG-SOC-eu/lm2/blob/main/README.md>

Training Definition: <https://github.com/NG-SOC-eu/lm2/blob/main/v2%20Risk%20Management%20and%20threat%20modeling.json>

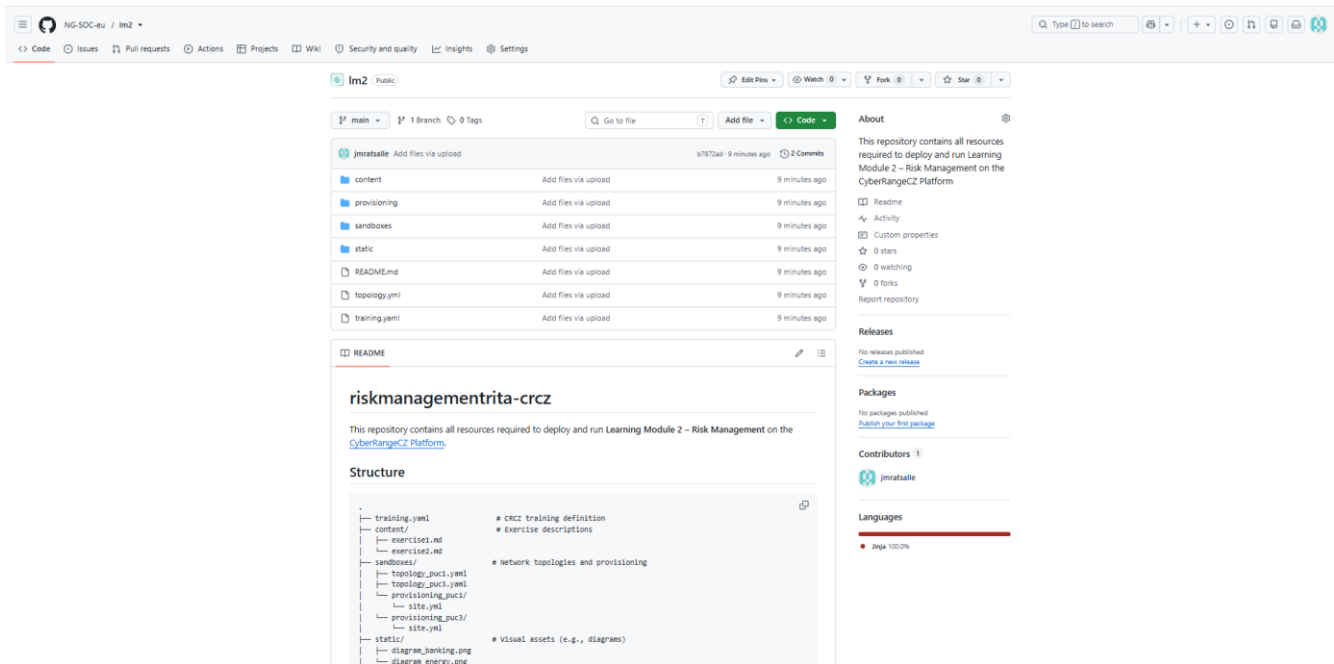


Figure 59 KYPO/CRCZ LM2 Risk Management source code on GitHub

3.1.2 Testing

This project has been validated. Only NG-SOC members (ED & FUNITEC) may participate in testing.

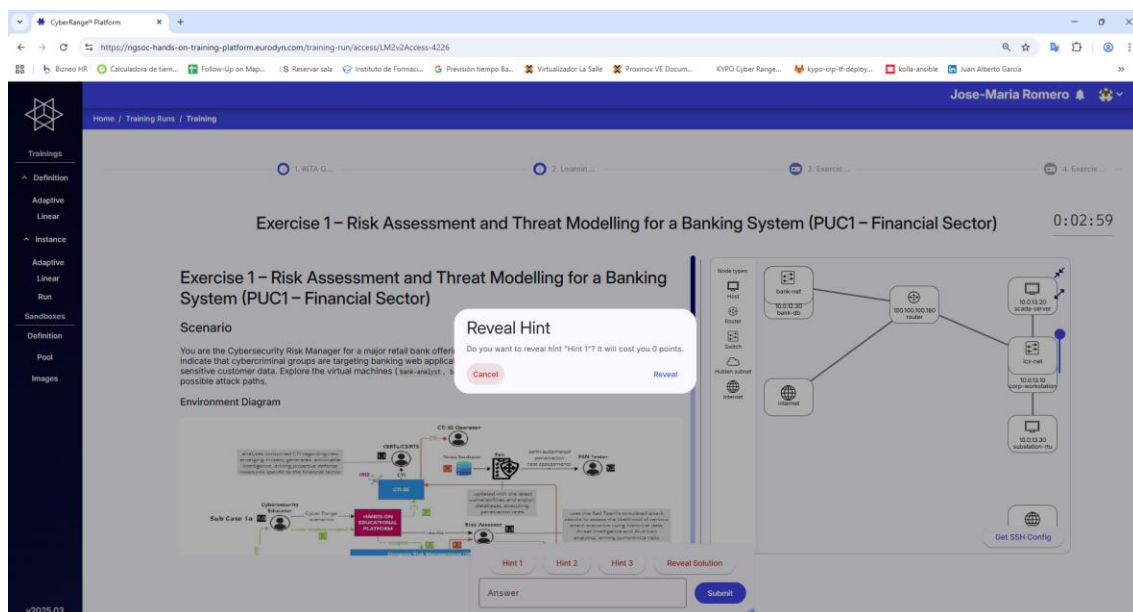


Figure 60 Exercise 1 - Risk Assessment and Threat Modelling for a Banking System (PUC1 - Financial Sector).

3.1.3 General context: KYPO, CyberRangeCZ and this learning module

Within that ecosystem, riskmanagementritra-crcz is best understood as a cyber range scenario package. It includes the content and technical scaffolding needed for learners to act as cybersecurity risk managers in two different critical-sector settings. The README states that the repository contains all resources required to deploy

and run Learning Module 2, “Risk Management”, on the CyberRangeCZ Platform. It also names the main components of the repository: a CRCZ training definition, exercise descriptions, network topologies, provisioning resources and static diagrams.

3.1.4 Repository purpose and educational intent

The central purpose of the module is to train learners in proactive cybersecurity risk management. The training.yaml file describes the scenario as consisting of two hands-on exercises focused on critical sectors, specifically financial services and energy infrastructure. Learners use the RITA platform for dynamic risk analysis while taking on the role of a Cybersecurity Risk Manager for a banking institution and an energy infrastructure operator.

The module is aimed at learners who already have some cybersecurity knowledge. The prerequisites in training.yaml include basic understanding of threats, vulnerabilities and security controls, as well as familiarity with risk assessment methodologies such as ISO 27005 and NIST 800-30, and with attack frameworks. This positions the module at an intermediate to advanced level rather than as an introductory lab for absolute beginners.

The learning outcomes are also clearly risk-oriented. Learners are expected to apply threat modelling methods such as STRIDE and MITRE ATT&CK, qualitatively assess risks using likelihood and impact, prioritise based on business and safety consequences, recommend technical and procedural controls, translate technical analysis into plans for technical and executive audiences, and adapt risk management to OT and ICS environments. This is a broad GRC-oriented skill set, but with enough technical grounding to make the risk analysis evidence-based rather than purely theoretical.

3.1.5 Overall structure of the repository

The repository has a compact and understandable structure. The README.md identifies training.yaml as the CyberRangeCZ training definition, content/ as the folder containing exercise descriptions, sandboxes/ as the location for network topologies and provisioning playbooks, and static/ as the location of visual assets such as banking and energy diagrams. The two exercise files are exercise1.md and exercise2.md, and the sandbox area includes separate topology and provisioning material for PUC1 and PUC3.

This organisation is appropriate for a cyber range module. Pedagogical content is separated from the technical environment definition, and both are separated from visual assets. That makes the repository easier to understand for two different audiences. Learners mainly need the scenario, the tasks and the deliverables. Instructors and platform administrators need the topology definitions, machine roles, provisioning playbooks and deployment instructions.

The structure also shows that this is not an application repository in the usual software engineering sense. There is no indication that the repository contains the source code of RITA itself, nor does it include a large application codebase, unit tests or a conventional build pipeline. Instead, it is a scenario definition repository. Its value lies in combining training narratives, network layouts and automated setup scripts into a coherent cyber range exercise.

3.1.6 The role of RITA

RITA is the key methodological tool in the training. The README expands RITA as “Risk Identification and Threat Assessment”⁶ and describes it as a web interface for cataloguing assets, mapping threats and recording risk calculations during the exercises. The README also states that the exercises require RITA to build asset inventories, model threats and document overall risk evaluations.

The RITA quick guide defines the workflow expected from learners. It covers logging in, creating assets with name, description and owner, assigning threats to assets, linking vulnerabilities, recording references or evidence, estimating likelihood and impact, documenting existing controls and recommended treatments, and importing records from CSV or JSON templates. In other words, RITA is used to make the learner’s reasoning traceable: an asset is identified, threats and vulnerabilities are attached to it, risk is evaluated, and controls or treatments are then recorded.

There is an important implementation caveat. The repository does not include the RITA application itself. The provisioning playbooks simply attempt to install a package called rita and start the RITA service. This means that the training is only fully reproducible in an environment where that package is available through the configured package sources or image baseline. For a preconfigured CyberRangeCZ deployment in the NG-SOC context, that may be intentional and sufficient. For an external user trying to reproduce the training independently, it is a dependency that would need clearer documentation.

Exercise 1: banking-sector risk assessment and threat modelling

The first exercise, PUC1, is titled “Risk Assessment and Threat Modelling for a Banking System”. The learner acts as Cybersecurity Risk Manager for a major retail bank offering online services. The scenario introduces recent threat intelligence reporting that cybercriminal groups are targeting banking web applications and payment systems in order to commit fraud and exfiltrate sensitive customer data.

The banking exercise uses three main machines: bank-analyst, bank-web and bank-db. Learners are instructed to explore these virtual machines to identify high-value assets and possible attack paths. The connection guide directs them to open a terminal in the CyberRangeCZ interface, connect to the analysis workstation and then connect from there to the web and database servers. They are also instructed to use Nmap to scan services on bank-web and bank-db, and Wireshark or tcpdump to capture traffic between machines.

The task design is intentionally hybrid. It starts with technical discovery, but the objective is not exploitation for its own sake. Learners must map critical assets and data flows, log into RITA, model bank assets, threats and countermeasures, build threat scenarios using STRIDE and MITRE ATT&CK, assess likelihood and impact, propose mitigations and prepare documentation for both technical and executive audiences. This sequence is a strong example of turning technical observations into risk management outputs.

The deliverables requested for the banking exercise include a threat model, a 5×5 likelihood-versus-impact risk matrix, RITA risk evaluation results, a prioritised risk treatment plan and an executive summary. This is useful because it forces learners to work across multiple levels of abstraction. They must identify what is technically present in the environment, reason about what could go wrong, assess the significance of those scenarios and express the result in a form that leadership could understand.

⁶ RITA is actually DRME.

The expected findings in training.yaml further clarify the intended learning path. For the banking scenario, the expected answer includes an inventory of critical banking assets such as core banking services, digital channels, SWIFT interfaces and customer databases. It also expects mapping of dependencies involving internal systems, third parties, cloud services and payment processors, as well as threat identification aligned with MITRE ATT&CK for financial environments, including targeted phishing, credential abuse and data exfiltration.

The risks identified in the expected answer are business-relevant rather than merely technical. They include privileged credential compromise enabling fraudulent transactions or manipulation of accounting records, ransomware affecting payment platforms, exfiltration of sensitive customer data leading to PSD2 or GDPR penalties and reputational damage, and excessive reliance on suppliers without strong continuity plans. The recommended mitigations include privileged access management, continuous monitoring, credential rotation, phishing resilience, network segmentation, immutable backups, supplier SLAs, contingency planning and SIEM-integrated anomalous behaviour alerts.

This makes the banking exercise particularly valuable for learners who need to practise the bridge between security architecture and governance. The scenario is simple enough to run in a limited lab window, but it points towards realistic enterprise risk themes: identity compromise, payment disruption, regulatory exposure, supplier concentration, ransomware resilience and executive communication.

Exercise 2: energy-sector and ICS/SCADA risk assessment

The second exercise, PUC3, is titled “Risk Assessment and Threat Modelling for an Energy Infrastructure”. In this exercise, the learner acts as Cybersecurity Risk Manager for a national power transmission operator. The environment includes IT/OT interconnection, SCADA servers, RTUs and engineering workstations, and the scenario is motivated by alerts about ICS-specific malware.

The main machines in the energy exercise are corp-workstation, scada-server and substation-rtu. Learners are asked to explore how the IT and OT networks interact, connecting first to the corporate workstation and then from there to the SCADA server and substation RTU. They are instructed to use tools such as nmap to map reachable services and Wireshark to inspect industrial protocols.

The task sequence again combines technical discovery with formal risk analysis. Learners must identify ICS and IT assets critical to operations, use RITA to model ICS assets and threats, model scenarios such as malware propagation from IT to OT, insider manipulation of SCADA and unauthorised RTU commands, assess safety, operational and strategic impact, recommend controls suited for industrial environments and summarise findings for leadership and engineers.

This exercise is especially important because OT risk differs from conventional IT risk. In a banking environment, confidentiality, integrity, fraud prevention and regulatory compliance are central. In an energy environment, availability and physical safety become dominant concerns. A technically modest vulnerability may have high consequence if it affects grid operations, remote control of substations, engineering workstations or the integrity of telemetry.

The deliverables for the energy exercise include an ICS threat model, a 5x5 risk matrix considering operational impact, a RITA-generated risk report covering energy infrastructure assets, threats and vulnerabilities, a prioritised mitigation plan for protecting the OT network and a cyber risk report for both technical leads and

executives. The reflection prompts ask learners to identify the most significant safety risk and consider which mitigations would be hardest to implement, which encourages practical thinking about operational constraints.

The training definition expects learners to adapt risk management approaches to industrial environments, explicitly accounting for availability and physical safety considerations. This is one of the strongest aspects of the module because it avoids treating OT security as a simple copy of IT security. In real industrial settings, patching windows, asset lifecycles, deterministic communications, safety requirements and vendor dependencies all influence what mitigations are realistic.

3.1.7 Training design and learner progression

The module has a clear two-stage progression. The banking exercise introduces risk assessment in a familiar IT-heavy business context. Learners work with web and database components, payment-related risk, credential compromise and data protection concerns. The energy exercise then shifts the learner into an industrial context where business impact includes safety, operational continuity and critical infrastructure resilience.

This sequencing is effective because it allows the same risk management discipline to be applied in two different domains. Learners can reuse the general logic of asset identification, threat modelling, likelihood and impact assessment, prioritised mitigation and executive reporting, while also learning that the meaning of “impact” changes between sectors. In banking, impact may mean fraud, customer data loss, payment disruption or regulatory penalties. In energy, impact may mean loss of visibility, unsafe control actions, operational outages or physical consequences.

The training is configured as released and uses two training levels, each estimated at 90 minutes. The total implied learning time is therefore approximately three hours. Given the number of activities in each exercise, this is a dense but plausible format for an instructor-led cyber range session, especially if the technical environment is already deployed and learners are guided through the expected workflow.

3.1.8 Standards, frameworks and competence alignment

The repository explicitly references MITRE ATT&CK, STRIDE Threat Modelling, ENISA ECSF competence mapping, ISO 27005 and IEC 62443 for ICS. This mixture is appropriate. STRIDE gives learners a structured way to think about threat categories. MITRE ATT&CK provides a common language for adversary behaviours. ISO 27005 and NIST 800-30 provide risk assessment context. IEC 62443 is relevant to the industrial case because it deals with security for industrial automation and control systems.

The practical value of these frameworks is that learners are not merely asked to “find risks”. They are expected to use recognisable methods to reason about risks. In the banking exercise, MITRE ATT&CK and STRIDE help learners structure fraud, credential abuse, lateral movement and data exfiltration scenarios. In the energy exercise, the same modelling mindset is adapted to ICS and SCADA scenarios, where unauthorised commands, malware propagation and manipulation of engineering or control systems may have safety and availability implications.

The ENISA ECSF reference also matters because the module is role oriented. The README names Cybersecurity Risk Manager, Security Architect and OT/ICS Security Analyst as target roles. That makes the learning objectives more concrete: the module is not only teaching tool usage but also training learners to think and communicate like professionals in defined cybersecurity roles.

3.1.9 Sandbox topologies and virtual infrastructure

The repository includes both a root topology.yml and two scenario-specific topologies under sandboxes/. The root topology defines a combined environment named ngsoc-lm2, containing banking hosts, ICS hosts, a rita-server and a router. It includes two networks, bank-net with CIDR 10.0.12.0/24 and ics-net with CIDR 10.0.13.0/24. In that combined topology, RITA is mapped to bank-net at 10.0.12.60.

The PUC1-specific topology defines a separate banking sandbox named ngsoc-lm2-puc1. It uses bank-net with CIDR 10.0.1.0/24 and maps bank-analyst to 10.0.1.10, bank-web to 10.0.1.20, bank-db to 10.0.1.30, rita-server to 10.0.1.40 and the router to 10.0.1.1. The machines use images such as kali and debian-11, with the management user set to Debian.

The PUC3-specific topology defines an ICS sandbox named ngsoc-lm2-puc3. It uses ics-net with CIDR 10.0.2.0/24 and maps corp-workstation to 10.0.2.10, scada-server to 10.0.2.20, substation-rtu to 10.0.2.30, rita-server to 10.0.2.40 and the router to 10.0.2.1. This clean separation makes sense for independent delivery of the banking and energy exercises.

There is, however, a documentation issue worth noting. The root topology and the scenario-specific topologies use different network ranges, different environment names and different image names. The README tells users to choose sandboxes/topology_puc1.yaml for the banking use case or sandboxes/topology_puc3.yaml for the ICS use case, but the presence of the combined root topology could still cause confusion for someone importing the module for the first time.

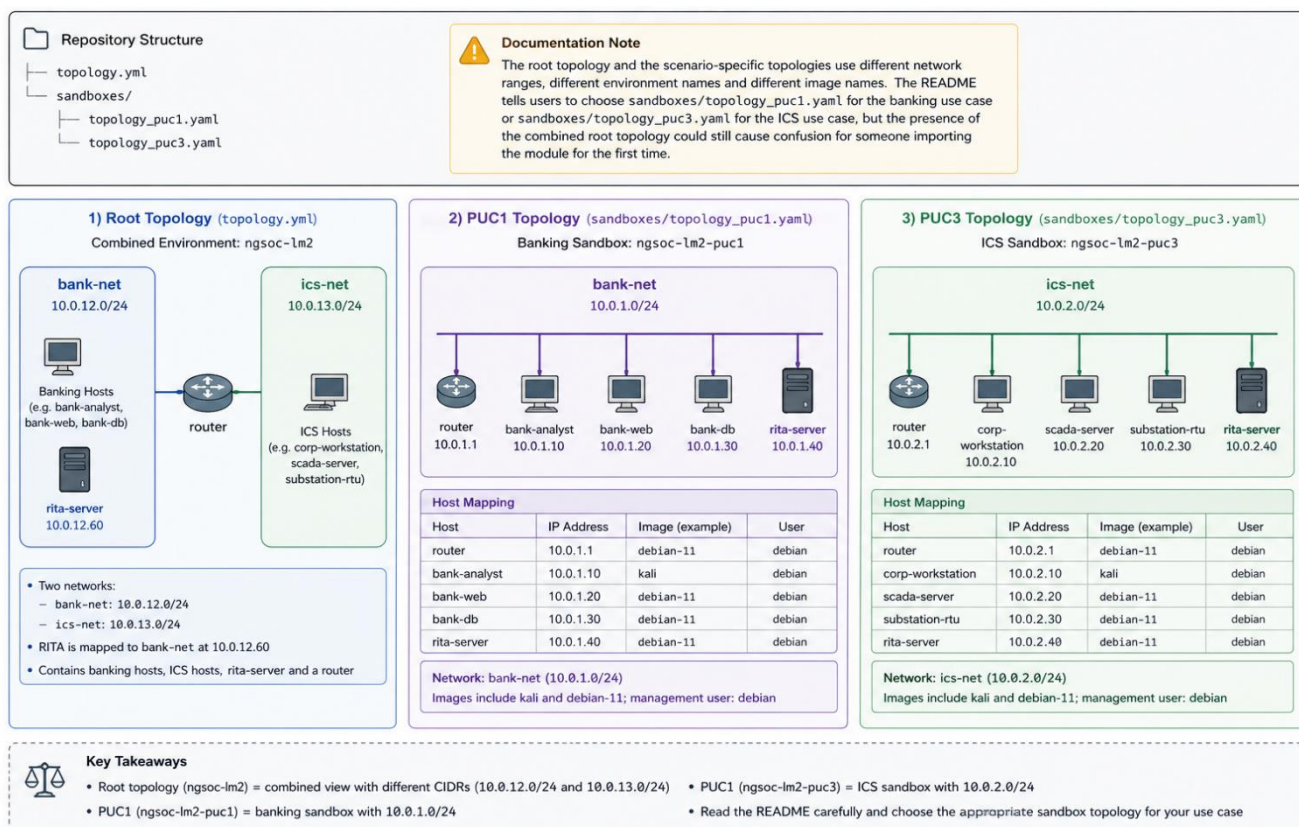


Figure 61 LM2 Topologies Overview

3.1.10 Provisioning approach and security implications

The PUC1 provisioning playbook configures the router by enabling IPv4 forwarding, installing iptables-persistent, applying NAT for 10.0.1.0/24 and persisting the iptables rules. It then configures the banking web server by installing Apache2 and deploying a minimal “Online Banking” page. It configures the banking database by installing MariaDB and changing the bind address to 0.0.0.0, and it installs and starts RITA on rita-server. Finally, it removes UFW from all hosts.

From a teaching perspective, this is straightforward and effective. Learners can discover a web server and a database server, observe basic network flows and identify obvious risk-relevant design choices. From a real-world security perspective, however, allowing MariaDB to listen on all interfaces and removing the host firewall would be unsafe in production. In a cyber range, those choices are understandable because they make the environment easier to analyse. The repository would still benefit from explicitly stating that these are deliberate lab simplifications, not deployment recommendations.

The PUC3 provisioning playbook follows a similar router setup pattern, enabling forwarding, installing iptables-persistent, applying NAT for 10.0.2.0/24 and saving the rules. It then configures substation-rtu by installing netcat, deploying a systemd template for a netcat listener and starting services on port 502 and port 102. The same playbook also installs and starts RITA and removes UFW from all hosts.

The ICS service simulation is intentionally lightweight. Port 502 is commonly associated with Modbus, and port 102 is associated with S7comm-style industrial communications, so exposing listeners on these ports helps learners identify industrial-looking services during scanning. However, netcat listeners do not implement actual industrial protocol logic, PLC behaviour, process simulation or SCADA semantics. This is adequate for a risk modelling exercise, but it would not support deep protocol analysis or realistic OT attack emulation.

3.1.11 Deployment and operating workflow

The README provides a concise deployment workflow. It recommends Ansible 2.12 or later and states that the provisioning playbooks use modules from the ansible.posix and community.general collections. It gives the relevant ansible-galaxy command for installing those collections. The README then instructs users to import the training through CyberRangeCZ Platform’s Training Management area, upload all repository files including training.yaml, select the appropriate sandbox variant and run the matching provisioning playbook.

The getting-started instructions are also practical. Once the environment is deployed, learners connect via SSH using the management account Debian, with the default password usually also being Debian unless the instructor states otherwise. The recommended workflow is to open a terminal in the CyberRangeCZ interface, connect first to the main analyst machine, then access the remaining machines via SSH and follow the appropriate exercise guide.

This deployment model assumes that the instructor or platform administrator is already comfortable with CyberRangeCZ concepts such as training imports, sandbox variants, provisioning playbooks and machine access. That is reasonable for a CyberRangeCZ module, but the documentation would be stronger if it included a short “known-good deployment path” with expected post-provisioning checks, such as verifying that the web server responds, MariaDB is listening, RITA is reachable and the ICS listener ports are open.

3.1.12 Strengths of the repository

The strongest aspect of the repository is the clarity of its educational purpose. It is not trying to be too many things at once. It focuses on cybersecurity risk management, makes RITA the central tool, and gives learners two domain-specific scenarios in which to practise the discipline. The banking and energy cases are distinct enough to show that risk management is context-dependent, while similar enough in structure to let learners apply a repeatable method.

A second strength is the balance between technical and managerial thinking. Learners are asked to scan hosts and inspect traffic, but those tasks feed into threat models, risk matrices, treatment plans and executive summaries. This mirrors real cybersecurity work, where technical evidence must often be translated into prioritised action, funding decisions and risk acceptance conversations.

A third strength is the inclusion of OT/ICS content. Many training scenarios stay in conventional IT environments, but this module includes SCADA servers, RTUs, engineering workstations and IT/OT interconnection. Even if the protocol simulation is lightweight, the scenario encourages learners to think about availability, safety and operational impact, which are essential in critical infrastructure risk management.

A fourth strength is modularity. The two use cases can be run independently, and the repository separates the training definition, content, topologies, provisioning and diagrams. This makes it easier for instructors to adapt or extend the module. For example, an instructor could enrich the banking environment with more realistic authentication flaws or expand the ICS environment with a more capable protocol simulator without rewriting the entire training structure.

3.1.13 Assessment of suitability for training delivery

For an instructor-led training session inside an already prepared CyberRangeCZ environment, the repository appears suitable and coherent. It has clear scenarios, defined roles, structured tasks, expected deliverables and automated provisioning. It should work particularly well for learners who already understand basic networking and security concepts but need practice turning technical observations into risk analysis and prioritised mitigation.

For self-study, the module may be less smooth unless the learner has access to a CyberRangeCZ deployment and the required RITA package. The content files are readable on their own, but the experience depends heavily on the virtual environment and RITA workflow. Without those components, the learner can still study the scenario design, but cannot fully perform the intended exercise.

For reuse by another organisation, the repository is promising but would benefit from hardening as a distributable training package. The most useful additions would be clearer dependency documentation, a deployment checklist, expected service validation commands, known issues, screenshots of the expected RITA workflow, explicit instructor notes, and a short explanation of how to adapt the scenario to different CyberRangeCZ images or networks.

3.1.14 Final assessment

Overall, NG-SOC-eu/riskmanagementrita-crcz is a focused and useful cyber range training repository for teaching cybersecurity risk management. Its value lies in the combination of domain narrative, technical discovery, structured threat modelling, RITA-based risk documentation and executive communication. It does not attempt

to be a sophisticated attack simulation platform, and it should not be judged primarily on the complexity of its services. Its real contribution is pedagogical.

The banking scenario gives learners a practical way to think about online services, databases, payment risk, fraud, credential abuse, ransomware, supplier dependency and data protection. The energy scenario extends the same risk management discipline into OT and ICS, where availability, safety, segmentation and operational continuity are central. Together, the two exercises help learners understand that cybersecurity risk is not just a list of vulnerabilities, but a structured judgement about assets, threats, controls, consequences and priorities.

The repository would be classified as a well-targeted technical GRC training module. It is strongest as an instructor-led exercise for intermediate or advanced learners in Cybersecurity Risk Manager, Security Architect, SOC Analyst or OT/ICS Security Analyst roles. Its main limitations are not conceptual, but operational: RITA dependency documentation, topology clarity, deployment validation and ICS realism could all be improved. With those refinements, it would become a more robust and reusable cyber range package for organisations wanting to teach risk management across IT and OT environments.

Link to this video demonstration on SharePoint: [lm2 cyber range.mp4](#)

3.1.15 Scenario status and public-release readiness

This scenario is sufficiently mature for publication as an open training asset. The repository already provides the main elements expected from a reusable cyber range package: training definition, learner-facing exercise descriptions, sandbox topology, provisioning resources and static diagrams. The practical value of the scenario is increased by the two use-case perspectives: financial-sector risk assessment and energy/ICS risk analysis.

Table 12 Scenario status and public-release readiness

Scenario name	Repository / resource	Machine-readable format	Validation state	Deployment constraints	Public-release readiness
LM2 Risk Management : banking-sector PUC1 and energy/ICS PUC3 exercises	https://github.com/NGSOC-eu/lm2	JSON training definition, training.yaml , KYPO/CRCZ topology YAML, Ansible provisioning artefacts, CSV/JSON RITA templates	Validated for deployment and operation in CyberRangeCZ	Requires CyberRangeCZ/KYP O-compatible infrastructure, Debian/Kali images, the RITA dependency, and two isolated networks for the banking and ICS scenarios	Ready with caveats: public release is suitable once the external RITA dependency and lab-only assumptions are documented clearly

3.1.16 Public-dissemination hygiene review

Table 13 Public-dissemination hygiene review

Hygiene items	Assessment	Required public-release action
Default credentials	No production credentials should be published. Any trainer, analyst or RITA access values must be presented as deployment placeholders only.	Replace any environment-specific values with placeholders and document that operators must inject credentials through CyberRangeCZ, Ansible Vault or equivalent mechanisms.
Weak passwords	The scenario is educational and may rely on simplified lab accounts. However, weak-password examples must not be framed as reusable deployment credentials.	Add a short warning that weak credentials, if present, are intentionally limited to the isolated training environment.
RITA dependency	The repository expects RITA to be available during provisioning, but the RITA application itself is not part of the scenario package.	Document installation source, version expectation, fallback procedure and offline-deployment considerations.
TODO / password-hash caveats	Any TODO markers related to accounts, password hashes or deployment secrets should be treated as release blockers.	Ensure all TODOs are resolved or clearly moved to operator-facing deployment instructions.
Public dissemination	The scenario is suitable for publication because it is risk-management oriented and does not require exploit delivery.	Add a “public-release note” confirming that all organisational names, assets and risk data are synthetic.

3.1.17 YAML/JSON artefact inventory

Table 14 YAML/JSON artefact inventory

Artefact	Format	Location / role	Release note
Training definition	JSON	Main training definition file for the LM2 risk-management exercise	Should remain schema-valid and importable into CyberRangeCZ.
Scenario outline	YAML	training.yaml	Describes the learner flow and scenario metadata.
Sandbox topology	YAML	Root and PUC-specific topology definitions	Must be checked for non-overlapping CIDRs and valid image/flavour references.
Provisioning playbooks	YAML / Ansible	Sandbox provisioning area	Should be idempotent and free of embedded deployment secrets.
RITA import templates	CSV / JSON	Used for dynamic risk analysis	Should include synthetic risk examples only.
Static diagrams	Image / supporting artefacts	Repository static folder	Safe for publication if no internal infrastructure names are exposed.

3.2 KYPO/CRCZ LM8 Incident Response Subcase 1a (status: **done**)

3.2.1 Source code

The KYPO/CRCZ project is imported from a public GitHub repository maintained by the NG-SOC consortium:

Link to GitHub: <https://github.com/NG-SOC-eu/lm8-1a-2>

README: <https://github.com/NG-SOC-eu/lm8-1a-2/blob/main/README.md>

Training Definition: [https://github.com/NG-SOC-eu/lm8-1a-2/blob/main/Subcase%201a%20%E2%80%93%20Instructor-led%20training%20of%20incidentresponse-crcz%20\(LM8\).json](https://github.com/NG-SOC-eu/lm8-1a-2/blob/main/Subcase%201a%20%E2%80%93%20Instructor-led%20training%20of%20incidentresponse-crcz%20(LM8).json)

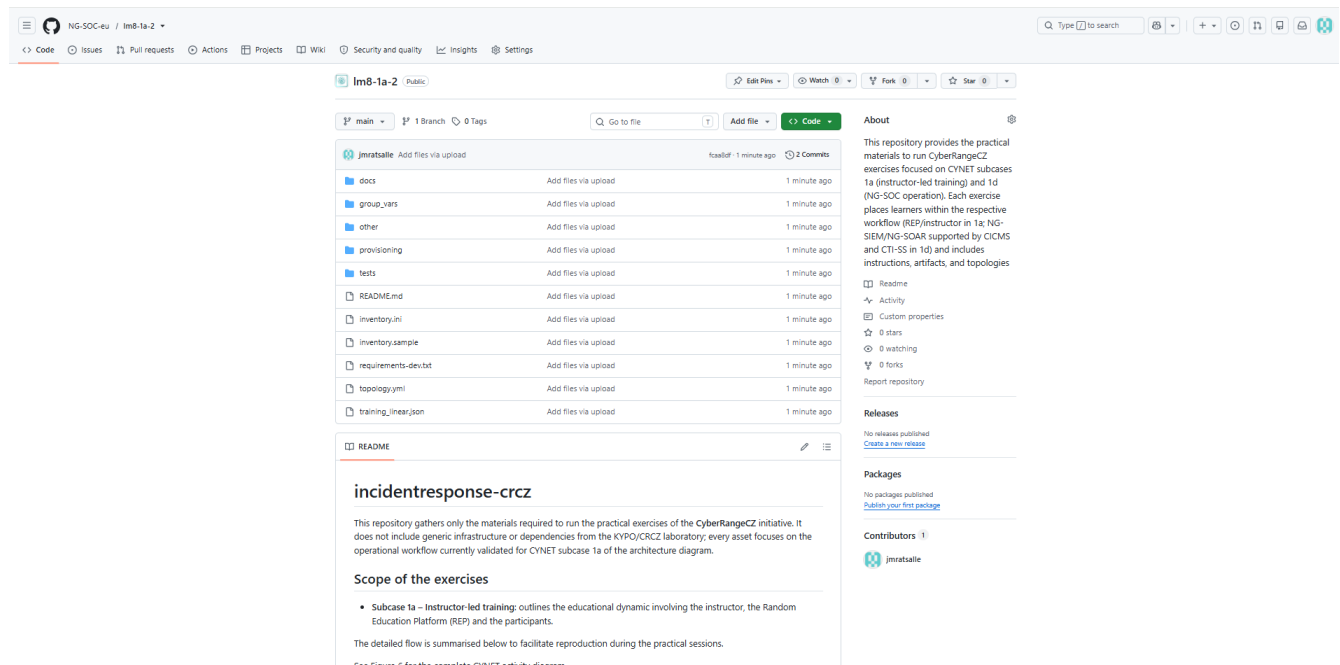


Figure 62 KYPO/CRCZ LM8 Incident Response Subcase 1a source code on GitHub

3.2.2 Testing

The repository includes an explicit “Validating the repository” section and a runnable local validation workflow based on pytest (install dev requirements and run pytest). The checks focus on structural consistency of training_linear.json, internal references in topology.yml, and the KYPO topology mappings under provisioning/.

No additional participation restrictions (e.g., “only consortium members may test”) are stated in the repository; the content is provided for educational purposes.

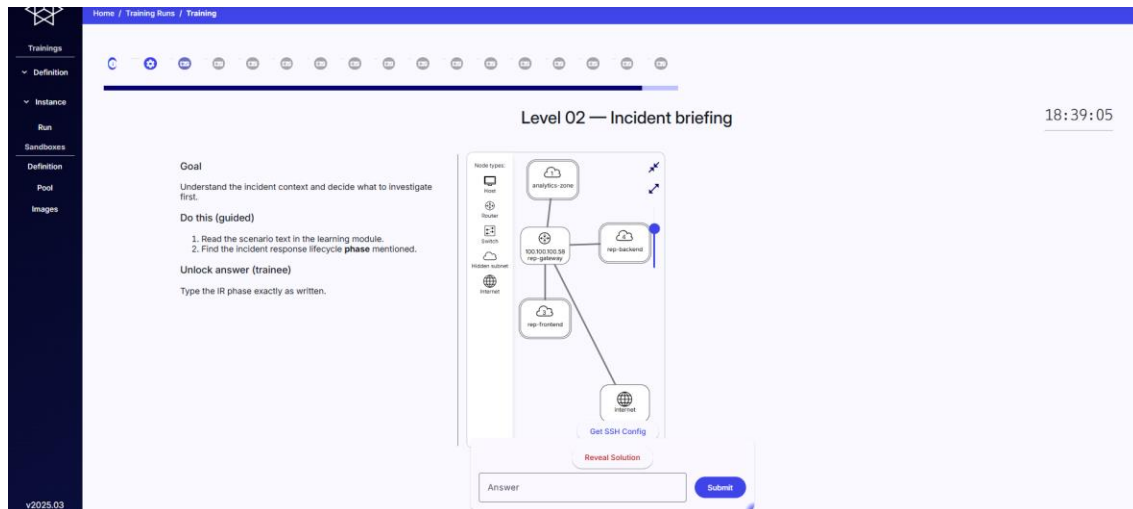


Figure 63 Level 02 - Incident briefing

3.2.3 CyberRangeCZ and KYPO context

This context matters because the repository is not intended to be a standalone application. It is a content and provisioning package designed for a cyber range platform where virtual machines, networks and training flows are described in human-readable files such as YAML and JSON. CyberRangeCZ's own documentation highlights this approach: virtual machines, networks and trainings are defined using open-source tooling, including Ansible for describing machine content.

KYPO CRP itself remains open source, although active development of the original platform has ended. The KYPO site states that CyberRangeCZ is its enhanced successor and maintains compatibility. This repository therefore sits in the KYPO/CRCZ lineage: it uses cyber range topologies, sandbox provisioning, Ansible roles and structured training material to reproduce a specific educational workflow.

3.2.4 Repository identity and project status

The repository is named `incidentresponse-crcz-2-1a` and belongs to the NG-SOC-eu organisation. GitHub shows it as a public repository on the `main2` branch, with 59 commits, no open issues, no open pull requests, no published releases and no package artefacts shown on the repository page. GitHub reports the language mix as mainly Shell, Python and Jinja.

The README explicitly states that the repository gathers only the materials required to run the practical exercises of the CyberRangeCZ initiative and does not include generic infrastructure or dependencies from the wider KYPO/CRCZ laboratory. It also states that every asset focuses on the operational workflow validated for CYNET subcase 2a. This means the repository should be assessed as a targeted training-support package rather than as a complete incident response platform.

3.2.5 Overall purpose of the project

The project is designed to support an instructor-led cyber range training session in which participants learn phishing awareness, suspicious email analysis, basic incident reporting and collaborative response practices. The central educational environment is REP, the Random Education Platform. The workflow begins with instructor preparation, continues through live session delivery, formative quizzes and practical tests, and expands into

more advanced phishing-related exercises such as multi-channel spear phishing, collaborative response and express forensic reporting.

The training is not written as a conventional “capture the flag” or highly technical compromise-and-remediation exercise. Instead, it is a platform-orchestrated training process. The instructor schedules modules, REP distributes short theory capsules and guided simulations, trainees complete quizzes and practical labs, and the reporting workspace consolidates results for final feedback. In that sense, the incident response aspect is procedural, collaborative and educational, rather than a deep forensic investigation of a compromised infrastructure.

The practical scenario is centred on phishing awareness. The dedicated guide `docs/subcase-1a-phishing-awareness.md` describes suspicious email analysis, header verification, attachment inspection, use of collaborative channels, reporting of findings and production of an express forensic report. This makes the repository particularly relevant for awareness training, first-response skills, user reporting behaviour, coordination between roles and instructor-led assessment.

3.2.6 Repository structure and content organisation

The repository is organised around a small number of key files and directories. The README identifies `training_linear.json` as the file describing the learning modules for subcase 1a, `topology.yml` as the description of CyberRangeCZ components, `docs/` as the area for supporting materials, `inventory.sample` as a credential-safe inventory template, and `provisioning/` as the location of KYPO/CRCZ topology files and Ansible playbooks.

The `docs/` directory contains the provisioning guide and the phishing awareness guide, as well as a `figures/` directory containing the CYNET activity diagram image referenced by the README. The documentation is therefore split between conceptual exercise material and deployment guidance.

The `provisioning/` directory contains the operational automation. It includes `case-1a/`, role directories, scripts, a provisioning README, a collections file, the main playbook and a wrapper script. This is the part of the repository that turns the scenario concept into configured infrastructure: REP backend services, reporting, instructor console and trainee workstations.

The `tests/` directory contains a Python validation test file, and `requirements-dev.txt` lists `pyyaml`, `pytest` and `jinja2` as development dependencies. This is notable because many training repositories contain only static YAML and Markdown; here, the authors have added structural tests to verify that the training sequence and topology remain consistent.

3.2.7 Training design and pedagogical flow

The learning sequence is defined in `training_linear.json`. It is named “CyberRangeCZ Practical Modules” and described as a learning sequence for subcase 1a in the CyberRangeCZ environment, aimed at instructors and trainees. It contains one module, `subcase-1a`, titled “Subcase 1a - Instructor-led training”. The module is organised into phases, each containing sequential activities and associated tools.

The first phases are preparation and delivery. The instructor defines objectives, materials and timings in the CyberRangeCZ control panel, then schedules the activity in REP Scheduler. During delivery, the instructor starts the live session, presents objectives and enables collaborative channels such as chat, videoconferencing and whiteboard. REP then distributes theory capsules and guided simulations to trainees.

The middle phases focus on assessment and feedback. Trainees answer interactive quizzes with immediate feedback, while the instructor reviews real-time results through analytics and reinforces key points. Supervised labs or challenges are then launched through REP Practical Labs and the CyberRangeCZ environment. REP consolidates results and produces a report for final feedback.

The later phases add more incident-response-like elements. The training sequence includes a multi-channel spear phishing simulation using email, SMS and voice, followed by trainee inspection of attack vectors and reporting through REP forms. It then adds a collaborative response chain with a coordination room, secure chat, videoconferencing and a task board. Finally, it requires an express forensic report based on artefacts such as headers, logs and captures.

This progression is pedagogically sound. It begins with instructor-led explanation, then moves into knowledge checks, then into practical exercises, then into collaborative response and finally into concise reporting. The structure is well suited to awareness and first-response training because it does not assume that every participant is a specialist analyst; instead, it gradually introduces technical evidence, reporting discipline and team coordination.

3.2.8 The phishing awareness scenario

The file docs/subcase-1a-phishing-awareness.md is the most explicit description of the learning activity. It states that the guide describes activities carried out by instructors and trainees within REP for the phishing awareness module, mirroring components documented in the CyberRangeCZ architecture.

The instructor's preparation tasks include defining module objectives, assigning resources from the CyberRangeCZ content repository, creating a themed course in REP Scheduler, enabling theory blocks, guided exercises and practical work on suspicious email analysis, and synchronising dashboards in the Reporting Workspace. This places the instructor in a coordination and orchestration role rather than simply a lecturer role.

The trainee experience is built around live delivery, quizzes and practical email analysis. Trainees receive personalised itineraries, complete formative quizzes on phishing concepts, classify potentially malicious emails, verify headers and inspect attachments in a controlled environment. Their actions are recorded and linked to course objectives for later assessment.

The advanced exercises extend the basic awareness module into more realistic incident handling. The multi-channel spear phishing campaign combines email, instant messaging and simulated calls. The collaborative response chain assigns roles such as analyst, communications lead and legal support. The express forensic report requires participants to review evidence, generate preliminary findings, structure a report and upload it to the Reporting Workspace for validation against a template.

The assessment criteria are practical and measurable. The guide expects complete REP Scheduler configuration, quiz performance above a threshold defined by the instructor, lab coverage including header review, indicator analysis and attachment inspection, successful execution of advanced exercises, and a final report summarising risks, findings and recommendations.

3.2.9 Topology and virtual infrastructure

The root topology.yml defines a sandbox named lm8-subcase-1a-phishing-awareness. It includes Ubuntu-based REP components, Windows trainee workstations, a Debian router and three networks: rep-backend, rep-

frontend and analytics-zone. The REP backend contains the scheduler, live session, quiz engine and practical labs services. The frontend network contains the instructor console and trainee workstations. The analytics zone contains the reporting workspace.

The provisioning-specific topology under provisioning/case-1a/topology.yml mirrors the same conceptual design but uses the sandbox name subcase_1a_phishing_awareness. It defines the same functional hosts: instructor-console, rep-scheduler, rep-live-session, rep-quiz-engine, rep-practical-labs, reporting-workspace, two trainee Windows workstations and a rep-gateway router. It also uses the same three subnets: 10.20.10.0/24 for the REP backend, 10.20.20.0/24 for the frontend and 10.20.30.0/24 for analytics.

The network design is sensible for the scenario. REP backend services are isolated from direct user access, the instructor and trainees sit on an accessible frontend segment, and reporting is placed on a separate analytics segment. The router rep-gateway connects all three networks, with addresses ending in .1 on each segment. This gives the exercise a simple but meaningful structure: service delivery, user interaction and analytics are logically separated.

The VM image choices also reflect the learning environment. The REP components and instructor/reporting machines use Ubuntu Noble images, the router uses Debian 12, and the trainee machines use Windows 10 accessed through WinRM. That is coherent for a phishing-awareness scenario because trainees often need a Windows desktop-like environment, while backend and reporting services are more naturally provisioned on Linux.

There is one small consistency issue. The root topology uses win10 as the trainee image name, while the provisioning topology uses windows-10. That may simply reflect different naming conventions or image aliases, but it should be documented because CyberRangeCZ image names are environment-specific, and a mismatch can break deployment if the expected image is not available.

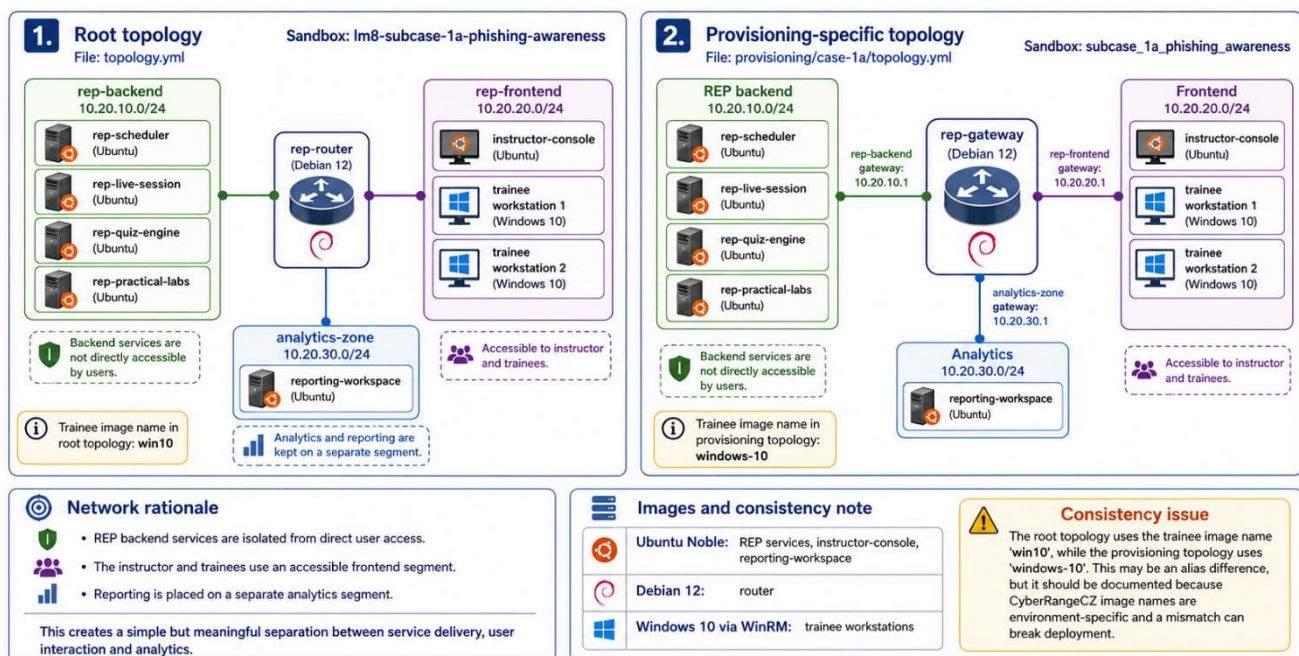


Figure 64 LM8 Subcase 1a Topology Overview

3.2.10 Provisioning workflow and deployment process

The provisioning guide explains that deployment has two main phases: importing the KYPO/CRCZ topology and configuring virtual machines with Ansible. The guide instructs users to sign in to the KYPO portal with sandbox creation rights, upload provisioning/case-1a/topology.yml, deploy the sandbox and wait until all machines are reachable.

The guide then covers credentials. It tells users to duplicate inventory.sample to inventory.ini, keep hostnames and IP addresses aligned with the topology, and export credentials as environment variables or use Ansible Vault. This is a good security practice because it avoids committing real passwords to version control.

System prerequisites include wget, Python pip, virtualbmc, Ansible, pywinrm and the Ansible collections declared in provisioning/collections.yml. The collections file requires ansible.windows, community.general and community.windows, reflecting the mixed Linux and Windows nature of the sandbox.

The repository provides a wrapper script, provisioning/run_playbook.sh, which checks for required commands, installs the declared Ansible collections and then runs provisioning/playbook.yml against the selected inventory. The provisioning README explicitly warns that running ansible-playbook directly is unsupported in KYPO/CRCZ because the control node may lack required collections, and it recommends always using the wrapper.

3.2.11 Ansible playbook architecture

The main playbook is organised into several phases. It first verifies that the ansible.windows collection is installed on the control node. It then configures the Windows trainee machines, configures REP core services on the backend hosts, prepares the reporting workspace, personalises the instructor console and finally configures the trainee workstation role with variables from group_vars/trainees.yml.

The provisioning role structure is clear. The rep-core role handles the REP platform behind Nginx. The reporting-workspace role provisions Grafana dashboards and data sources. The instructor-console role prepares tmux configuration and shell shortcuts. The trainee-workstation role distributes the REP collector configuration, Windows shortcuts and lab welcome material. The windows role applies basic Windows lab configuration such as RDP, WinRM and firewall changes.

This architecture is more mature than a minimal training repository. Rather than placing all tasks in a single monolithic playbook, the authors have divided responsibilities into roles with defaults, templates, validation tasks and handlers. That makes the package more maintainable and easier to adapt for different CyberRangeCZ deployments.

3.2.12 REP core services

The rep-core role is responsible for publishing the REP platform behind Nginx, with load balancing towards the scheduler, live session and quiz engine services. Its default configuration defines upstreams for 10.20.10.10:9001, 10.20.10.20:9002 and 10.20.10.30:9003, corresponding to scheduler, live session and quiz engine respectively. TLS is disabled by default because the lab images do not ship with certificates; operators can enable TLS by providing certificate and key material.

The tasks install and start Nginx, create REP-related directories, deploy the virtual host template, enable the site, optionally install TLS material, create a rep system user and group, provision a shared secret if provided, validate Nginx configuration with `nginx -t`, and optionally check the health endpoint when TLS is enabled.

A notable operational caveat is that the health endpoint check appears conditional on TLS being enabled. Since TLS is disabled by default, the default lab deployment may validate Nginx syntax but not necessarily validate the REP health endpoint. That is understandable if the health endpoint depends on services not fully simulated in the lab, but it means the default deployment may not prove functional REP application behaviour end-to-end.

3.2.13 Reporting workspace and analytics

The reporting-workspace role provisions Grafana. The defaults define the Grafana package, configuration path, provisioning directories, a PostgreSQL data source called `rep_postgresql`, and a dashboard titled “REP Overview”. The role also defines the Grafana APT repository using `https://apt.grafana.com` and a signed keyring.

The tasks configure the Grafana repository, install the Grafana package, ensure the Grafana service is enabled and started, create provisioning directories, deploy the main configuration, data source and dashboard provider files, create dashboard folders, deploy dashboards, restart Grafana as required and validate the health endpoint at `http://127.0.0.1:3000/api/health`.

The implementation includes useful diagnostic behaviour. If Grafana fails to start, the role reads `systemctl` status and recent `journalctl` output and fails with diagnostics. The validation logic also accounts for non-JSON responses and checks that the Grafana health response reports the database as ok. This is a positive sign of operational maturity in the provisioning code.

There is, however, a default placeholder password in the reporting workspace data source configuration. It is marked as a default and can be overridden, but the presence of *changeme* reinforces the need for inventory or group variable hardening before any real deployment.

3.2.14 Instructor console

The instructor console role creates an instructor user, prepares a workspace, deploys a tmux configuration and publishes shell shortcuts. The default shortcuts include launching the scheduler via SSH, opening the quiz dashboard in Firefox and opening a ticket queue by connecting to ng-soc. The default tmux windows include scheduler, broadcast and monitoring sessions.

The role validates the tmux configuration and checks that generated shell shortcuts are executable functions. This is a small but useful quality measure: it catches template or configuration mistakes during provisioning rather than leaving the instructor to discover them during a live session.

The presence of the `open_ticket_queue` shortcut to ng-soc is interesting because the main subcase 1a topology does not define an NG-SOC host. The `inventory.sample` does include groups and hosts for `ng_soc`, `ng_siem`, `ng_soar`, `cti_ss`, `cicms`, `playbook library` and `telemetry feeder`, but these are not part of the subcase 1a topology. This suggests that the repository is either prepared for integration with wider NG-SOC subcases or retains references to a broader architecture.

3.2.15 Trainee workstation configuration

The trainee workstation role is one of the more technically detailed parts of the repository. Its defaults define a REP collector service running through PowerShell, a collector configuration file under C:\ProgramData\REP, log paths, an ingestion pipeline with HTTPS transport to <https://rep-core.internal/ingest>, a syslog transport to soc-gateway.internal:514, a desktop shortcut to the live session and a welcome note under C:\Labs.

The role validates that the collector ingestion token is not still set to *changeme*, creates required directories, deploys the welcome note, renders the collector configuration and PowerShell script, determines the correct NSSM architecture, copies or downloads *nssm-2.24.zip*, extracts it, installs the collector as a Windows service, starts it and validates both service status and heartbeat log entries.

This design is practical for a cyber range. It gives the trainee workstation an agent-like component that can send telemetry or evidence back to the REP infrastructure, while also providing shortcuts and a simple lab entry point. The validation logic is again relatively mature: it collects service status, event logs and collector logs when startup or heartbeat checks fail.

There is also a security concern. The group variable *group_vars/trainees.yml* contains a non-default-looking ingestion token, *rep-core-trainee-collector-7b92de11*. It may be only a lab token, but because it is committed in the repository, it should be treated as non-secret or replaced per deployment. The trainee role correctly rejects the literal placeholder *changeme*, but committed reusable tokens can still be problematic if the same value is used across environments.

3.2.16 Windows base configuration

The windows role applies basic Windows lab changes. It stops and disables Windows Update, disables automatic reboot for updates, disables the Windows Licensing Monitoring Service, aborts pending shutdowns, sets the network profile to private, enables RDP, disables Network Level Authentication, allows ICMP, enables firewall groups for Remote Desktop and WinRM, explicitly opens WinRM and RDP ports, completely disables the Windows firewall and changes the windows user password to *qwerty!23*.

From a lab reliability perspective, these choices are understandable. Disabling updates and automatic reboots prevents disruption during exercises. Enabling RDP and WinRM improves manageability. Allowing ping and remote management helps instructors and provisioning scripts validate connectivity.

From a security perspective, however, this role is deliberately unsafe outside an isolated cyber range. Disabling the Windows firewall and setting a hard-coded password are not acceptable production practices. The repository would benefit from more explicit documentation stating that these settings are lab-only measures and must not be reused in real environments.

3.2.17 Helper scripts and automation utilities

The repository includes helper scripts under *provisioning/case-1a/scripts/*. The script *schedule_rep_lab.sh* submits a JSON lab schedule payload to the REP Scheduler endpoint, requiring *REP_SCHEDULER_API_BASE* and *REP_API_TOKEN*. The script *export_quiz_report.sh* downloads quiz analytics from the Reporting Workspace, requiring *REP_REPORTING_API_BASE* and the same token.

The example schedule payload defines a course called rep-phishing-awareness, a lab named “Email analysis practical”, a start time, duration, communication channels and objectives such as validating phishing indicators and recording evidence in Practical Labs. It also includes participant groups.

These helper scripts are useful because they make dry runs and integrations easier. They also show that the authors expect the platform to expose API-like endpoints for scheduling and reporting, rather than relying entirely on manual UI operations. That aligns with the broader CyberRangeCZ principle of automation and repeatability.

3.2.18 Validation and quality controls

The repository includes explicit validation tests in `tests/test_validation.py`. These tests check that `training_linear.json` has the expected structure, that modules, phases, activities and tools are populated, and that step numbers are sequential. They also check that provisioning topology files contain required keys, and that host, router and network mappings refer to defined objects.

The tests also inspect specific Ansible role behaviour. They verify that instructor console shortcut validation handles empty lists correctly, that reporting workspace health check defaults expose fallbacks, that the Grafana OSS repository is included in defaults, that non-JSON Grafana health responses are handled, and that repository setup happens before Grafana package installation.

This is a notable strength. Many cyber range content repositories rely on manual review and break easily when YAML files drift. Here, the repository includes automated structural checks, and the README explains that users can install development dependencies and run `pytest` to validate the repository.

3.2.19 Credential and secret management

The repository shows awareness of credential management. The README instructs users to replace password placeholders in `inventory.sample` by referencing Ansible Vault files or environment variables. The inventory template itself uses `lookup('env', ...)` expressions for passwords rather than hard-coded real secrets.

This is good practice for a public training repository. It lets the repository remain usable while avoiding committed operational passwords. The provisioning documentation also reinforces the same pattern by instructing users to export credentials as environment variables or use Ansible Vault files.

At the same time, there are two caveats. First, the Windows role contains a hard-coded password change to `qwerty!23`, which should be treated as a lab-only convenience. Second, the trainee group variables include a concrete-looking collector token. Even if that token is not sensitive in practice, a clearer convention would be to use a placeholder and require deployment-specific override, as the trainee role already does for the default changeme token.

3.2.20 Strengths of the repository

The main strength of the repository is that it is coherent as a training operations package. It does not merely describe a phishing awareness class; it provides a training sequence, topology, provisioning roles, instructor tools, trainee workstation configuration, reporting workspace, helper scripts and validation tests. That makes it more complete than a static exercise guide.

A second strength is that the pedagogical flow is clear. The module moves from instructor preparation to live delivery, quiz-based formative assessment, practical phishing analysis, collaborative response and express forensic reporting. This progression is well suited to incident response education at awareness and first-response level.

A third strength is the separation of concerns in the infrastructure design. Backend REP services, frontend instructor and trainee access, and analytics/reporting are placed into separate network zones. That gives the sandbox a meaningful architecture without making it too complex for a focused training session.

A fourth strength is the use of Ansible roles and validation checks. The repository does not simply assume that provisioning works; it includes role-level validation for Nginx, Grafana, tmux shortcuts and Windows collector service status. It also includes Python tests for training and topology consistency.

3.2.21 Suitability for training delivery

The repository is well suited for instructor-led training where the objective is phishing awareness, suspicious email analysis, coordinated response and rapid reporting. It would be particularly useful for mixed technical and non-technical groups because the scenario includes both user-facing activities, such as recognising phishing and reporting suspicious messages, and more structured response activities, such as role assignment, evidence collection and express forensic reporting.

It is also suitable for demonstrating how a cyber range can support a training platform rather than only attack-defence labs. The inclusion of REP Scheduler, Live Session, Quiz Engine, Practical Labs and Reporting Workspace shows an education-centric workflow: content delivery, guided simulation, assessment, telemetry and feedback.

It is less suitable as a standalone technical incident response lab if the expected outcome is deep malware analysis, full forensic disk imaging, SOC alert triage, SIEM correlation or SOAR playbook execution. Some of those ideas are hinted at through the broader inventory and the repository's About text, but the concrete subcase 1a material focuses on phishing awareness and first-response coordination.

For external reuse, the repository would benefit from a clearer "minimum viable deployment" section explaining exactly which services are real, which are simulated, which hostnames must resolve, which credentials must be overridden, and which parts of the inventory belong to other subcases. That would make it easier for instructors outside the original project context to reproduce the training reliably.

3.2.22 Final assessment

Overall, NG-SOC-eu/incidentresponse-crcz-2-1a is a focused CyberRangeCZ/KYPO training repository for CYNET subcase 2a, centred on instructor-led phishing awareness and response activities delivered through REP. Its value lies in the integration of a learning sequence, cyber range topology, Ansible provisioning, instructor console preparation, Windows trainee workstation configuration, reporting dashboards, helper scripts and validation tests.

The repository is strongest as an educational orchestration package. It shows how a cyber range can support structured training, live instruction, formative quizzes, practical phishing analysis, collaborative response and concise reporting. It is not primarily an advanced technical incident response environment, although it contains hooks and references that could connect to wider NG-SOC, SIEM, SOAR, CTI and CICMS workflows.

From an engineering perspective, the repository is more mature than a simple Markdown-only training guide because it contains role-based provisioning and automated checks. From a security perspective, several lab-only shortcuts need clearer warnings, especially the Windows firewall disablement, hard-coded password and reusable-looking collector token.

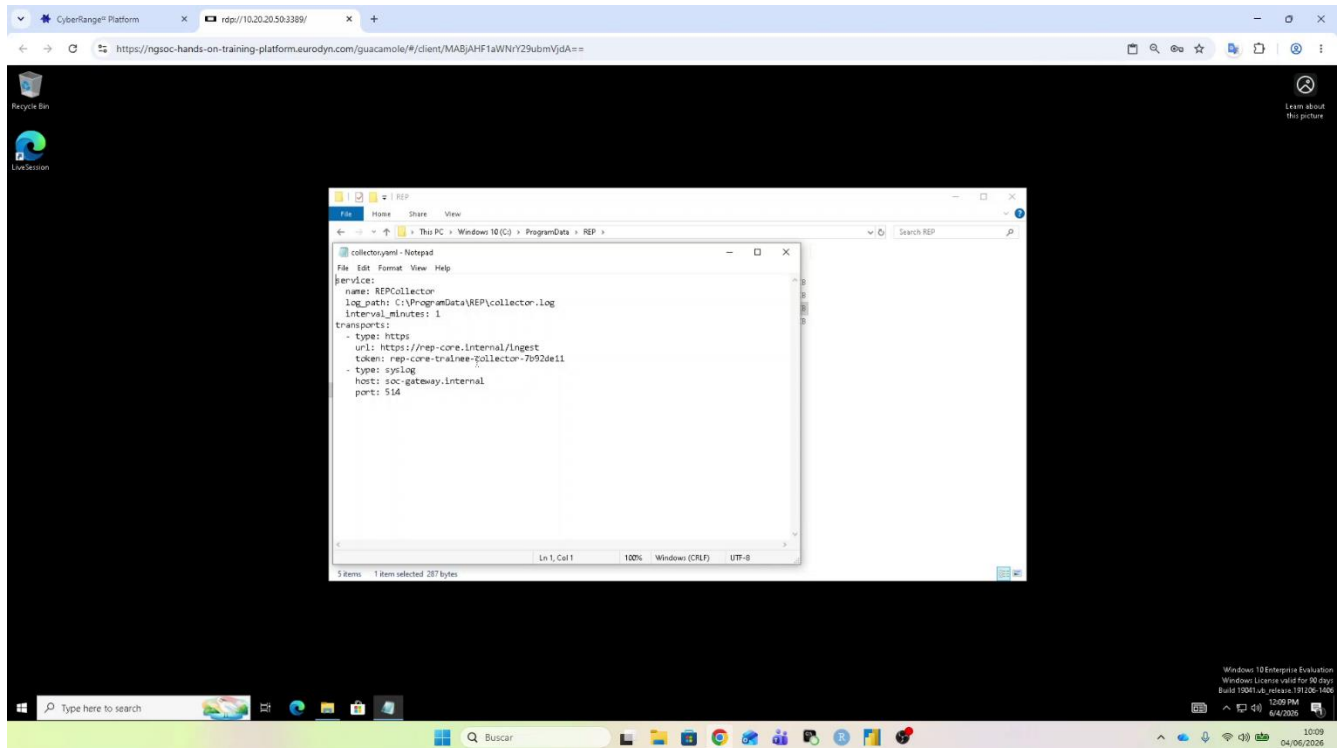


Figure 65 LM8 Subcase 1a exercise (screenshot)

Link to this video demonstration on SharePoint: [lm8-1a-2 cyber range.mp4](#)

3.2.23 Scenario status and public-release readiness

This scenario provides a realistic instructor-led incident-response and phishing-awareness environment. It is strong from a training-delivery perspective because it combines learner activities, reporting, analytics and instructor supervision. Its public-release readiness depends mainly on dissemination hygiene, not on pedagogical completeness.

Table 15 Scenario status and public-release readiness

Scenario name	Repository / resource	Machine-readable format	Validation state	Deployment constraints	Public-release readiness
LM8 Incident Response Subcase 1a	https://github.com/NG-SOC-eu/lm8-1a-2	JSON training definition, topology YAML, Ansible provisioning, REP	Locally validated through automated checks for training	Requires REP services, reporting workspace, instructor console and	Conditionally ready: suitable for controlled publication after credential, token and Windows

		configuration, validation tests	structure, topology references and selected provisioning assumptions	Windows trainee workstations	hardening caveats are cleaned or explicitly labelled as lab-only
--	--	---------------------------------	--	------------------------------	--

3.2.24 Public-dissemination hygiene review

Table 16 Public-dissemination hygiene review

Hygiene items	Assessment	Required public-release action
Default credentials	The scenario contains lab accounts and service-access assumptions. These must not be interpreted as production defaults.	Replace examples with placeholders or move them to a protected deployment guide.
Weak passwords	The Windows trainee configuration includes intentionally weak lab access settings.	Do not publish the actual password value in public guidance; describe it as a lab-only weak credential.
Collector token	A concrete trainee collector token appears to be present in configuration material.	Treat it as a non-secret training token or replace it with a generated deployment token.
Windows security posture	The lab disables or relaxes several Windows security features to simplify training access.	Add an explicit statement that these settings are unsafe outside an isolated cyber range.
TODO / password-hash caveats	Any unresolved account, token or password-hash TODOs should be considered release blockers.	Resolve before public release or document them as operator setup steps.

3.2.25 YAML/JSON artefact inventory

Table 17 YAML/JSON artefact inventory

Artefact	Format	Location / role	Release note
Training definition	JSON	Instructor-led incident-response training definition	Must remain compatible with CyberRangeCZ import.
Topology definition	YAML	Root scenario topology	Should be validated against provisioning group names and network mappings.
Provisioning roles	YAML / Ansible	REP, reporting, instructor console and trainee workstation roles	Must not contain reusable secrets.

Inventory sample	INI / YAML-like Ansible inventory	Deployment input	Should use environment lookups or vault placeholders only.
Validation tests	Python / YAML / JSON checks	Repository test folder	Should be retained as public quality evidence.
Reporting configuration	JSON / dashboard configuration	Reporting workspace and analytics components	Should contain synthetic data only.

3.3 KYPO/CRCZ LM8 Incident Response Subcase 1a-3 (status: testing on execution)

3.3.1 Source code

The KYPO/CRCZ project is imported from a public GitHub repository maintained by the NG-SOC consortium:

Link to GitHub: <https://github.com/NG-SOC-eu/lm8-1a-3>

README: <https://github.com/NG-SOC-eu/lm8-1a-3/blob/main/README.md>

Training Definition: <https://github.com/NG-SOC-eu/lm8-1a-3/blob/main/ngsoc-lm8-subcase1a-training.json>

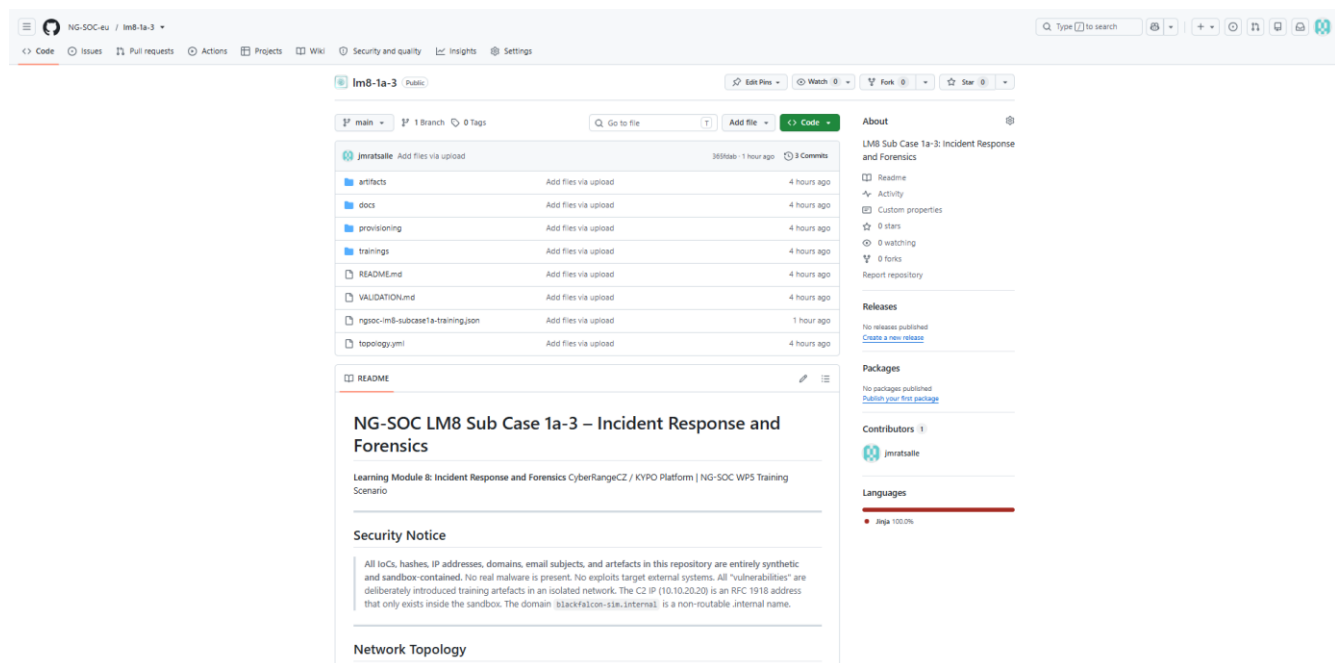
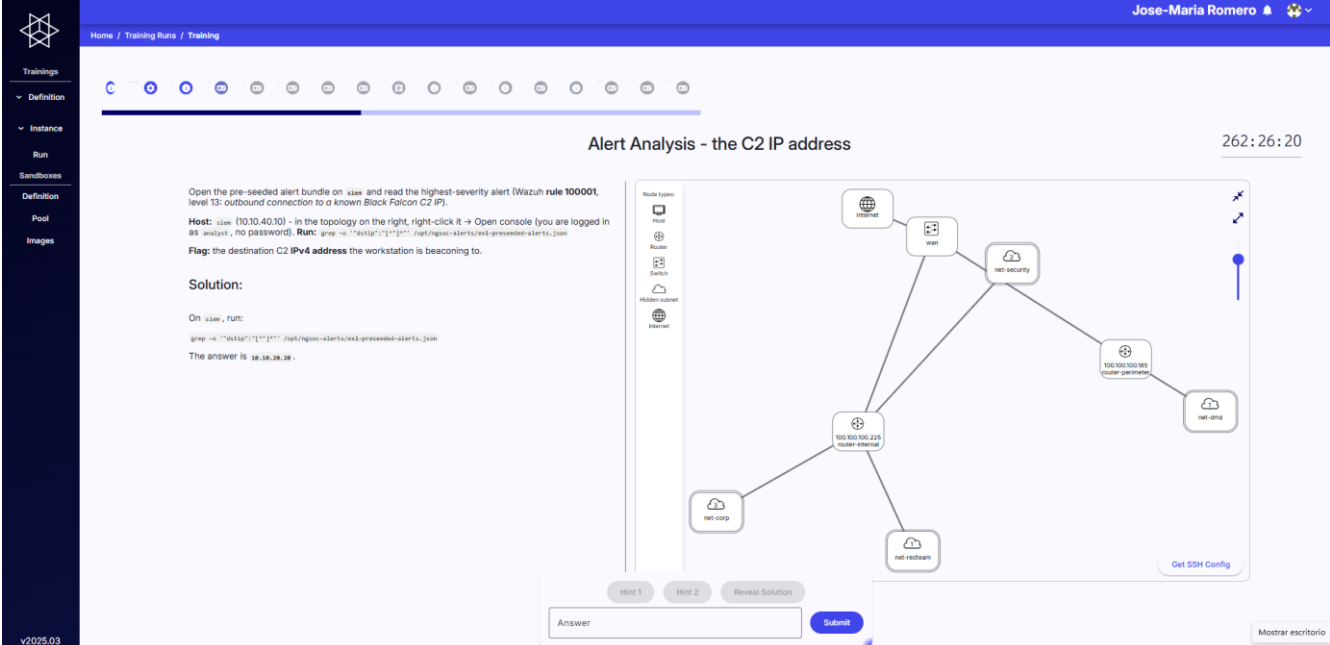


Figure 66 KYPO/CRCZ Incident Response Subcase 1a-3 source code on GitHub

It is explicitly positioned as a CyberRangeCZ/KYPO training scenario for **Learning Module 8: Incident Response and Forensics**, under the NG-SOC WP5 training context.

The repository is not a conventional application and should not be assessed as one. It is a cyber range scenario package: its purpose is to define a sandbox topology, provision deliberately vulnerable and deliberately compromised systems, deliver structured training exercises, and provide synthetic evidence bundles for

assessment. The README is explicit that all IoCs, hashes, domains, email subjects and artefacts are synthetic and sandbox-contained, that no real malware is present, and that all vulnerabilities are deliberately introduced training artefacts in an isolated network. The C2 IP address is a private RFC 1918 address, and the blackfalcon-sim.internal domain is non-routable.



Alert Analysis - the C2 IP address 262:26:20

Open the pre-seeded alert bundle on `siem` and read the highest-severity alert (Wazuh rule 100001, level 13: outbound connection to a known Black Falcon C2 IP).

Host: `siem` (10.10.40.10) - in the topology on the right, right-click it → Open console (you are logged in as `analyst`, no password). **Run:** `grep -r "/opt/nginx/alerts/red-preseeded-alerts.json"`

Flag: the destination C2 IPv4 address the workstation is beaconing to.

Solution:

On `siem`, run:

```
grep -r "/opt/nginx/alerts/red-preseeded-alerts.json"
```

The answer is `10.10.20.20`.

Network diagram showing a topology with nodes: `net`, `net-security`, `100.100.100.100 router-gateway`, `100.100.100.220 router-internal`, `net-corp`, and `net-redteam`. The diagram illustrates a network structure with various components and their interconnections.

Figure 67 Level 04 - Alert Analysis - the C2 IP address

3.3.2 Overall purpose of the project

The project is designed to deliver a broad incident response and forensics learning experience around a fictional banking-sector intrusion by a synthetic threat actor called **Black Falcon**. Unlike the earlier phishing-awareness-style subcase, this repository implements a more operationally complete scenario. It spans SOC triage, incident containment, CTI analysis, threat-informed penetration testing, ransomware crisis coordination, multi-channel phishing triage, collaborative response and express forensic reporting. The README maps the scenario to WP5:M8 topics, ECSF roles and MITRE ATT&CK techniques, showing that the repository aims to cover not only technical analysis but also role-based collaboration and regulatory decision-making.

The educational value of the repository lies in its integrated storyline. A trainee can begin as a SOC analyst reviewing suspicious outbound C2 traffic from employee-ws, move into CSIRT containment of a broader compromise involving web-banking, file-server and db-server, pivot into CTI work through MISP, conduct an authorised penetration test against the same vulnerable banking application, and finally coordinate a ransomware tabletop that synthesises the earlier technical events into crisis management. The scenario therefore models incident response as a chain of interdependent roles rather than as a single isolated lab.

3.3.3 Repository structure and content organisation

The repository is organised around four main content areas: infrastructure definition, provisioning, training definitions and evidence artefacts. The root contains topology.yml, README.md and VALIDATION.md. The provisioning/ directory contains the main Ansible playbook.yml, group variables and in-repository roles. The trainings/ directory contains five JSON exercise definitions, and the artifacts/ directory contains phishing, forensic and ransomware tabletop materials. The docs/ directory contains the instructor guide and student handouts, including exercise-specific guides, an after-action report template and an express forensic report template.

This structure is coherent for CyberRangeCZ delivery. The topology defines what exists; the provisioning tree defines how each host behaves; the training JSON files define the learner journey; the artefacts provide evidence; and the documentation gives instructors and students the operational context needed to run the session. The result is closer to a complete training operations package than to a simple lab description.

3.3.4 Network topology and sandbox architecture

The sandbox topology is significantly more ambitious than a minimal phishing-awareness scenario. It defines two routers and four user-defined networks: net-dmz at 10.10.20.0/24, net-corp at 10.10.30.0/24, net-security at 10.10.40.0/24 and net-redteam at 10.10.50.0/24. The management/WAN network is platform-managed at 100.100.100.0/24. The README estimates the resource footprint at approximately **14 vCPU and 70 GB RAM** per sandbox instance, which is substantial and reflects the inclusion of Wazuh/OpenSearch, MISP, Velociraptor and a Kali workstation.

The DMZ contains the deliberately vulnerable web-banking host and the hidden c2-server. The corporate LAN contains employee-ws, file-server and db-server, and is not directly accessible to trainees. The security segment contains the main blue-team tooling: siem, analyst-host and cti. The red-team segment contains kali, used for the penetration-testing exercise. This segmentation is pedagogically strong because it forces different roles to interact with different parts of the environment: SOC and IR students work through security tooling, red-team students operate from Kali, and internal corporate assets are not simply handed to the trainee as directly accessible machines.

The topology also uses routers to enforce training boundaries. router-perimeter acts as the DMZ gateway and permits HTTP/HTTPS to the banking application and restricted C2 traffic for the exercise. router-internal connects the corporate, security and red-team segments, allowing security tools to reach corporate hosts, allowing corporate hosts to communicate with the SIEM, and allowing red-team access to the DMZ while explicitly blocking red-team access to corporate and security-tool networks. This is an important design feature because it turns the topology into part of the exercise control mechanism, not merely a network diagram.

3.3.5 Host roles and simulated enterprise environment

The host design is coherent and deliberately role-rich. The web-banking host represents a vulnerable banking web application with Apache, PHP and MySQL. It deliberately exposes a SQL injection flaw in login.php, weak

credentials for the admin account and an accessible `/backup/` directory. These weaknesses are not accidental; the role documentation states clearly that they are educational weaknesses and must never be deployed outside an isolated training sandbox.

The employee-ws host is configured as the initially compromised endpoint. It deploys a beacon script under `/opt/c2-beacon/`, schedules it through cron every five minutes, writes syslog entries that simulate a Trojan infection, and attempts TCP connections to the synthetic C2 server. This creates the telemetry required for the SOC triage exercise and provides a concrete artefact for persistence and C2 mapping.

The file-server host provides the ransomware and data-impact portion of the scenario. It creates a Samba share, places synthetic customer data in `/srv/data`, creates .locked file stubs, writes a ransom note and generates a simulated encryption event log. This makes the file server useful both for hands-on containment and for the ransomware tabletop exercise.

The c2-server is deliberately simple and deliberately safe. It runs a Python listener on port 4444, logs incoming connections and returns an acknowledgement, but the role comments state that it is a listener only and has no offensive capability or real malware functionality. It also publishes a simple web panel stub so that the host can be discovered during scanning or threat analysis.

3.3.6 Provisioning workflow and Ansible design

The main provisioning playbook follows the dependency order of the environment. It first applies a common baseline to all nodes, then configures routers, then provisions DMZ hosts, corporate LAN hosts, security-tooling hosts and the red-team workstation. The security segment receives Wazuh/OpenSearch, the CICMS workstation and CTI-SS; the red-team host receives Kali tooling and artefact templates. This sequencing is sensible because routing and baseline configuration must exist before the host-specific training services can function reliably.

The common role sets the timezone and locale, installs base packages, writes `/etc/hosts`, creates the student analyst user, injects the platform SSH key and grants passwordless sudo in the training environment. This is useful for reducing instructor overhead and ensuring a consistent access model, although the passwordless sudo decision should be considered a lab-only convenience rather than a secure operational pattern.

The repository uses in-repository Ansible roles rather than depending heavily on external Galaxy roles. The `requirements.yml` file declares the `ansible.posix` collection and states that no external Galaxy roles are required, while leaving commented alternatives for community MySQL and PHP roles. This makes the repository more self-contained and easier to review, although it still depends on external package sources and downloads during provisioning.

3.3.7 Security tooling: SIEM, DFIR and CTI

The SIEM role deploys Wazuh with OpenSearch and Wazuh Dashboard on the siem host. It pre-loads custom detection rules for key scenario events, including outbound C2 communication, possible Trojan infection, lateral movement, ransomware-style .locked changes and DNS queries to the synthetic Black Falcon domain. It also

places pre-seeded alert JSON files on the SIEM host, so instructors are not wholly dependent on live telemetry generation during a session.

The forensics-host role equips the analyst-host with a broad DFIR toolkit: tcpdump, tshark, Sleuth Kit, Autopsy, binwalk, foremost, hashdeep, Volatility 3 and Velociraptor. It also deploys a chain-of-custody template, an express forensic report template and a forensic quick-reference card. This is a notable strength because it treats forensics as a process with evidence handling and reporting requirements, not just as command execution.

The cti-misp role deploys CTI-SS through Docker and includes a seed script for the Black Falcon campaign. The seeded event includes synthetic IoCs such as the C2 IP, C2 domain, hashes, email subjects, filename and C2 URL, and tags the event with MITRE ATT&CK and TLP-style metadata. There is, however, an operational caveat: the script initially uses `CHANGE_AFTER_INSTALL` for the API key and requires the instructor or operator to replace it manually after obtaining a valid MISP auth key. That means MISP event seeding may not be fully automatic without post-install intervention.

3.3.8 Red-team and penetration-testing component

The Kali red-team role prepares the offensive testing workstation for Exercise 4. It installs tools such as nmap, Nikto, Hydra, Gobuster, dirb, sqlmap, tcpdump, tshark, smbclient, John, Hashcat and Metasploit, and it clones SecLists. It also deploys a formal engagement brief and a penetration test report template. This is important because the exercise is not simply “attack the box”; it is framed as an authorised, scoped, threat-informed assessment with rules of engagement, in-scope and out-of-scope networks, reporting expectations and MITRE mapping.

Exercise 4 uses the Black Falcon MISP intelligence as context for prioritising attack vectors. The training content instructs trainees to use reconnaissance, web enumeration, SQL injection testing, brute forcing of weak admin credentials, discovery of database credentials and a narrative attack chain. The expected findings include SQL injection, weak admin credentials and information disclosure through `/backup/`, all mapped to relevant ATT&CK techniques.

3.3.9 Training design and pedagogical flow

The training set is built around five main exercises. Exercise 1 is SOC triage: the trainee starts with Wazuh alerts showing outbound traffic from `employee-ws` to `10.10.20.20:4444`, endpoint logs for `/tmp/.svc_update`, suspicious DNS activity and a requirement to decide whether the event is a true positive. This is a strong starting point because it teaches alert corroboration, IoC extraction, severity assessment and escalation.

Exercise 2 shifts into incident response. The scenario expands the incident from one infected workstation to a broader compromise involving the vulnerable web application, file server, database server, possible exfiltration and cron-based persistence. The tasks require scoping, evidence collection, chain of custody, containment decisions, eradication, recovery planning and management communication. This progression mirrors a realistic hand-off from SOC detection into CSIRT ownership.

Exercise 3 introduces CTI analysis through MISP. The trainee must review the Black Falcon event, connect MISP IoCs with evidence from the SIEM, assess organisational risk and produce a threat intelligence brief with team-specific recommendations. The exercise is particularly useful because it links CTI to action: the point is not merely to list IoCs, but to decide what SOC, IR and IT should do with them.

Exercise 5 is a ransomware crisis tabletop for the IR Coordinator role. It requires the trainee to determine whether the ransomware situation is a confirmed incident, establish incident command, resolve conflicts between evidence preservation and service restoration, coordinate technical and business stakeholders, consider NIS2 and GDPR-style obligations, and produce an after-action review. This gives the module an executive and governance dimension that pure technical labs often lack.

3.3.10 Practical assessed activities

Beyond the five exercises, the repository includes three assessed practical activities. Activity 2.0.1 is a multi-channel spear-phishing simulation using email, SMS, voice-script and attachment metadata artefacts. Activity 2.0.2 is a collaborative response chain using REP coordination features, task boards, decision logs, SITREPs and handover notes. Activity 2.0.3 is an express forensic report based on an artefact bundle released during the incident response exercise. The instructor guide integrates these activities into delivery and grading, rather than leaving them as disconnected optional extras.

The artefact role reinforces this design by deploying phishing materials, forensic bundle files, tabletop materials and templates for phishing triage notes, decision logs, SITREPs and handover notes. This is a good operational choice because it ensures students have standardised deliverable formats and instructors can assess outputs against consistent criteria.

3.3.11 Synthetic evidence and realism

The artefacts are detailed enough to support realistic analysis while remaining safe. The phishing email includes a plausible banking-authorisation lure, an internal synthetic sender domain, an apparently macro-enabled attachment placeholder and explicit metadata marking it as a training artefact. The message content uses urgency, regulatory pressure and financial authorisation as social-engineering themes, which are appropriate for a financial-sector scenario.

The forensic bundle provides a coherent chain of evidence. The Wazuh alert bundle contains eight synthetic alerts covering C2 traffic, endpoint infection, suspicious DNS, SMB lateral movement, sudo escalation, ransomware-style file renaming, C2 traffic from db-server and unusual database access. This gives students enough material to reconstruct a multi-stage incident without needing real malware or uncontrolled exploit execution.

The timeline clues file is especially useful pedagogically. It groups evidence into initial access, C2 establishment, lateral movement, data access, ransomware deployment and persistence. It asks students to sort timestamps chronologically and answer questions about detection gap, attack stages, affected hosts and evidence of

exfiltration. This supports the express forensic report activity well because it forces synthesis rather than simple artefact lookup.

3.3.12 Validation and quality controls

The repository includes a `VALIDATION.md` file that serves as a resource and tool reference validation table. It validates platform images and flavours, checks that the user-defined CIDRs do not overlap with the management network, lists deployed tools and services, identifies all synthetic artefacts, maps training JSON files to level types and ATT&CK techniques, and records WP5:M8 topic coverage. It also states that all seven module topics are covered across the exercises and assessed activities.

This validation is valuable, but it is primarily documentary rather than automated. I did not find a visible tests/ directory, CI workflow or pytest-style validation suite in the repository listing. That distinguishes this project from more engineering-oriented training repositories where structural checks are executable. The validation table is still useful for instructor review and deployment readiness, but it would be stronger if backed by automated checks for topology validity, JSON schema compliance, Ansible syntax, role idempotence and broken artefact references.

3.3.13 Deployment requirements and operational caveats

Deployment requires CyberRangeCZ/KYPO platform access, an OpenStack tenant with enough quota for approximately 14 vCPU and 70 GB RAM per instance, and internet connectivity from sandbox hosts for package downloads during provisioning. The README states that the repository should be uploaded to the KYPO platform, a sandbox definition should point to the root topology.yml, and provisioning is expected to take about 30-45 minutes.

Several dependencies require external access during provisioning. `VALIDATION.md` specifically calls out Wazuh downloads from `packages.wazuh.com`, MISP Docker images from Docker Hub, SecLists cloning from GitHub and Velociraptor binary downloads from GitHub releases. In an isolated or restricted OpenStack environment, these would need local mirrors, pre-baked images or offline packages. This is not a flaw in the scenario design, but it is an important deployment constraint for real training delivery.

There are also credential and security caveats. The README lists default access details for Wazuh, MISP and the web-banking application, and explicitly notes that the banking credentials are deliberately weak. The group variables include a concrete database password, and the global variables include a TODO comment instructing operators to replace the student password hash before deployment. These are acceptable in an isolated training package if documented clearly, but they must not be reused outside the range.

3.3.14 Strengths of the repository

The main strength of the repository is its end-to-end learning design. It does not merely provide a vulnerable web application or a set of isolated tasks; it builds a multi-role incident narrative with detection, containment,

intelligence, adversarial testing, ransomware coordination and formal reporting. This makes it well suited to instructor-led training where the aim is to practise both technical actions and cross-team decision-making.

A second strength is the integration of realistic tooling. Wazuh, OpenSearch Dashboard, MISP, Velociraptor, Kali tooling, Samba, Apache/PHP/MySQL and DFIR utilities are all represented in the environment. Even where functionality is simulated or simplified, the learner is exposed to plausible workflows and deliverables rather than abstract quizzes alone.

A third strength is the explicit attention to safety. The repository repeatedly marks artefacts as synthetic, avoids real malware, uses private/internal addressing, and frames exploitability as intentional training design. This is important because the repository includes phishing, C2, ransomware and penetration-testing themes that could otherwise be misinterpreted.

3.3.15 Suitability for training delivery

This repository is highly suitable for advanced or intermediate incident response training, especially where the learning goal is to show how SOC, CSIRT, CTI, penetration testing and incident coordination functions depend on one another. It is also suitable for a capstone module because it combines hands-on investigation with formal outputs such as triage notes, escalation tickets, CTI briefs, penetration test reports, decision logs, SITREPs, after-action reports and forensic reports.

It is less suitable as a small introductory lab for absolute beginners. The number of systems, tools, roles and artefacts could overwhelm trainees who have not previously used SIEM dashboards, MISP, basic Linux, web testing tools or incident response terminology. For mixed audiences, the instructor would likely need to split the module into role-based groups and provide strong facilitation, which the repository's instructor guide anticipates through its REP preparation checklist and exercise-by-exercise delivery notes.

3.3.16 Final assessment

Overall, NG-SOC-eu/lm8-1a-3 is a well-conceived CyberRangeCZ/KYPO scenario package for **Learning Module 8: Incident Response and Forensics**. Its strongest feature is the way it turns one synthetic Black Falcon campaign into a complete training ecosystem: suspicious C2 traffic, endpoint compromise, SQL injection, weak credentials, database access, ransomware impact, CTI enrichment, red-team validation, collaborative response and forensic reporting.

From an educational perspective, the repository is stronger than a single-purpose cyber range exercise because it addresses both technical and organisational response capabilities. From an engineering perspective, it is coherent and mostly self-contained, but would benefit from automated validation, offline deployment guidance and more explicit hardening notes around credentials and lab-only privileges. From a security perspective, the repeated synthetic-data warnings and isolation assumptions are appropriate, but they must be respected: this material is designed for an isolated cyber range and should not be deployed on a live or internet-facing environment.

3.3.17 Scenario status and public-release readiness

This scenario is one of the most complete incident-response environments in the deliverable. It covers SOC triage, containment, CTI enrichment, penetration-testing support, ransomware coordination, phishing triage, collaborative response and express forensic reporting. It also uses a deliberately synthetic threat actor and sandbox-contained artefacts, which is appropriate for public dissemination.

Table 18 Scenario status and public-release readiness

Scenario name	Repository / resource	Machine-readable format	Validation state	Deployment constraints	Public-release readiness
LM8 Incident Response Subcase 1a-3	https://github.com/NG-SOC-eu/lm8-1a-3	JSON exercise definitions, topology YAML, Ansible provisioning, synthetic alert JSON, CTI artefacts, forensic evidence bundles	Documented validation through VALIDATION.md; automated validation should be added	Requires CyberRangeCZ/KYPO, OpenStack resources, Wazuh/OpenSearch, MISP, Velociraptor, Kali tooling and internet or mirrored package sources	Not fully public-ready until default credentials, TODO password-hash notes and dependency validation are resolved

3.3.18 Public-dissemination hygiene review

Table 19 Public-dissemination hygiene review

Hygiene items	Assessment	Required public-release action
Default credentials	The repository documents access details for several services and vulnerable systems.	Replace operational values with placeholders or clearly mark them as disposable cyber range credentials.
Weak passwords	Weak credentials are intentionally part of the simulated banking and compromise environment.	Keep weak credentials only inside learner tasks or instructor notes, with an explicit lab-only warning.
TODO password hash	A TODO marker exists for replacing a student password hash before deployment.	Resolve before public release; unresolved password-hash TODOs should not appear in a public package.
Synthetic artefacts	The scenario states that IoCs, hashes, domains, email subjects and artefacts are synthetic.	Keep this statement prominent in the README and instructor guide.
External dependencies	Wazuh, MISP, Velociraptor and SecLists dependencies may require internet access.	Document offline deployment through mirrors or pre-baked images.

3.3.19 YAML/JSON/CACAO artefact inventory

Table 20 YAML/JSON/CACAO artefact inventory

Artefact	Format	Location / role	Release note
Scenario topology	YAML	Root topology.yml	Must remain consistent with four cyber range networks and router mappings.
Provisioning playbook	YAML / Ansible	provisioning/playbook.yml and roles	Should pass syntax, idempotence and dependency checks.
Training exercises	JSON	trainings/ folder	Five exercise definitions should be schema-checked.
Synthetic SIEM alerts	JSON	Wazuh/OpenSearch seed material	Must not contain real incident data.
CTI event data	JSON / MISP-compatible artefacts	MISP Black Falcon event and indicators	Must remain synthetic and non-routable.
Forensic evidence bundles	Mixed structured artefacts	artifacts/ and docs/	Should include only generated or anonymised evidence.
CACAO artefacts	Not applicable	This is not a CACAO-authoring scenario	No CACAO release requirement for this scenario.

3.4 KYPO/CRCZ LM5 Network Vulnerability Identification Training 1b⁷ (status: testing on execution)

3.4.1 Source code

The KYPO/CRCZ project is imported from a public GitHub repository maintained by the NG-SOC consortium:

Link to GitHub: <https://github.com/NG-SOC-eu/lm5-1b>

README: <https://github.com/NG-SOC-eu/lm5-1b/blob/main/README.md>

Training Definition: https://github.com/NG-SOC-eu/lm5-1b/blob/main/puc2_sub_case_2b_network_vulnerability_training.json

⁷ Aligned to consortium's UML of CYNET-UC-2b.

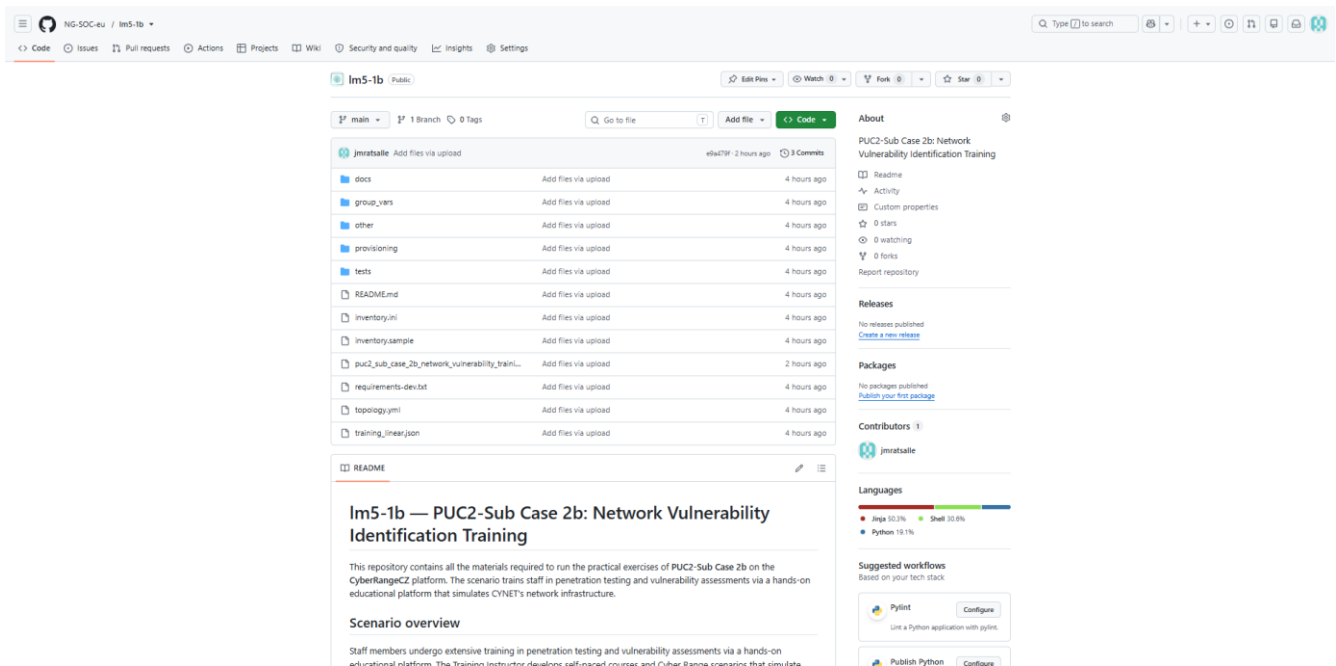


Figure 68 KYPO/CRCZ LM5 Network Vulnerability Identification Training 1b source code on GitHub

The README describes the repository as containing all materials required to run the practical exercises of PUC2-Sub Case 2b on the CyberRangeCZ platform. The scenario is aimed at training staff in penetration testing and vulnerability assessment through a hands-on environment that simulates CYNET network infrastructure. This framing is important: the repository is not presenting a reusable vulnerability scanner or production security system, but a deliberately constructed educational sandbox for controlled reconnaissance, scanning, exploitation basics and reporting.

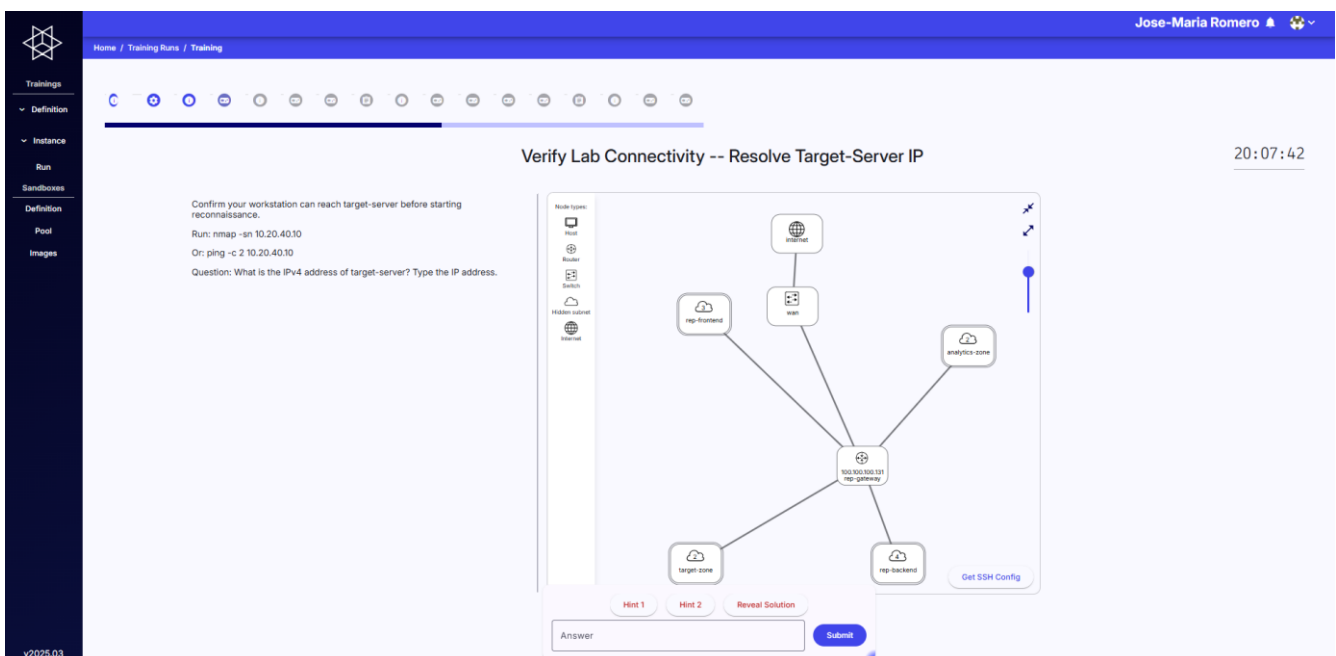


Figure 69 Level 04 - Verify Lab Connectivity -- Resolve Target-Server IP

3.4.2 Overall purpose of the project

The central purpose of Im5-1b is to teach **network vulnerability identification** through a controlled CYNET-like environment. The scenario trains learners to gather technical information about a target network, discover domain names, IP addresses and services, run semi-automated vulnerability assessments, identify misconfigurations and potential entry points, and produce vulnerability reports with CVE/CVSS-style severity and remediation recommendations. The README summarises this as a three-phase learning flow: training and invitation, reconnaissance and scanning, then reporting and recommendations.

The repository is therefore more focused than the earlier LM8 incident response scenario. It does not primarily train SOC triage, crisis coordination, ransomware response or forensic reconstruction. Instead, it is a penetration-testing and vulnerability-assessment module. The learner acts as a junior tester working from a prepared pentest workstation, enumerates a target subnet, identifies exposed services, validates weaknesses in a vulnerable web application and weak SSH configuration, then submits a professional report through Gitea⁸. The separate training definition states that the intended outcomes include running Nmap scans, identifying outdated or misconfigured services, exploiting SQL injection in a web application, authenticating with weak SSH credentials and producing a structured vulnerability report.

3.4.3 Repository structure and content organisation

The repository is organised as a compact but fairly complete cyber range package. The root includes README.md, topology.yml, training_linear.json, a more detailed training definition named puc2_sub_case_2b_network_vulnerability_training.json, inventories, development requirements and a tests/ directory. The docs/ directory contains a provisioning guide and an operational guide for the subcase. The provisioning/ tree contains the main playbook, collections file, wrapper script, case-specific topology and roles for the REP core, LMS portal, target network, report repository, reporting workspace, instructor console, pentest workstations, pentest tools and a contextual CYNET DC1 identity node.

This organisation is appropriate for CyberRangeCZ delivery because each layer has a clear function. The topology defines the sandbox resources and networks. The training JSON defines the learning journey. The Ansible roles turn plain virtual machines into functioning course components. The documentation explains deployment and operation. The tests provide structural validation before delivery. In that sense, the repository is more than a static lesson plan: it is a small training operations package.

3.4.4 Training design and pedagogical flow

The linear training file defines a module called **“PUC2-Sub Case 2b - Network Vulnerability Identification Training”** and organises it into three phases and eleven steps. The first phase covers instructor preparation, course creation, invitation and trainee access to material. The second phase covers reconnaissance and scanning

⁸ Self-hosted Git repository management platform.

with tools such as Nmap, OWASP ZAP and Burp Suite. The third phase covers report writing, Gitea submission, instructor review, feedback and cohort-level reporting through Grafana.

The more detailed training JSON expands this into a learner-facing CyberRangeCZ training sequence with information levels, access levels, training questions, assessment checks and a final test. It introduces the trainee to the target range 10.20.40.0/24, the target-server at 10.20.40.10, the contextual cynet-dc1 node at 10.20.40.20, and a progression from host discovery to service enumeration, web application reconnaissance, vulnerability exploitation, report submission and reflection. The estimated duration is 120 minutes, which is realistic for a guided introductory-to-intermediate vulnerability assessment lab.

The pedagogical flow is sound because it begins with low-risk orientation and connectivity checks, then moves into reconnaissance, then service identification, then vulnerability validation, and only afterwards into reporting. This order mirrors a conventional vulnerability assessment workflow. The trainee is not simply told which issues exist; they are expected to discover live hosts, identify ports, interpret banners, recognise exposed services, verify weak credentials and compile findings into a structured report.

3.4.5 Scenario content and target vulnerabilities

The target environment is deliberately vulnerable. The training materials identify a DVWA web application on port 80, phpMyAdmin on port 8080, MariaDB on port 3306 and SSH on port 22. The practical tasks guide the learner towards findings such as an outdated Apache version, default DVWA credentials, SQL injection in the DVWA SQLi module, an exposed phpMyAdmin interface, weak SSH credentials and an exposed database service. These are listed as the minimum findings expected in the reporting phase.

The target-network role implements this environment through Docker. Its defaults define DVWA on port 80, MariaDB on port 3306, phpMyAdmin on port 8080, a core services nginx portal on port 8443, DVWA default credentials and a weak SSH user. The role installs Docker, deploys a Compose file, starts the vulnerable services, waits for DVWA and phpMyAdmin health checks, creates the weak SSH user and enables password authentication in SSH as a lab-only measure.

The target Docker Compose template shows that the vulnerable design is intentional. It exposes the MariaDB database port to the host network, exposes phpMyAdmin without network restriction, runs DVWA and adds an nginx “core services” page that simulates a default or insufficiently customised service front end. The template also labels these choices as CYNET-like application, database, core services and storage-layer simulations, which helps connect the lab to enterprise architecture rather than leaving it as a generic vulnerable machine.

3.4.6 Topology and virtual infrastructure

The root topology defines a sandbox named lm5-subcase-2b-network-vuln-training. It includes eleven Ubuntu-based hosts and one Debian 12 router. The hosts are instructor-console, four REP-related backend nodes, two pentest workstations, target-server, cynet-dc1, reporting-workspace and report-repository. The single router, rep-gateway, interconnects four networks: rep-backend, rep-frontend, analytics-zone and target-zone.

The network segmentation is simple but appropriate. The rep-backend network hosts the REP scheduler, live session, quiz engine and practical labs portal. The rep-frontend network is user-accessible and contains the instructor console and two pentest workstations. The analytics-zone contains Grafana and Gitea. The target-zone contains the deliberately vulnerable target-server and contextual cynet-dc1 node. Only the frontend network is marked as user-accessible, which keeps trainees on workstations rather than giving direct access to backend, analytics or target infrastructure.

The same topology is duplicated under provisioning/case-2b/topology.yml, which is useful because the README and provisioning guide allow either the root topology or the case-specific topology to be imported. The case-specific file mirrors the root topology, including the same host names, addresses, networks and router mappings. This consistency reduces deployment ambiguity.

3.4.7 REP, LMS and course delivery components

The repository models the educational platform itself as part of the cyber range. The REP backend is represented by rep-scheduler, rep-live-session, rep-quiz-engine and rep-practical-labs. The playbook first writes internal hostnames to /etc/hosts, then applies the rep-core role to the backend hosts, then deploys LMS content on rep-practical-labs. This makes the sandbox act not only as a target network but also as a local learning delivery environment.

The rep-core role installs and starts nginx, creates REP directories, deploys a virtual host configuration, optionally installs TLS material, creates a rep system user and group, provisions an internal shared secret where configured, validates nginx syntax and conditionally checks a REP health endpoint when TLS is enabled. This is a relatively lightweight simulation or proxy layer rather than a full external REP platform implementation, but it gives the training environment internal service endpoints and consistent naming.

The lms-content role adds a second nginx virtual host on port 8080 and deploys course content under a web root with three module directories. The operational guide points trainees to <http://lms.internal:8080/> for course modules and the exercise form, and the README identifies rep-practical-labs at 10.20.10.40 as the LMS course portal. This gives the module a self-paced instructional layer rather than relying only on instructor narration.

3.4.8 Pentest workstations and toolchain

The pentest workstations are central to the trainee experience. The topology provides two Ubuntu-based pentest workstations on the frontend network, at 10.20.20.50 and 10.20.20.60. The group variables define the target range as 10.20.40.0/24, the target host as 10.20.40.10, a results directory under /opt/pentest/results, and a welcome note that reminds trainees of the LMS URL, Gitea URL, reporting URL and target range.

The pentest-tools role installs Nmap and supporting packages, including Git, curl, wget, DNS utilities, Python, Java, Nikto, OpenSSH client, sqlmap and Hydra. It also installs Docker so OWASP ZAP can run as a container, pulls the ZAP image, downloads Burp Suite Community Edition, deploys preconfigured scan scripts and verifies that Nmap, ZAP and Burp are available. This creates a practical assessment workstation with both network and web application testing capability.

The training flow explicitly uses Nmap for network reconnaissance, ZAP for web application scanning and Burp Suite for manual web application analysis. This combination is pedagogically useful because it exposes learners to the difference between network-level enumeration, automated web scanning and interactive manual validation. The repository therefore teaches tool correlation, not just one-command scanning.

3.4.9 Reporting, feedback and analytics

The repository treats reporting as a first-class learning objective. The training file requires trainees to compile a structured vulnerability report with affected host and service, vulnerability description, CVE reference where applicable, CVSS severity, proof-of-concept evidence and prioritised remediation recommendations. The report is then committed to a Gitea repository and reviewed by the instructor through Gitea comments or issues.

The report-repository role deploys Gitea through Docker, creates an administrator account, creates a cyberrange-2b organisation, creates a trainee user and creates a trainee report repository. The defaults define Gitea on port 3000, an SSH port on 2222, an admin user, an organisation name and a default trainee repository. This design is valuable because it uses version control as a professional reporting mechanism, mirroring how security reports, evidence and remediation tracking may be handled in real internal workflows.

The reporting-workspace role installs PostgreSQL and Grafana, configures a PostgreSQL datasource named `rep_postgresql`, registers a dashboard provider and deploys a dashboard titled **“Network Vuln Overview”**. The operational guide describes Grafana as the instructor’s cohort metrics dashboard, showing report submission status, average findings per trainee, CVSS distribution, identification accuracy and traffic-light status.

The repository also includes an export script for instructor use. That script expects a Gitea API token, exports trainee repository metadata, fetches open feedback issues and generates a cohort summary JSON file. This is a practical addition because it gives instructors a path to extract results after the session rather than only reviewing them manually in the UI.

3.4.10 CYNET DC1 and identity-layer simulation

The `cynet-dc1` host is a contextual identity and access node in the target zone. The topology places it at 10.20.40.20, and the training JSON introduces it as a second live host discovered during reconnaissance. The playbook deploys the `cynet-dc1` role after the pentest workstation configuration and marks it with `ignore_errors: true`, suggesting that it is helpful to the scenario but not necessarily critical to the core DVWA/target-server learning path.

The `cynet-dc1` role deploys OpenLDAP and phpLDAPadmin through Docker and creates a weak management SSH user. Its defaults explicitly describe anonymous bind as a vulnerability, phpLDAPadmin exposed over HTTP as a vulnerability, and weak SSH management credentials as a vulnerability. This enriches the target-zone narrative: the lab is not only a single vulnerable web application but a small CYNET-style infrastructure segment with application, database, management and identity-layer weaknesses.

3.4.11 Provisioning workflow and deployment process

The provisioning guide explains that deployment has two phases: importing the topology into KYPO/CRCZ and then configuring the machines with Ansible. It instructs operators to upload the case topology, wait for the sandbox machines to become reachable, duplicate `inventory.sample` to `inventory.ini`, export credentials as environment variables or use Ansible Vault, install Ansible dependencies and run the wrapper script.

The main playbook is well structured. It first configures internal hostname resolution across all nodes, then configures REP core services, deploys the LMS portal, deploys vulnerable target services, deploys the Gitea report repository, prepares the Grafana reporting workspace, personalises the instructor console, configures pentest workstations and finally deploys the CYNET DC1 identity services. This ordering reflects the dependencies of the training environment: names and base services first, target and tools next, then reporting and instructor-facing support.

The wrapper script `provisioning/run_playbook.sh` is a useful operational guardrail. It checks for required commands, verifies the collections file, playbook and inventory, installs Ansible collections and then runs the playbook. It also explicitly advises operators to use the wrapper rather than calling `ansible-playbook` directly on KYPO/CRCZ, to avoid missing modules.

3.4.12 Validation and quality controls

The repository includes an explicit validation workflow. The README instructs users to install `requirements-dev.txt` and run `pytest`, and states that the tests verify the structure and step sequence of `training_linear.json` and that topology files reference only defined hosts, networks and routers. The development requirements are minimal: `pyyaml`, `pytest`, `jinja2` and `passlib`.

The test suite is more extensive than a superficial syntax check. It validates that the training file has required keys, non-empty modules, phases and activities, sequential step numbering, exactly three subcase phases and exactly eleven steps. It also validates topology consistency, confirms that `target-zone`, `target-server`, `pentest-workstation-01` and `report-repository` exist, and checks several Ansible role assumptions, including instructor shortcut validation, Grafana health-check behaviour, Grafana repository defaults, pentest target range defaults, target-network defaults and Gitea defaults.

This is a notable strength. Many cyber range repositories rely entirely on manual review. Here, the authors have added regression-style checks for the training structure, topology and selected role details. The tests do not prove that a full deployment will succeed, but they do reduce the risk of broken references, missing phases or inconsistent role defaults.

3.4.13 Credential and secret management

The repository shows awareness of credential handling but also includes lab-only credentials that must be treated carefully. The README tells operators to replace password placeholders in `inventory.sample` using Ansible Vault files or exported environment variables and explicitly warns not to commit real credentials. The

inventory sample follows that model by using lookup ('env', ...) expressions for the Ansible passwords of the REP, instructor, pentest, target, reporting and report repository hosts.

At the same time, several defaults are intentionally weak because the environment is a lab. The pentest workstation group variables set the trainee password to `qwerty!23`, the target role defines weak SSH credentials, the Gitea defaults include concrete admin and trainee passwords, and the CYNET DC1 role includes default LDAP and SSH credentials. These are acceptable for an isolated cyber range if instructors understand their purpose, but they should never be reused in any real environment.

3.4.14 Operational inconsistencies and caveats

There are several small but important consistency issues. The operational guide states that the target SSH weak credentials are `labuser / Password123`, and the provisioning guide repeats `Password123` for the target SSH check. However, the target role defaults define the weak SSH password as `labuser`, and the training JSON also teaches that the SSH account uses a password equal to the username. This should be corrected, because credential mismatch can derail a live exercise.

A second inconsistency concerns Ansible collections. The operational guide says the prerequisites are `community.general` and `community.docker`, but the repository's `provisioning/collections.yml` declares `ansible.windows`, `community.general` and `community.windows`, and does not declare `community.docker`. Because the `cynet-dc1` role uses `community.docker.docker_login`, this mismatch is worth resolving before delivery.

A third caveat concerns Gitea repository organisation. The instructor workflow describes creating one repository per trainee under the `cyberrange-2b` organisation, and the export script queries repositories under that organisation. However, the `report-repository` role creates a trainee repository through the authenticated trainee user endpoint, while the detailed training JSON asks the trainee to clone `git/cynet-report.git`. This may still work depending on how Gitea resolves repository ownership, but the intended ownership model should be clarified so that instructor review, trainee submission and export automation all point to the same repository structure.

There is also a minor documentation gap in credential variables. The README lists required Ansible password variables for the REP nodes, instructor console, pentest workstations, target server, reporting workspace and report repository, but the inventory sample also references `ANSIBLE_PASSWORD_CYNET_DC1`. Since `cynet-dc1` is now part of the topology, that variable should be included consistently in the README and provisioning guide.

3.4.15 Security posture and lab-only assumptions

The repository is deliberately unsafe by design, because its purpose is to teach vulnerability identification. It exposes intentionally weak services, default credentials, database ports, `phpMyAdmin`, vulnerable DVWA functionality and lab-only password SSH access. The operational guide correctly states that all vulnerable services and weak credentials are intentional, that the target zone is isolated from the REP backend, and that scanning outside `10.20.40.0/24` should be prohibited through firewall rules in production deployments.

The main security requirement is therefore environmental isolation. This repository should be run only inside a CyberRangeCZ/KYPO sandbox or an equivalent isolated lab. It should not be exposed to the internet or reused as a real internal platform. The vulnerable services are useful because they are controlled, predictable and aligned with the learning outcomes; outside that context, the same characteristics would be operational weaknesses.

3.4.16 Strengths of the repository

The repository's first major strength is its coherence as a training package. It combines topology, provisioning, course content, trainee workstations, vulnerable targets, reporting infrastructure, instructor support and validation tests. This is stronger than a simple "vulnerable VM plus README" approach, because the whole learner journey is represented from invitation to assessment feedback.

Its second strength is the practical toolchain. Learners work with Nmap, OWASP ZAP, Burp Suite Community, Nikto, sqlmap, Hydra, Git and Gitea. The module therefore connects scanning, manual validation and professional reporting. That is well aligned with the stated aim of training staff in penetration testing and vulnerability assessment.

Its third strength is the assessment design. The training JSON includes formative checks, final assessment questions and a required report submission. The instructor guide uses Gitea review and Grafana cohort dashboards, while the export script provides a way to capture results after delivery. This gives instructors multiple forms of evidence: scan outputs, quiz answers, report content, Gitea feedback and cohort summaries.

3.4.17 Suitability for training delivery

Im5-1b is well suited for a self-paced or instructor-supported module on network reconnaissance, service enumeration, basic web application vulnerability assessment and reporting. It would work especially well for junior security analysts, junior penetration testers, SOC staff learning attacker-perspective reconnaissance, system administrators learning how misconfigurations appear to testers, or students who need a practical bridge between theory and hands-on assessment.

It is less suitable for advanced red-team operations or full incident response training. The exploitation path is intentionally guided, the target services are deliberately vulnerable, and the reporting requirements are educational. That makes it effective for structured learning, but less representative of a mature enterprise penetration test where stealth, scoping complexity, authentication boundaries, change windows, evidence handling and stakeholder communication are broader.

3.4.18 Final assessment

Overall, NG-SOC-eu/Im5-1b is a focused and useful CyberRangeCZ/KYPO training repository for **PUC2-Sub Case 2b: Network Vulnerability Identification Training**. Its value lies in the integration of a CYNET-like target zone, two trainee pentest workstations, an LMS portal, a Gitea report repository, a Grafana reporting workspace, instructor console support, Ansible provisioning and automated validation tests.

From an educational perspective, the repository is strongest as a vulnerability-assessment workflow exercise. It teaches learners to move from reconnaissance to scanning, from scanning to vulnerability validation, and from validation to documented remediation advice. From an engineering perspective, it is reasonably well structured and test-aware but would benefit from cleaning up the documented credential values, Ansible collection requirements and Gitea repository workflow. From a security perspective, its weaknesses are intentional, but that intention must be respected: this repository belongs in an isolated cyber range and should not be deployed as a live or internet-facing environment.

We also reached an agreement with the CYNET partner regarding their simulated infrastructure:

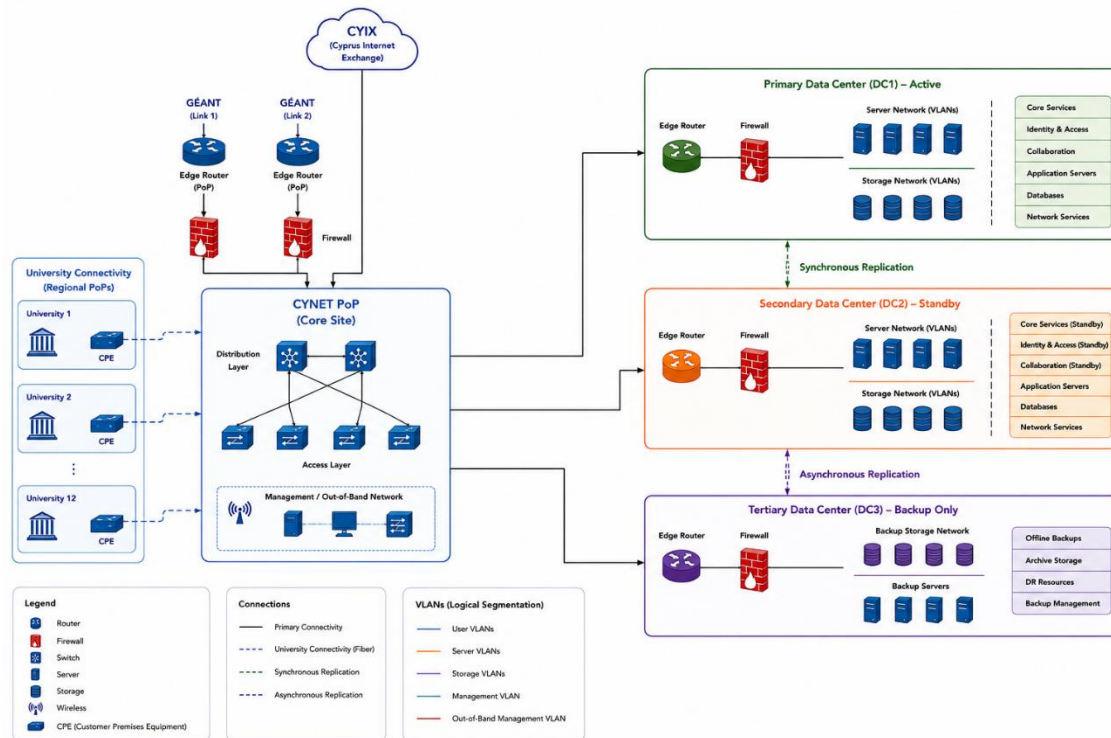


Figure 70 CYNET-Like Infrastructure

3.4.19 Scenario status and public-release readiness

This scenario is pedagogically strong because it connects vulnerability discovery, scanning, service enumeration, reporting and instructor review. It is suitable for teaching junior analysts how to use Nmap, OWASP ZAP, Burp Suite Community, Nikto, sqlmap, Hydra and Gitea-based reporting within a controlled vulnerable infrastructure.

Table 21 Scenario status and public-release readiness

Scenario name	Repository / resource	Machine-readable format	Validation state	Deployment constraints	Public-release readiness
LM5 Network Vulnerability	https://github.com/NG-SOC-eu/lm5-1b	JSON training definition, topology	Automated local validation	Requires CyberRangeCZ/KYP O, vulnerable target	Conditionally ready after resolving

Identification Training 1b		YAML, Ansible provisioning, Docker Compose configuration, validation tests	exists for training structure, topology consistency and selected role assumptions	services, pentest workstations, reporting services and controlled target-zone isolation	credential inconsistencies, inventory gaps and collection dependency issues
----------------------------	--	--	---	---	---

3.4.20 Public-dissemination hygiene review

Table 22 Public-dissemination hygiene review

Hygiene items	Assessment	Required public-release action
Default credentials	The scenario intentionally includes vulnerable services and default-style lab credentials.	Avoid publishing exact values in the main deliverable; keep them in learner material only where essential.
Weak passwords	Weak SSH, DVWA, Gitea and directory-style credentials are part of the exercise logic.	Add a warning that all weak credentials are deliberate and must remain isolated to the cyber range.
Credential inconsistency	The guide and target defaults appear to describe weak SSH access differently.	Align the learner instructions, target defaults and validation tests before release.
Dependency caveats	Collection and Docker-related dependencies require clarification.	Update requirements so provisioning instructions match the roles actually used.
Public scanning safety	The exercise teaches active scanning and exploitation validation.	State clearly that scanning is restricted to the target subnet provided by the scenario.

3.4.21 YAML/JSON artefact inventory

Table 23 YAML/JSON artefact inventory

Artefact	Format	Location / role	Release note
Training definition	JSON	Detailed network vulnerability training definition	Should remain aligned with the eleven-step learner flow.
Linear training file	JSON	training_linear.json	Used for CyberRangeCZ training import and sequencing.
Sandbox topology	YAML	topology.yml	Must define the REP, analytics and target zones without overlap.
Provisioning playbooks	YAML / Ansible	provisioning/ roles and playbooks	Should avoid embedded reusable credentials.

Vulnerable target definition	YAML / Docker Compose	Target-server service deployment	Must be labelled as intentionally vulnerable.
Reporting workflow	JSON / service configuration	Gitea and Grafana-related components	Should use synthetic reports and demonstration accounts only.
Validation tests	Python	Repository test folder	Should be extended to cover credential consistency and dependency completeness.

3.5 KYPO/CRCZ LM8 Phishing Attack Training Scenario Subcase 1a⁹ (status: testing on execution)

3.5.1 Source code

The KYPO/CRCZ project is imported from a public GitHub repository maintained by the NG-SOC consortium:

Link to GitHub: <https://github.com/NG-SOC-eu/lm8-1a>

README: <https://github.com/NG-SOC-eu/lm8-1a/blob/main/README.md>

Training Definition: https://github.com/NG-SOC-eu/lm8-1a/blob/main/puc2_sub_case_2a_phishing_training.json

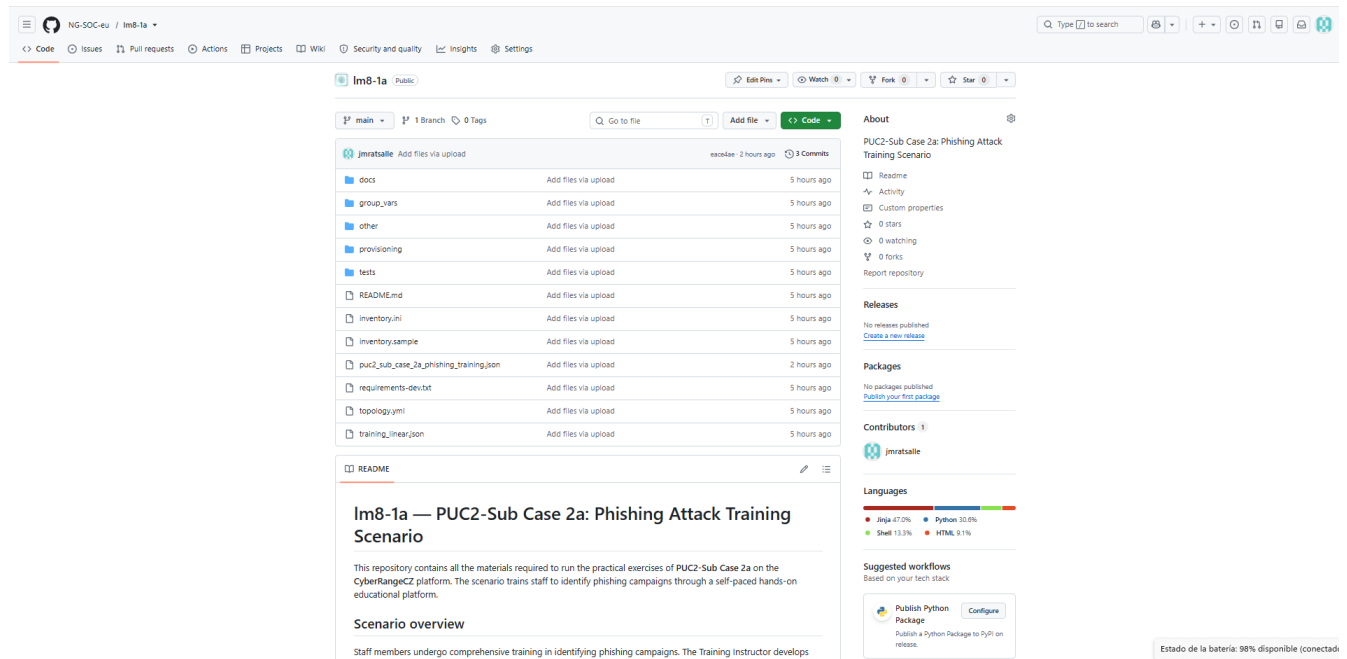
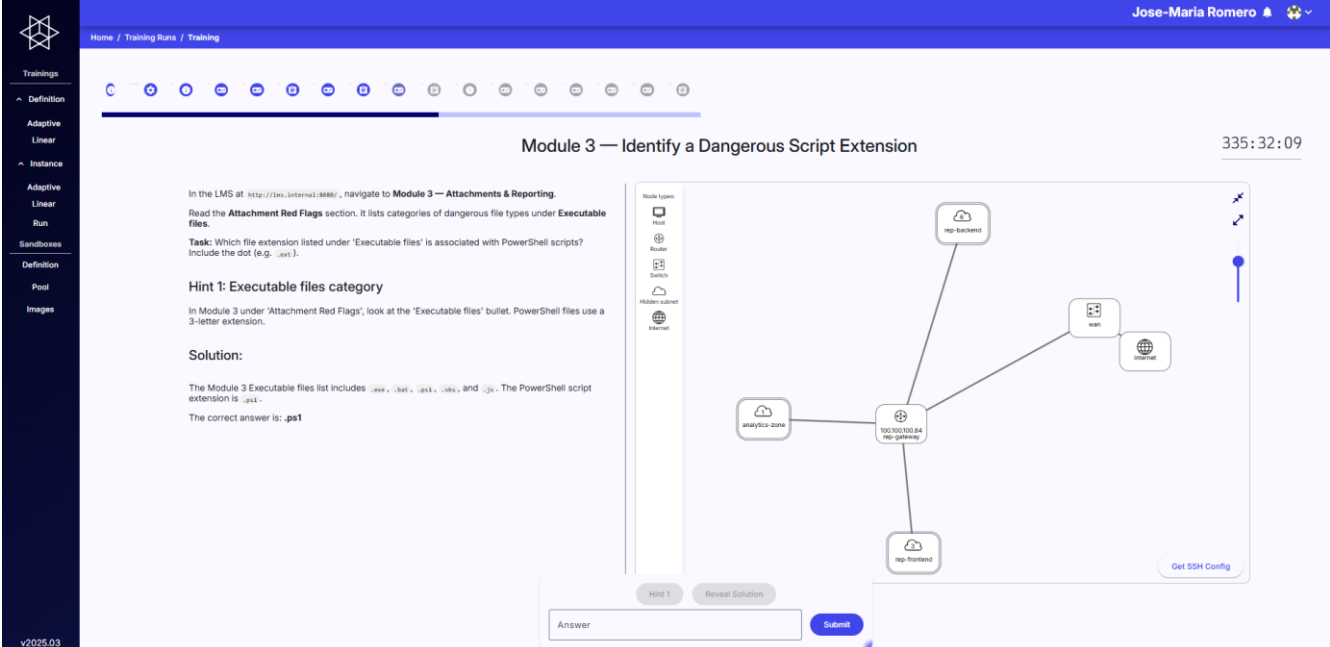


Figure 71 KYPO/CRCZ LM8 Phishing Attack Training Scenario Subcase 1a source code on GitHub

⁹ Aligned to consortium's UML of CYNET-UC-2a.

The README states that the repository contains all materials required to run the practical exercises of **PUC2-Sub Case 2a** on the CyberRangeCZ platform. The scenario trains staff to identify phishing campaigns through a self-paced, hands-on educational platform. Its stated learning targets are practical and user-facing: scrutinising sender information, analysing email content for red flags, verifying attachments and reporting suspicious emails through organisational procedures.

This is therefore not an incident response platform in the narrow technical sense, nor a malware-analysis range, nor a red-team exercise. It is best understood as an awareness and first-response training package that uses realistic phishing infrastructure, sandboxed mail delivery, LMS theory modules, trainee Windows workstations, automated scoring and instructor dashboards to teach phishing recognition and reporting behaviour.



The screenshot displays the NGSOC training interface. The top navigation bar shows 'Home / Training Runs / Training' and the user 'Jose-Maria Romero'. The sidebar on the left lists various training components. The main content area is titled 'Module 3 — Identify a Dangerous Script Extension' with a timer at 335:32:09. The task instructions refer to the LMS at <http://lms.internal.8888/> and Module 3 — Attachments & Reporting. The task asks for the file extension associated with PowerShell scripts. A hint points to the 'Executable files category'. The solution states that PowerShell scripts use a 3-letter extension, and the correct answer is `.ps1`. A network diagram on the right shows a central '100.100.100.84 nsg-gateway' connected to 'nsg-backend', 'nsg-frontent', 'analystico-zone', 'mail', and 'internet'.

Figure 72 Level 09 - Module 3 — Identify a Dangerous Script Extension

3.5.2 Overall purpose of the project

The repository's purpose is to train staff in recognising and reporting phishing campaigns. The scenario is built around a simulated campaign in which an instructor prepares a self-paced phishing course, launches a GoPhish campaign, delivers emails through an internal mail relay, and uses platform scoring to evaluate each trainee's behaviour. The training flow is explicitly divided into three phases and eight steps: training setup, trainee execution, and assessment with feedback.

The learning design is deliberately focused on human-centred detection rather than deep technical compromise analysis. Trainees are expected to detect display-name and domain spoofing, urgency and fear language, masked links, unsafe attachments and reporting requirements. The detailed training definition expands this into a 30-level learner journey covering LMS theory modules, Mailpit inbox analysis, GoPhish link inspection, detection report submission, automated scoring, feedback review and cohort metrics.

This makes the repository suitable for awareness training, user reporting discipline, helpdesk or junior SOC onboarding, and general staff cyber hygiene exercises. It is less suitable as a standalone technical incident response lab if the goal is forensic imaging, SIEM correlation, endpoint investigation, malware reverse engineering or containment engineering.

3.5.3 Repository structure and content organisation

The repository is organised into a small but coherent cyber range package. The root contains the README, topology.yml, training_linear.json, the detailed training definition puc2_sub_case_2a_phishing_training.json, inventory files, development requirements, group variables, documentation, provisioning roles and tests. The README identifies the key operational files: the sandbox topology, the linear learning sequence, the Ansible playbook, the scenario-specific provisioning directory, the detailed operational guide, trainee group variables and the inventory template.

The provisioning/ directory is the operational centre of the project. Its README maps host groups to training functions: REP backend microservices, LMS course content, GoPhish, the sandboxed mail relay, Grafana/PostgreSQL reporting, the instructor console and Windows trainee workstations. This makes the repository more complete than a static Markdown awareness lesson because it defines the training platform, the mail flow, the user machines and the reporting layer.

The other/ directory contains older or alternative topology material. One file describes a generic CyberRangeCZ core component model with instructor console, random education platform, trainee workstations, reporting workspace and simulators, while another older topology describes an unrelated-looking attacker/SOC/user-PC/internal-server environment. These files appear to be supporting or legacy artefacts rather than the active topology used for the PUC2 Sub Case 2a deployment.

3.5.4 Training design and pedagogical flow

The main learning sequence in training_linear.json defines **“CyberRangeCZ Practical Modules”** for PUC2-Sub Case 2a and uses a three-phase structure. In the setup phase, the instructor configures GoPhish email templates, simulated landing pages, campaign parameters and LMS theory modules. In the execution phase, trainees access the LMS, complete awareness modules and receive a simulated phishing email. In the assessment phase, the platform records trainee behaviour, scores the results, sends personalised feedback and gives the instructor cohort-level metrics.

The more detailed training JSON is particularly important because it turns the scenario into a learner-facing sequence. It starts with workstation access, then introduces three theory modules: sender analysis, content red flags, and attachments and reporting. It uses a mixture of information levels, access levels, training tasks and assessment questions. The learning outcomes include identifying phishing indicators in headers and body content, detecting social-engineering tactics, safely inspecting attachments and links, applying reporting protocols and interpreting automated feedback.

The practical sequence is well designed for awareness training. Trainees first learn concepts, then apply them to a live simulated email in their lab inbox. They are asked to inspect the actual sender domain, identify the first urgency word in the message body, copy or hover over a GoPhish link without clicking it, identify the rid tracking parameter, count urgency cues and submit a detection report through the LMS practical exercise. The training explicitly warns that clicking the phishing link is tracked and affects the no-click bonus.

The assessment phase is also stronger than a simple quiz. It asks trainees to perform a full email analysis across sender domain, Reply-To header, embedded links, body language and greeting style. The reference solution identifies three actual phishing indicator categories in the scenario: a spoofed .net sender domain instead of the legitimate .com, an embedded URL pointing to phishing-simulator.internal, and urgency/fear language. This is pedagogically useful because the exercise also teaches that some checks may come back clean and should not be falsely flagged.

3.5.5 Scenario realism and phishing content

The scenario is realistic enough for user-awareness training without introducing real malware. The LMS content teaches display-name spoofing, typosquatting, Reply-To mismatches, suspicious URLs, urgency and fear tactics, generic salutations, dangerous attachments, double extensions and safe reporting channels. The practical exercise asks trainees to inspect a simulated email, avoid unsafe clicks, document red flags and submit a detection report.

The simulated phishing campaign is built around a plausible IT security compliance lure. The example GoPhish campaign configuration uses an “IT Security Compliance Notice”, a credential-capture-style landing page, a MailHog/Mailpit relay profile and a redirect back to the learning portal after capture. The landing-page text makes clear that this is a simulated phishing exercise, which is appropriate for a controlled awareness lab.

The scenario’s main phishing indicators are deliberately chosen for accessibility. They are not obscure forensic artefacts; they are user-recognisable signs such as a suspicious sender domain, urgency language, masked links, tracking parameters and official-looking but questionable policy references. This makes the package particularly suitable for broad staff populations, not only for technical analysts.

3.5.6 Topology and virtual infrastructure

The root topology.yml defines a sandbox named lm8-subcase-2a-phishing-training. It contains ten hosts and one router. The Linux hosts are instructor-console, four REP-related nodes, phishing-simulator, mail-relay and reporting-workspace. The two trainee machines are Windows 10 workstations managed through WinRM. The only router is rep-gateway, using a Debian 12 image.

The network design is simple and appropriate for the training goal. The rep-backend network at 10.20.10.0/24 hosts LMS, REP, GoPhish and mail relay services. The rep-frontend network at 10.20.20.0/24 contains the instructor console and trainee Windows workstations and is marked as user-accessible. The analytics-zone at 10.20.30.0/24 contains the reporting workspace. This segmentation separates trainee interaction from backend delivery and analytics while keeping the environment understandable for an awareness course.

The detailed guide presents the same architecture in operational terms. It identifies rep-practical-labs as the LMS portal on port 8080, phishing-simulator as the GoPhish host with admin access on port 3333 and phishing pages on port 80, mail-relay as the SMTP and web inbox service, and reporting-workspace as the Grafana/PostgreSQL reporting node.

3.5.7 LMS course portal

The LMS portal is served from rep-practical-labs and is implemented by the lms-content role. This role creates the LMS web root, module directories and feedback directory, deploys a course index page, configures an nginx virtual host on port 8080 and validates that the portal responds locally.

The course content is substantial for a lightweight range package. It provides an overview, learning objectives, scoring model, links to the lab inbox, three theory modules and a practical detection exercise. The scoring model shown to trainees is the same one used by the later scoring engine: 40% detection accuracy, 30% incident report completeness, 20% time to detection and report, plus a 10% no-click bonus.

The LMS is therefore not merely a static web page. It is the trainee's central learning space, exercise guide, reporting form and feedback landing area. Its content mirrors the learning outcomes in the JSON training definition, which gives the repository good alignment between platform-level training flow and the material actually presented to the learner.

3.5.8 GoPhish phishing simulator

The phishing simulator role deploys GoPhish through Docker Compose. It installs Docker, configures the Docker repository and registry mirror, deploys a GoPhish configuration with TLS disabled for the lab, pulls and tags the GoPhish image, starts the service, waits for the admin port and records initial administrator credentials for instructor use. It also extracts the GoPhish API key from the container database and uses it to pre-configure a MailHog/Mailpit SMTP sending profile.

The defaults expose GoPhish admin on port 3333 and phishing pages on port 80. The default sender is security@company-corp.net, which intentionally differs from the legitimate .com domain used in the course material. This supports the sender-domain mismatch exercise and makes the simulated email internally consistent with the learning objectives.

The GoPhish configuration disables TLS on both the admin and phishing servers. That is acceptable for an isolated CyberRangeCZ lab but should not be interpreted as a production deployment pattern. The repository itself frames the content as educational, and the operational guide instructs the instructor to change the GoPhish password after first login.

3.5.9 Mail relay and sandboxed email delivery

The mail relay is presented in some documentation as MailHog, but the actual role defaults use the axllent/mailpit:latest image and deploy a container named mailpit. The service exposes SMTP on port 1025 and

a web UI on port 8025. This difference is operationally minor because Mailpit is a MailHog-like sandbox inbox, but it is a documentation consistency issue: the README and guide mostly say MailHog, while trainee-facing content and role implementation often say Mailpit.

The mail relay is an important safety feature. The provisioning README states that all emails remain inside the sandbox and do not reach the internet. The training material reinforces this by describing the lab inbox as a sandboxed relay where the GoPhish campaign delivers exactly one simulated phishing email per trainee.

This design is appropriate for a cyber range because it allows realistic email behaviour without the risk of accidentally sending phishing content outside the controlled environment. It also gives trainees a browser-accessible inbox, so the exercise does not depend on configuring full email clients on Windows workstations.

3.5.10 Reporting workspace, scoring and feedback

The reporting workspace is one of the repository's stronger components. It uses PostgreSQL to store trainee scores and Grafana to present cohort metrics. The reporting defaults define a `rep_reporting` datasource, a REP Overview dashboard and a health check against Grafana's API. The role installs PostgreSQL, creates the reporting database, creates the reporting user, creates a `trainee_scores` table and deploys scoring and feedback scripts under `/opt/rep-scoring`.

The scoring engine fetches GoPhish campaign results, computes per-trainee scores and upserts them into PostgreSQL. Its model matches the training design: detection accuracy is worth 40 points, report completeness 30, time to report 20 and no-click behaviour 10. It also assigns traffic-light status: green from 70 upwards, amber from 40 to 69 and red below 40.

The feedback engine reads the scoring table, sends personalised HTML feedback messages through the sandbox mail relay and writes feedback pages that can be published to the LMS. It includes score breakdown, missed indicators and recommended study areas. This is a valuable feature because it closes the learning loop: trainees do not merely complete an exercise; they receive feedback tied to their actual behaviour.

The Grafana dashboard template provides detection rate, click-through rate, average score, number of trainees scored, per-trainee score breakdown, score distribution and component averages. This gives the instructor a useful cohort view of risk behaviour and training effectiveness.

3.5.11 Instructor console

The instructor console role creates an instructor user, prepares a workspace, generates an SSH key pair for publishing LMS content, deploys editable LMS module content, installs a publishing script, configures tmux and exposes shell shortcuts. The shortcuts include opening GoPhish, the LMS portal, the mail inbox and Grafana, showing GoPhish credentials, scoring a campaign, delivering feedback, publishing feedback and publishing LMS content.

This is a practical design choice. In live training sessions, instructors need fast access to the phishing simulator, mail relay, reporting workspace and LMS content, and the shortcuts reduce manual typing and operational friction. The role also validates tmux configuration and verifies that generated shortcuts are executable, which is a small but useful quality-control step.

There is, however, a lab-only security caveat. The documentation states that the ubuntu user password on the instructor console is hard-coded as Instructor#Lab2a, stored as a pre-generated SHA-512 hash in the instructor-console task. The guide explicitly states that this is acceptable only for a disposable lab environment and must never be reused in real or shared infrastructure.

3.5.12 Windows trainee workstations and REP collector

The trainee workstations are Windows 10 hosts accessible from the frontend network. Their group variables define the trainee learning portal, lab inbox, phishing landing page and reporting dashboard links, and write a welcome note under C:\Labs. The same file also sets a concrete REP collector ingestion token, rep-core-trainee-collector-7b92de11, rather than leaving only the default placeholder.

The trainee-workstation role deploys a REP collector configuration and PowerShell script, installs NSSM as a Windows service wrapper, creates shortcuts, starts the REPCollector service and validates both service status and heartbeat log entries. Its default configuration explicitly warns that the ingestion token should be overridden before deployment, and the task file asserts that the default changeme token is not still in use.

The Windows base role is deliberately permissive for lab reliability. It disables Windows Update and automatic reboot, enables RDP and WinRM, opens management firewall rules, completely disables the Windows firewall, changes the windows user password to qwerty!23, and writes internal hostnames to the Windows hosts file. These actions make sense in a controlled, disposable range, but they are not safe production practices.

3.5.13 Provisioning workflow

The main Ansible playbook first verifies that the ansible.windows collection is available, then writes internal hostname mappings on Linux hosts, configures Windows base settings, deploys REP core services, adds the LMS portal, deploys GoPhish, deploys the mail relay, prepares the Grafana/PostgreSQL reporting workspace, personalises the instructor console, authorises the instructor SSH key on the LMS host and finally configures the Windows trainee workstations.

The wrapper script provisioning/run_playbook.sh checks for required commands, validates that the playbook, collection requirements and inventory file exist, installs Ansible collections from provisioning/requirements.yml, and then runs the playbook. The script explicitly advises users to use the wrapper rather than calling ansible-playbook directly on KYPO/CRCZ, to avoid missing modules.

The collections declared are ansible.windows, community.general and community.windows, which are consistent with the use of Windows modules, NSSM service handling and general Linux provisioning.

3.5.14 Validation and quality controls

The README provides a validation workflow using `pip install -r requirements-dev.txt` followed by `pytest`, and states that tests verify the structure and sequence of `training_linear.json` and check that topology files reference only defined hosts, networks and routers.

The actual test suite validates the training JSON structure, verifies sequential step numbering, checks topology consistency in `provisioning/case-2a/topology.yml`, and includes role-specific tests for instructor console shortcut validation and Grafana repository and health-check behaviour. It also checks that Grafana repository setup precedes package installation.

This is a meaningful strength. Many training repositories contain only Markdown and YAML, but this one includes automated checks for structural drift. The tests do not prove that the full sandbox will deploy successfully, and they do not perform end-to-end GoPhish, Mailpit, LMS or Grafana validation. They do, however, catch a useful class of mistakes before instructors try to run the training.

3.5.15 Credential management and operational caveats

The repository shows awareness of credential management, but it also contains lab-only shortcuts. The README instructs operators to replace password placeholders in `inventory.sample` using Ansible Vault files or exported environment variables and warns not to commit real credentials. The inventory files use lookup (`'env', ...`) expressions for host passwords.

There are several caveats. First, the `inventory.sample` file does not include the `phishing_simulator` and `mail_relay` groups, even though the playbook deploys those hosts and the checked-in `inventory.ini` does include them. A user who follows the README literally and copies `inventory.sample` may need to add those groups before provisioning will cover the GoPhish and mail relay hosts correctly.

Second, both inventory files include broader NG-SOC groups such as `ng_soc`, `ng_siem`, `ng_soar`, `cti_ss`, `cicms`, `playbook_library` and `telemetry_feeder`, but those hosts are not present in the active root topology. This suggests reuse from a wider NG-SOC architecture or earlier scenarios. It is not harmful if ignored, but it may confuse operators trying to understand the minimum viable deployment for this specific phishing-awareness sandbox.

Third, the repository uses several explicit lab credentials or lab-only defaults. Grafana defaults to `admin/admin`, the instructor console password is documented as a hard-coded lab password, Windows trainee machines are set to `qwerty!23`, and the trainee group variables contain a concrete collector token. These are acceptable for a disposable CyberRangeCZ sandbox only if the environment is properly isolated.

3.5.16 Strengths of the repository

The principal strength of `lm8-1a` is coherence. The repository aligns its README, topology, training JSON, LMS content, GoPhish deployment, mail relay, scoring engine, feedback generator and Grafana dashboard around

the same educational goal: teaching users to identify and report phishing attempts. This makes it stronger than a simple awareness slide deck or a standalone GoPhish deployment.

A second strength is the closed feedback loop. The platform does not merely send a phishing email and record clicks. It teaches theory, asks trainees to perform structured analysis, records GoPhish events, scores behaviour, stores results in PostgreSQL, visualises cohort metrics in Grafana and generates personalised feedback. This is exactly the kind of loop that improves awareness training because it connects action, consequence and remediation.

A third strength is operational repeatability. The scenario can be rebuilt from topology and Ansible roles, and the tests give maintainers some confidence that the main training sequence and topology references have not broken. The instructor console shortcuts and helper export script also make repeated classroom delivery easier.

3.5.17 Suitability for training delivery

Im8-1a is well suited for instructor-led or self-paced phishing awareness training in a cyber range. It is especially appropriate for staff awareness, junior analyst onboarding, helpdesk teams, compliance training and exercises where the desired outcome is faster and more accurate reporting of phishing emails. The use of Windows trainee workstations, an internal inbox, a realistic GoPhish campaign and a structured LMS makes the exercise accessible to non-specialists while still exposing them to real security-training tooling.

It is less suitable for advanced technical audiences if used alone. More experienced SOC or incident response trainees may find the main technical challenge too simple because the focus is not on log triage, forensic acquisition, malware analysis, containment or enterprise-scale investigation. For those audiences, this repository would work best as an introductory module before progressing to the more technical LM8 incident-response and forensics subcases.

3.5.18 Final assessment

Overall, NG-SOC-eu/Im8-1a is a focused and practically useful CyberRangeCZ/KYPO training repository for **PUC2-Sub Case 2a: Phishing Attack Training Scenario**. Its value lies in the integration of self-paced LMS theory, GoPhish simulation, sandboxed mail delivery, Windows trainee workstations, structured detection reporting, automated scoring, personalised feedback and instructor-facing Grafana analytics.

From an educational perspective, the repository is strongest as a phishing-awareness and first-reporting exercise. From an engineering perspective, it is reasonably mature for a cyber range content package because it includes Ansible provisioning, role separation, helper scripts and automated validation tests. From a security perspective, it is intentionally lab-oriented and contains several disposable-environment shortcuts, so it should only be deployed inside an isolated CyberRangeCZ/KYPO sandbox or an equivalent controlled environment.

3.5.19 Scenario status and public-release readiness

This scenario is well suited for awareness, detection and reporting training because it combines theory, simulated phishing delivery, sandboxed mail handling, trainee workstation activity, automated scoring and

personalised feedback. Its value lies in connecting user behaviour, phishing indicators, reporting speed, instructor analytics and practical response coordination.

Table 24 Scenario status and public-release readiness

Scenario name	Repository / resource	Machine-readable format	Validation state	Deployment constraints	Public-release readiness
LM8 Phishing Attack Training Scenario Subcase 1a	https://github.com/NG-SOC-eu/lm8-1a	JSON training definition, topology YAML, Ansible provisioning, GoPhish campaign configuration, reporting dashboards and scoring data	Local validation exists for training structure, topology consistency and selected reporting/instructor assumptions	Requires LMS portal, GoPhish simulator, sandbox mail relay, instructor console, Windows trainee workstations and analytics workspace	Conditionally ready after mail-relay documentation, inventory grouping and lab-credential caveats are cleaned

3.5.20 Public-dissemination hygiene review

Table 25 Public-dissemination hygiene review

Hygiene items	Assessment	Required public-release action
Default credentials	Instructor, Grafana, Windows and simulator access assumptions exist for lab delivery.	Replace exact values with placeholders in public text and keep operational values in protected deployment notes.
Weak passwords	Weak Windows and service credentials are used for controlled accessibility.	Add a lab-only statement and confirm that these credentials are never reused outside the sandbox.
Collector token	A concrete collector token is referenced for trainee telemetry.	Generate per deployment or explicitly mark it as a non-secret lab token.
Mail relay naming	Documentation appears to mix MailHog-style language with a Mailpit-based implementation.	Standardise terminology and port references before public release.
Phishing safety	The phishing content is simulated and sandboxed.	Confirm that all domains, links, mailboxes and payloads are non-public and training-only.

3.5.21 YAML/JSON artefact inventory

Table 26 YAML/JSON artefact inventory

Artefact	Format	Location / role	Release note
Training definition	JSON	Phishing training scenario definition	Must remain aligned with scoring and feedback logic.
Sandbox topology	YAML	Scenario topology	Should clearly separate backend, frontend and analytics zones.
Provisioning playbooks	YAML / Ansible	LMS, GoPhish, mail relay, instructor console and trainee roles	Must use placeholders or vault-managed secrets.
GoPhish campaign data	JSON / simulator configuration	Phishing simulator	Should include only synthetic sender domains and templates.
Scoring data model	SQL / JSON / scripts	Reporting workspace	Should contain no real trainee personal data in public examples.
Dashboard configuration	JSON	Grafana reporting workspace	Safe for release if populated with synthetic data only.
Learner feedback templates	HTML / JSON-supported content	Feedback engine	Must avoid real identities or operational indicators.

3.6 KYPO/CRCZ LM5 Malware Attack Detection & Response Training 1c (status: validation)

3.6.1 Source code

The KYPO/CRCZ project is imported from a public GitHub repository maintained by the NG-SOC consortium:

Link to GitHub: <https://github.com/NG-SOC-eu/lm5-1c>
 README: <https://github.com/NG-SOC-eu/lm5-1c/blob/main/README.md>

The subcase 2c is presented through a video tutorial where the tools and its functionalities are presented. Moreover, some questions are proposed for the consolidation of the knowledge and skills.

The lm5-1c scenario exposes trainees to a representative malware detection and response toolchain rather than a single isolated product. The defensive monitoring layer is built around **Wazuh**, used as the NG-SIEM component for endpoint telemetry ingestion, file-integrity monitoring, malware-alert generation and correlation. The endpoint hosts run the **Wazuh agent**, which monitors download and temporary directories so that the benign EICAR-equivalent payload produces observable file-hash telemetry. Threat intelligence enrichment is provided through **MISP**, acting as the CTI-SS component for malware IoCs, hash enrichment and intelligence sharing. Incident case handling is represented by **DFIR-IRIS**, used as the CICMS component for opening and enriching the incident case with SIEM and CTI context. Automated containment is represented by **NG-SOAR orchestration**, supported by playbooks such as host isolation, malicious IP blocking, credential reset, quarantine and patching. The SOC stack is containerised with **Docker Compose**, with **Portainer** included for container-operations convenience, while the attacker side uses a controlled phishing and payload-delivery mechanism that generates a safe EICAR-equivalent artefact rather than real malware. The module therefore gives learners practical

exposure to SIEM monitoring, endpoint telemetry, CTI enrichment, case management, SOAR containment, containerised SOC services and post-incident evaluation within a single CyberRangeCZ/KYPO sandbox.

3.7 KYPO/CRCZ LM8 CACAO Playbook Authoring Training (Firewall IP Block) 1d (status: validation)

3.7.1 Source code

The KYPO/CRCZ project is imported from a public GitHub repository maintained by the NG-SOC consortium:

Link to GitHub: <https://github.com/NG-SOC-eu/lm8-1d>

README: <https://github.com/NG-SOC-eu/lm8-1d/blob/main/README.md>

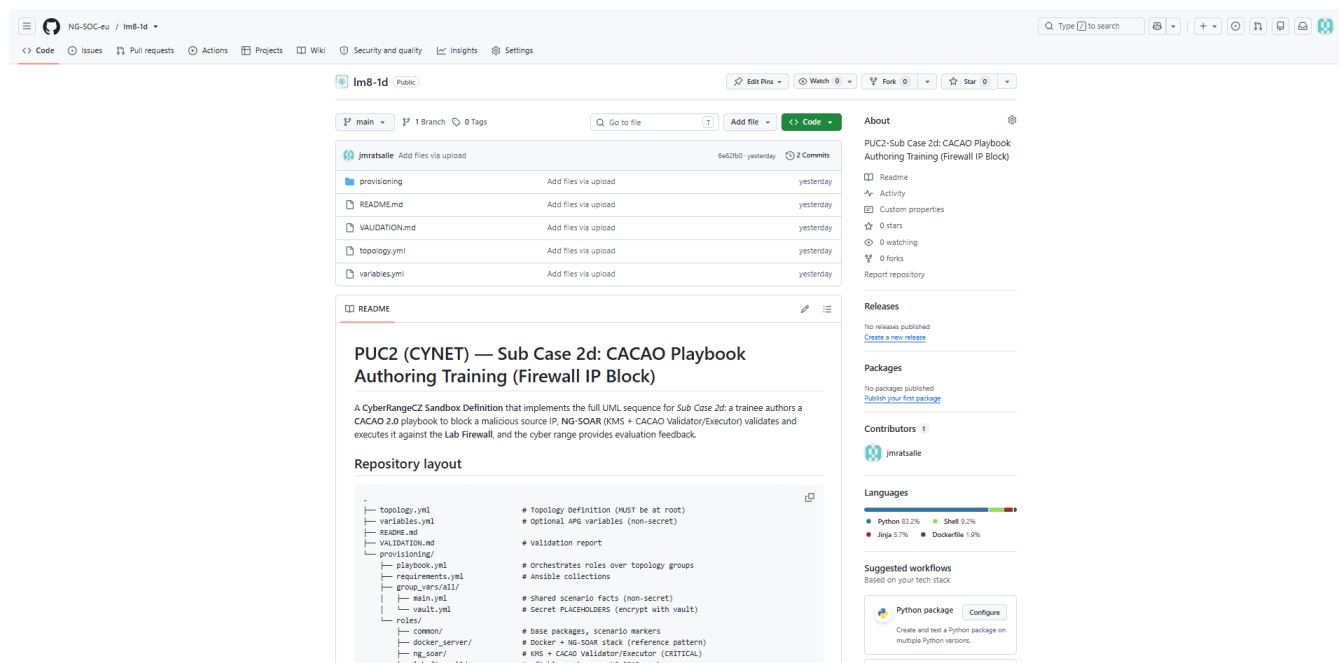


Figure 73 KYPO/CRCZ LM8 CACAO Playbook Authoring Training (Firewall IP Block) 1d source code on GitHub

The repository's purpose is very specific: it implements a hands-on training exercise in which a trainee writes a **CACAO 2.0 security playbook** to block a malicious source IP address on a lab firewall. The workflow is mediated by an NG-SOAR component, which provides a Knowledge Management System, a CACAO validator and a CACAO executor. The executor applies the requested defensive action to the firewall, verifies that traffic from the malicious test IP is blocked, and sends evidence to an evaluation and reporting service.

This makes lm8-1d different from the broader incident response or phishing-awareness repositories previously reviewed. It is not a large SOC investigation scenario, nor a general awareness training platform. It is a compact orchestration-and-automation exercise focused on one defensive course of action: transforming an incident response requirement into a machine-readable CACAO playbook and executing it safely against a controlled firewall enforcement point.

3.7.2 CACAO and the educational theme

The educational theme is CACAO playbook authoring. CACAO Security Playbooks v2.0 was approved by OASIS on 27 November 2023 and is intended to help organisations orchestrate, collaborate and share cybersecurity playbooks. The standard is designed around documenting and testing steps used to detect, investigate, mitigate and remediate threats. Im8-1d uses that standardised playbook idea in a deliberately narrow and assessable way: the trainee writes a playbook whose action step blocks traffic from a malicious source IP.

The scenario is therefore valuable as a bridge between incident response theory and SOAR automation practice. Rather than asking the trainee merely to describe a response procedure in prose, it requires them to encode that response as a structured CACAO 2.0 JSON document, validate its syntax and workflow logic, execute it through NG-SOAR, and review machine-generated evidence. This gives the learner a practical understanding of what it means for a playbook to be both human-understandable and machine-actionable.

3.7.3 Repository structure and content organisation

The repository is intentionally compact. Its root contains `topology.yml`, `variables.yml`, `README.md`, `VALIDATION.md` and the `provisioning/` directory. Inside `provisioning`, the project provides `playbook.yml`, `requirements.yml`, `group_vars/all/main.yml`, `group_vars/all/vault.yml`, and Ansible roles for common host setup, Docker and NG-SOAR deployment, CACAO validation and execution, the lab firewall, the lab target, the attacker, the student workstation and evaluation reporting.

A notable structural point is that this repository does not appear to contain a separate root-level `training_linear.json` or a conventional multi-level CyberRangeCZ training definition. The training journey is instead embedded in the sandbox resources themselves: the student workstation receives an exercise brief, schema hints, supported firewall commands, a template playbook and a `cacao-client` helper. The trainee workflow is therefore operational rather than quiz-driven.

This organisation is appropriate for the learning objective. The central artefacts are not slides or multiple-choice questions; they are a playbook template, a validator, an executor, a firewall, an attacker, a target and a reporting endpoint. The repository therefore models a short but complete SOAR automation loop, from playbook creation to validation, execution, evidence capture and summary.

3.7.4 Overall purpose of the project

The project implements **PUC2 Sub Case 2d**, a training scenario in which suspicious traffic originates from a malicious test IP and hits a protected lab service. The trainee's task is to create a CACAO 2.0 playbook that blocks the malicious source IP at the Lab Firewall. NG-SOAR validates the trainee's playbook, executes the firewall action, verifies that the attacker can no longer reach the target service, and sends the result to the reporting component.

The learning objective is precise: trainees practise authoring a defensive automation playbook and seeing the operational result of that playbook in a controlled cyber range. This is not designed as a stealthy red-team

exercise or a complex forensic investigation. The attacker is a known test host at 10.10.10.10, the protected target is at 10.10.20.10, and the enforcement point is a nftables-based Lab Firewall. The training challenge lies in writing a valid playbook, passing validation, and confirming that the correct block action has been applied.

The repository also exposes optional APG variables for the malicious source IP, target service IP and target service port. This suggests that the scenario was designed with some degree of per-sandbox variation in mind, although the default values are fixed to 10.10.10.10, 10.10.20.10 and port 80.

3.7.5 Topology and virtual infrastructure

The topology defines a sandbox named puc2-subcase2d-cacao-firewall-ip-block. It contains six end-host virtual machines: ng-soar, lab-firewall, lab-target, attacker, student-ws and evaluation-reporting. It also contains three routers, one for each lab network's WAN egress: soar-router, attacker-router and target-router. The images are Debian 12 for the SOAR, firewall, target, student and reporting hosts, and Kali 2020.4 for the attacker host.

The network design uses three disjoint lab networks and one WAN network. The soar-net network is 10.10.30.0/24 and hosts NG-SOAR, the student workstation, evaluation reporting and one firewall interface. The attacker-net network is 10.10.10.0/24 and hosts the attacker plus a firewall interface. The target-net network is 10.10.20.0/24 and hosts the protected target plus a firewall interface. The WAN network is 100.100.100.0/24 and is used by routers for provisioning egress.

The key architectural feature is that lab-firewall is connected to all three lab networks and uses .1 addresses on each. This makes it the Layer 3 enforcement point between the attacker and the target, which is essential for the exercise. The README and topology both emphasise that static routes are installed so that attacker-to-target traffic crosses the firewall, making the CACAO-injected source-IP block observable and verifiable.

One design choice worth noting is that all three lab networks are marked `accessible_by_user: True` in the topology. This may be intentional for instructor convenience and troubleshooting, but it is less restrictive than scenarios where trainees access only a workstation network. If the exercise is delivered to less trusted users, instructors may want to confirm how CyberRangeCZ exposes these networks and whether all of them should be user-accessible.

3.7.6 Host roles and scenario components

The ng-soar host is the central orchestration component. It runs the NG-SOAR stack and a training-specific CACAO Validator/Executor container. The validator/executor exposes a health endpoint on port 9100 and implements the server side of validation, execution, firewall rule application, verification and reporting. The role also publishes templates, schema hints and supported firewall commands through the KMS web root and locally under the SOAR toolkit path.

The lab-firewall host runs nftables and acts as the gateway between the attacker, target and SOAR networks. Its base ruleset uses an accept policy for the forward chain so that traffic initially succeeds, and CACAO execution appends a drop rule for the malicious source IP. The firewall role also creates a management user named soar-

fw, grants passwordless sudo only for /usr/sbin/nft, and authorises the executor's SSH public key. This is a sensible safety measure because the automation account can manage firewall rules without being given unrestricted sudo access.

The lab-target host provides the protected service used for verification. It installs nginx and OpenSSH, publishes a recognisable landing page, ensures HTTP and SSH are running, and routes attacker-network traffic back through the firewall. It also authorises the NG-SOAR executor key, allowing evidence collection and verification activity.

The attacker host is deliberately simple but important. It represents the malicious test source IP, installs traffic-generation tools such as curl, netcat, nmap and hping3, routes target-network traffic through the firewall, and starts a systemd service that generates suspicious traffic towards the target. The generator loops over HTTP requests to paths such as /admin and /.env, and also performs a light port check against SSH.

The student-ws host is the trainee authoring workstation. It creates a ~/cacao workspace, delivers the exercise brief, copies the CACAO toolkit from the NG-SOAR role, installs the cacao-client helper, and sets environment variables pointing the client to the NG-SOAR API and the evaluation service. This makes the learner's workflow very direct: edit a playbook, validate it, execute it and request a summary.

The evaluation-reporting host provides the feedback endpoint. It runs a small Python HTTP service that accepts execution reports through POST /ingest, stores them under /var/log/cacao-training/reports, and serves the most recent training summary through GET /summary. Its grading logic is intentionally simple: a result is marked PASS when validation is approved, and traffic is confirmed as blocked; otherwise it is marked for review.

3.7.7 Provisioning workflow and Ansible design

The provisioning playbook is organised around the scenario's operational dependency chain. It first applies a common baseline to all Linux hosts, then deploys Docker and the NG-SOAR stack, then configures the Lab Firewall, Lab Target, Attacker, Student Workstation and Evaluation/Reporting host. This ordering is sensible because the SOAR and firewall trust relationship depends on generated keys and group variables, while verification depends on the attacker, target and firewall routing being in place.

The common role installs base packages such as curl, jq, Python, chrony, net-tools and tcpdump, creates /var/log/cacao-training, and drops a scenario marker file at /etc/cacao-training.env containing key values such as the malicious source IP, target service IP and NG-SOAR IP. This is useful for both operational troubleshooting and evidence collection during the exercise.

The Ansible collection requirements are concise and appropriate for the repository's role design. The project requires community.docker, community.crypto and ansible.posix, matching its use of Docker Compose deployment, OpenSSH keypair generation, sysctl and mount-related tasks.

The Docker server role deliberately adapts an NG-SOC reference pattern but avoids embedding the plaintext secrets that the README says exist in the reference role. It installs Docker Engine and the Compose plugin,

optionally logs in to Docker Hub when a real PAT is provided, attempts a best-effort SMB mount for artefacts, and falls back to a bundled docker-compose.yml when the artefact share is unavailable.

3.7.8 NG-SOAR implementation

The NG-SOAR implementation has two layers. The docker server role deploys a fallback KMS component using an nginx container that serves playbooks and templates from /opt/NG-SOAR/kms/www. The repository notes that, in a production sandbox, this fallback may be replaced by a real NG-SOAR artefact pulled from an SMB share. The CACAO Validator/Executor itself is deployed separately by the NG-SOAR role.

The validator/executor is a small Python HTTP service packaged as a Docker container. It exposes POST /validate, POST /execute and GET /healthz. Validation checks required top-level fields, confirms that the document is a CACAO 2.x playbook, checks that the workflow has a valid start and end structure, verifies step references, requires at least one action step, and looks for a firewall block or drop command with a source IP parameter.

Execution is deliberately constrained. Although the trainee submits a playbook containing an action command, the server-side executor resolves the source_ip variable and constructs its own nftables command of the form `sudo nft add rule inet filter forward ip saddr <source_ip> counter drop`. It then connects to the firewall by SSH, applies the rule, lists the firewall ruleset as evidence, probes the target from the attacker host, and reports whether the traffic was blocked. This design reduces the risk of arbitrary command execution while still allowing the trainee to experience playbook-driven automation.

The executor also pushes the compiled result to the evaluation service. The report includes validation output, firewall evidence, verification results, execution status, logs, playbook ID, playbook name and completion time. This gives the scenario a closed loop from authoring to action to evidence to feedback.

3.7.9 CACAO toolkit and trainee experience

The trainee begins from a clear exercise brief. The brief states that a cyberattack is unfolding in the range, that suspicious traffic originates from 10.10.10.10, that the protected service is http://10.10.20.10:80, and that the enforcement point is the nftables-based Lab Firewall managed by NG-SOAR. The trainee must start from template_block_ip.json, read schema hints and supported command documentation, set a valid playbook ID and source IP, submit the result for validation, correct errors if needed, and then execute the approved playbook.

The template playbook is a CACAO 2.0 JSON document with a playbook_variables entry for source_ip, a start step, an action step and an end step. The action step is named “Block source IP on the Lab Firewall (nftables)” and contains an SSH command template using __SOURCE_IP__. A reference solution is also provided, already filled with the malicious IP 10.10.10.10.

The schema hints document is useful because it tells trainees what the validator is actually checking. It explains the required top-level fields, the need for exactly one start step and at least one end step, the need for valid on_completion references, and the requirement to define source_ip or use the placeholder in the block

command. This makes the exercise more educational than a black-box API rejection loop because learners can map validation errors to specific CACAO structure.

The cacao-client helper simplifies interaction with NG-SOAR. It wraps curl calls to /validate, /execute and /summary, formats JSON with jq when available, and uses default URLs for NG-SOAR and the evaluation service. This is a practical design choice because the learning focus remains on CACAO playbook structure and defensive automation, not on memorising HTTP request syntax.

3.7.10 Firewall action and verification model

The firewall model is straightforward and effective. The base nftables ruleset accepts forwarded traffic by default. That allows the attacker to reach the target before playbook execution and creates a measurable before-and-after condition. When the playbook is executed, NG-SOAR appends a source-IP drop rule to the inet filter forward chain.

The supported command guide reinforces this model. It explains that the exercise goal is to block a source IP using nftables, that NG-SOAR executes the block command over SSH as the soar-fw management user, and that packet counters provide evidence that the rule matched malicious traffic. It also documents related commands for more targeted blocking, rejection, evidence collection and rollback.

The verification step is particularly important. After applying the firewall rule, the executor drives a probe from the attacker host towards the target service and treats blocked or empty HTTP output as evidence that the malicious traffic is no longer reaching the service. This turns the exercise from a mere configuration-writing task into an observable security-control validation exercise.

3.7.11 Evaluation and reporting

The evaluation component is deliberately small but adequate for the exercise. It receives the execution report, stores it as JSON, and builds a summary containing the scenario name, playbook name, playbook ID, validation approval state, validation errors and warnings, blocked source IP, traffic-blocked result, execution status and grade. The grading rule is transparent: validation approval plus confirmed blocking yields PASS; otherwise, the result is marked REVIEW.

This simplicity is appropriate because the learning outcome is binary and operationally verifiable. The student either produced a valid playbook that caused the malicious source IP to be blocked, or they did not. For classroom use, this kind of immediate result is valuable because it supports rapid feedback and makes instructor review easier.

However, the reporting service is not a full learning analytics platform. It stores the last summary in memory and writes reports to disk, but it does not appear to provide cohort dashboards, persistent trainee identity management, rubric scoring, or multi-attempt analytics. This is not a defect for a compact sandbox exercise, but it limits its use as a large-scale assessment platform without additional integration.

3.7.12 Validation and quality controls

The repository includes a `VALIDATION.md` report dated 21 June 2026. It states that every component in the UML sequence diagram is backed by a concrete sandbox resource: CyberRangeCZ provides the hands-on educational platform, ng-soar provides KMS and CACAO validation/execution, lab-firewall provides nftables enforcement, lab-target provides the protected service, evaluation-reporting provides summary feedback, attacker provides the malicious test IP, and student-ws provides the trainee authoring environment.

The validation report also states that the NG-SOAR CACAO Validator/Executor has been functionally checked against the shipped sample playbook, template playbook and a broken playbook. According to the report, the sample is approved, the template is approved with placeholder detection, and the broken playbook is rejected with actionable errors. This is a useful quality-control measure because it validates the core behaviour of the most important component.

Topology validation is also covered. The report records that host, router and network names are unique; the lab CIDRs are disjoint; mappings reference existing resources; IPs fall inside their networks; images and flavours are valid; the firewall is on the attacker-to-target path; and the Ansible groups defined in the topology are consumed by the playbook.

The validation is stronger than mere documentation, but it is not complete CI/CD. The report states that YAML linting, YAML parsing, JSON validity checks, and Python compilation passed, while `ansible-playbook --syntax-check` could not be run in the author's Windows shell because of a Git Bash stdin issue. It instructs operators to run the Ansible syntax check on a Linux host or CyberRangeCZ management node.

3.7.13 Secrets management and security posture

The repository takes secrets management more seriously than some training packages. The README explicitly states that it does not replicate a referenced NG-SOC role's hard-coded plaintext secrets. Instead, secrets are externalised to `provisioning/group_vars/all/vault.yml` as inert `CHANGEME` placeholders intended for Ansible Vault encryption or platform secret injection. Docker Hub login is skipped while the PAT remains `CHANGEME`, and the NG-SOAR executor uses an SSH keypair generated during provisioning rather than an embedded private key.

The vault file contains placeholders for Docker Hub credentials, SMB share access, the SOAR-to-firewall public key and the firewall management user password hash. The default firewall management password hash is locked, implying key-based authentication by default. This is a good pattern for a public training repository because it avoids accidentally publishing operational secrets while keeping the playbook structurally runnable.

From a security perspective, the scenario is intentionally defensive and constrained. The attacker generates suspicious traffic, but the exercise does not deploy real malware. The SOAR executor applies a specific nftables drop rule and does not simply run arbitrary student-supplied shell commands. Passwordless sudo on the firewall is limited to `nft`, reducing the blast radius of the automation account.

The main security caveat is that this remains a training sandbox. It opens management paths between NG-SOAR, the firewall, the attacker and the target, and it depends on trust relationships created during provisioning. That is appropriate inside CyberRangeCZ/KYPO, but the components should not be lifted into a live network without hardening, proper identity management, audited command execution, rollback controls and real CACAO schema validation.

3.7.14 Strengths of the repository

The first major strength is traceability. The README maps all 16 UML steps to concrete resources and implementation points, from sandbox instantiation and suspicious traffic generation through playbook authoring, validation, execution, firewall enforcement, verification, reporting and summary delivery. That makes the repository unusually clear about how the educational sequence corresponds to infrastructure and code.

A second strength is the controlled execution model. The trainee writes a CACAO playbook, but the server-side executor validates it and constructs the actual firewall command from a resolved source IP. This preserves the educational experience of playbook-driven automation while avoiding the obvious risk of letting arbitrary submitted commands run on the firewall.

A third strength is the compactness of the environment. The exercise uses only six main hosts and three routers but still covers a meaningful defensive automation workflow: attacker traffic, protected service, firewall enforcement, SOAR validation, playbook execution and reporting. This makes it easier to understand and deliver than larger multi-tool SOC environments.

A fourth strength is its handling of secrets. The project explicitly calls out poor secret-handling patterns in a reference role and deliberately avoids copying them. For a public cyber range repository, that is a positive engineering and governance choice.

3.7.15 Suitability for training delivery

Im8-1d is well suited for a focused lesson on security automation, CACAO authoring and SOAR-controlled enforcement. It would be particularly useful for learners who already understand basic incident response concepts and now need to see how a response decision can be translated into a structured playbook and executed by automation. It is also suitable for junior SOAR engineers, SOC automation trainees, incident response coordinators learning playbook structure, and cyber range participants studying defensive orchestration.

It is less suitable as a broad incident response or forensics module. There is no multi-stage investigation, no evidence triage across endpoints, no malware analysis, no SIEM-led alert workflow and no complex decision-making around business impact. The scenario assumes the malicious IP and defensive objective are already known. Its value is in playbook construction and controlled execution, not in discovery or investigation.

For instructor-led use, the repository is attractive because the success criteria are clear and observable. The trainee receives an approved validation result, executes the playbook, sees whether the attacker-to-target traffic

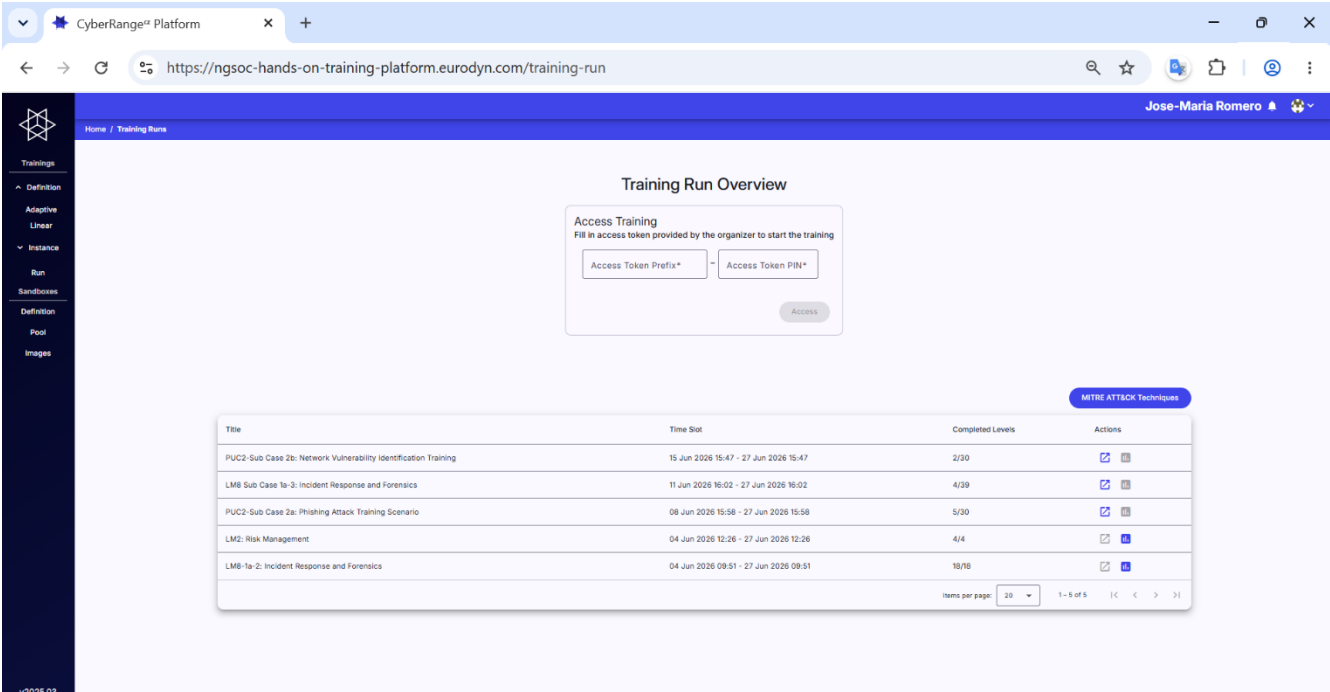
is blocked, and retrieves a summary. That makes the module easy to assess in a short session and easy to combine with a preceding lesson on detection or a following lesson on playbook governance and rollback.

3.7.16 Final assessment

Overall, NG-SOC-eu/lm8-1d is a focused and well-structured CyberRangeCZ/KYPO sandbox for **PUC2 Sub Case 2d: CACAO Playbook Authoring Training**. Its strongest feature is the end-to-end mapping from a defensive requirement to a CACAO playbook, from playbook validation to firewall execution, and from execution evidence to training feedback.

From an educational perspective, the repository is strongest as a compact security automation exercise. It teaches the practical relationship between CACAO structure, SOAR validation, firewall enforcement and verification evidence. From an engineering perspective, it is coherent, traceable and reasonably safe, especially because it avoids embedded secrets and limits the firewall management account. From a security perspective, it should still be treated as a lab-only package: the design is appropriate for an isolated CyberRangeCZ/KYPO sandbox, not for direct deployment into a production environment.

The following image shows a moment during the deployment of cyber ranges on the CyberRangeCZ platform.



The screenshot displays the 'Training Run Overview' page in the CyberRange Platform. The page includes a sidebar with navigation options: Trainings, Definition, Adaptive, Linear, Instance, Run, Sandboxes, Definition, Pool, and Images. The main content area shows a table of training runs. The table has four columns: Title, Time Slot, Completed Levels, and Actions. The table lists five training runs, including 'PUC2-Sub Case 2b: Network Vulnerability Identification Training' and 'LM8 Sub Case 1a-3: Incident Response and Forensics'. A sidebar on the left contains navigation links for Trainings, Definition, Adaptive, Linear, Instance, Run, Sandboxes, Definition, Pool, and Images. The top right shows the user 'Jose-Maria Romero'.

Title	Time Slot	Completed Levels	Actions
PUC2-Sub Case 2b: Network Vulnerability Identification Training	15 Jun 2026 15:47 - 27 Jun 2026 15:47	2/30	View Edit
LM8 Sub Case 1a-3: Incident Response and Forensics	11 Jun 2026 16:02 - 27 Jun 2026 16:02	4/39	View Edit
PUC2-Sub Case 2a: Phishing Attack Training Scenario	08 Jun 2026 15:58 - 27 Jun 2026 15:58	5/30	View Edit
LM2: Risk Management	04 Jun 2026 12:26 - 27 Jun 2026 12:26	4/4	View Edit
LM8-1a-2: Incident Response and Forensics	04 Jun 2026 09:51 - 27 Jun 2026 09:51	18/18	View Edit

Figure 74 List of cyber ranges deployed on a moment

3.7.17 Scenario status and public-release readiness

This scenario is well aligned with public dissemination because it is defensive, constrained and standards-oriented. Learners author and validate a CACAO playbook that blocks a malicious source IP through a lab firewall. The scenario avoids real malware and focuses on structured automation, verification and reporting.

Table 27 Scenario status and public-release readiness

Scenario name	Repository / resource	Machine-readable format	Validation state	Deployment constraints	Public-release readiness
LM8 CACAO Playbook Authoring Training (Firewall IP Block) 1d	https://github.com/NG-SOC-eu/lm8-1d	CACAO JSON playbooks, topology YAML, Ansible provisioning, NG-SOAR validation/execution JSON, evaluation reports	Strong documented validation exists; final Linux-based Ansible syntax check should be completed	Requires CyberRangeCZ/KYP O, NG-SOAR, lab firewall, attacker and target hosts, student workstation and evaluation/reporting service	Close to public-ready after completing the remaining syntax-check caveat and preserving vault-based secret handling

3.7.18 Public-dissemination hygiene review

Table 28 Public-dissemination hygiene review

Hygiene items	Assessment	Required public-release action
Default credentials	The scenario externalises sensitive deployment values into vault placeholders.	Keep this pattern and ensure no plaintext deployment secrets are introduced before publication.
Weak passwords	The firewall management posture is designed for lab use, with key-based access preferred.	State that management trust relationships are lab-only and not production-ready.
TODO / placeholder values	Vault fields use inert placeholders for deployment-time injection.	Keep placeholders, but document which values operators must replace.
Command execution	NG-SOAR executes a constrained firewall action rather than arbitrary shell execution.	Preserve command restrictions and document the allowed action boundary.
Validation caveat	One syntax-check step could not be completed in the original authoring shell.	Run the syntax check on Linux or a CyberRangeCZ management node and record the result.

3.7.19 YAML/JSON/CACAO artefact inventory

Table 29 YAML/JSON/CACAO artefact inventory

Artefact	Format	Location / role	Release note
CACAO sample playbook	JSON / CACAO	Student toolkit	Safe to publish if all IPs and identifiers remain synthetic.
CACAO template playbook	JSON / CACAO	Learner authoring exercise	Should retain placeholders and validation hints.

Broken CACAO example	JSON / CACAO	Negative validation exercise	Useful for teaching validator error handling.
Scenario topology	YAML	topology.yml	Must maintain firewall placement between attacker and target paths.
Provisioning playbooks	YAML / Ansible	provisioning/	Should pass syntax and avoid embedded secrets.
Vault placeholders	YAML / Ansible Vault input	group_vars style deployment configuration	Must remain inert until operator injection.
NG-SOAR validation responses	JSON	/validate, /execute and /summary workflow	Should be retained as machine-readable evidence.
Evaluation report	JSON	Evaluation/reporting component	Should include validation result, blocked IP, traffic status and pass/review outcome.

4 Conclusion and Future Enhancements

This deliverable has presented the open cybersecurity training and exercise scenarios developed within NG-SOC Task T5.3. Its contribution is twofold. First, it consolidates a structured set of Learning Modules that provide the conceptual, methodological and professional foundation for next-generation SOC capabilities. Second, it documents the KYPO/CRCZ cyber range scenarios that translate selected learning outcomes into practical, repeatable and technically grounded exercises. The value of the deliverable therefore lies in the combination of curriculum design and operational experimentation.

The **Learning Modules** form the educational backbone of the deliverable. They cover cybersecurity laws, regulations and compliance; risk management; auditing and assessment; cybersecurity policies and frameworks; technical analysis and security management; business integration and strategy; privacy and data protection; incident response and forensics; and collaboration and communication. This breadth is important because next-generation SOC's require more than technical detection skills. They need professionals who understand governance, legal obligations, risk, privacy, evidence handling, communication, decision-making and organisational alignment.

The modules also demonstrate a progressive approach to learning. They introduce foundational concepts, develop them through lessons and scenarios, and reinforce them through quizzes, review sections, practical exercises and case studies. This allows different learner profiles to benefit from the curriculum, including technical analysts, risk specialists, governance professionals, incident responders, privacy practitioners and managers. The Learning Modules therefore provide a common vocabulary and methodological baseline before learners move into hands-on cyber range activities.

A key achievement of the Learning Modules is their multidisciplinary scope. Risk management is linked to business impact and control selection; auditing is connected to evidence, reporting and remediation; privacy is addressed through data protection, DPIAs, PETs and forensic considerations; incident response is connected to standards, CSIRT operations, technical analysis and reporting; and collaboration is treated as an operational capability. This reflects the reality of modern SOC environments, where people, processes and technology must work together during both routine operations and crisis situations.

The **KYPO/CyberRangeCZ cyber ranges** complement this educational foundation by converting selected learning objectives into practical exercises. The scenarios documented in this deliverable cover several SOC-relevant areas, including risk management, phishing awareness, incident response, vulnerability identification, malware detection and response, CTI enrichment, SOAR-supported containment, CACAO playbook authoring and cyber range quality assurance. These exercises allow learners to apply theoretical knowledge in controlled environments with realistic tools, artefacts, workflows and reporting tasks.

The implementation maturity of the cyber ranges is already significant. Several repositories include topology definitions, Ansible provisioning, learning sequences, instructor documentation, trainee workspaces, reporting components, validation checks and reusable templates. Some scenarios are already completed, while others are in execution testing or validation. This staged status reflects a realistic engineering lifecycle, moving from

scenario design and implementation to deployment, testing, validation and refinement. It also shows that the consortium is building reusable training assets rather than one-off demonstrations.

The integration with CyberRangeCZ is a major technical achievement. The scenarios use the platform's approach to sandbox definition, topology modelling, virtual infrastructure orchestration and automated provisioning. This supports repeatable delivery, reduces manual setup effort and helps instructors validate exercises more consistently.

The cyber ranges that have been deployed in the CyberRangeCZ infrastructure pass 3 stages.

Sandbox Instances							
Name ↑	Notes And Comments	Lock	Created	Created By	State	Stages	Actions
Sandbox 454		unlocked	Jun 4, 2026	Jose-Maria Romero	build finished	🟢🟢🟢	🗑️ 👤 🔑

Figure 75 Deployment process (3 stages) in a pool with a sandbox on CyberRangeCZ

Exercises have also been conducted on them. Finally, an approach to automating the creation of scenarios on the CyberRangeCZ Platform is also presented. The following video demonstration focuses on how to move from a scenario defined as a project to its reproducible deployment for testing, reducing manual effort and accelerating the validation cycle.

The main objective is to simplify and standardise the preparation of training and testing environments, improving operational efficiency, consistency across executions, and the speed at which scenarios can be iterated, for example for assessment, training or capability verification activities in SOC contexts.

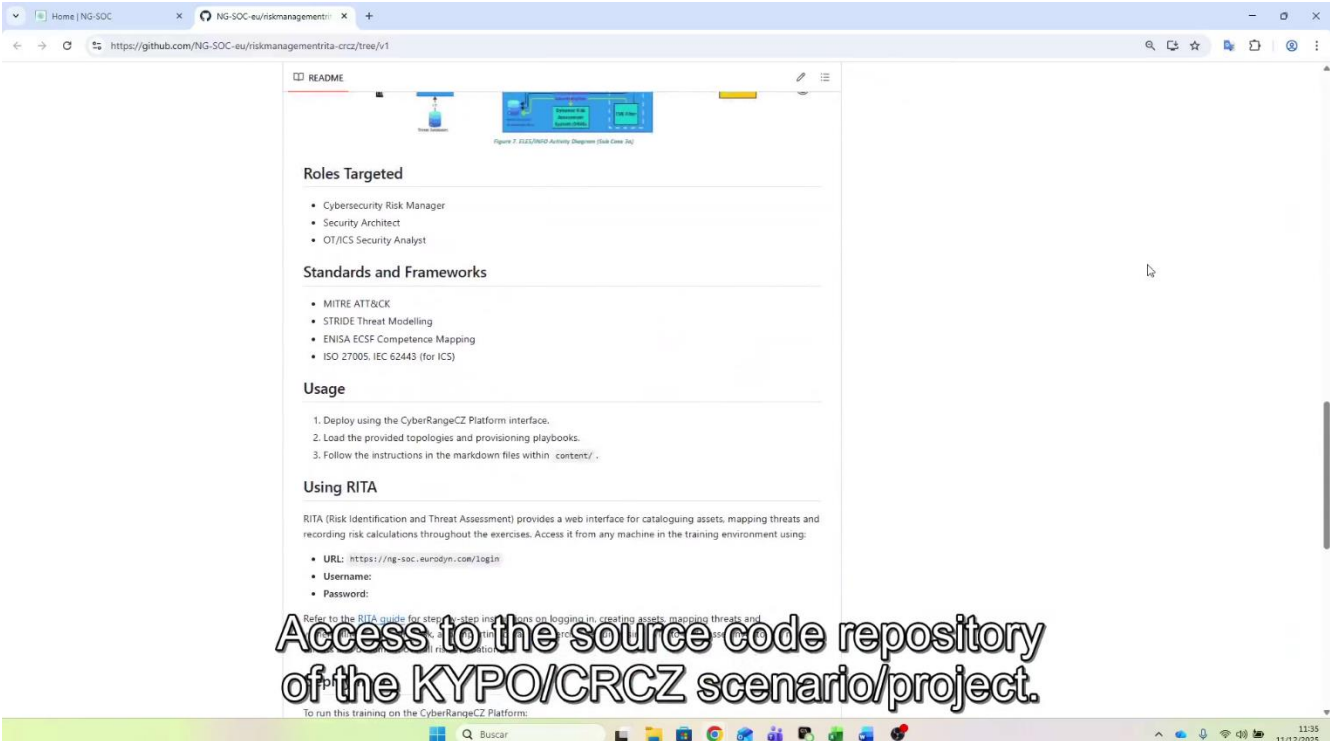


Figure 76 Automating the creation of CyberRangeCZ Platform scenarios (screenshot)

Link to this video demonstration on SharePoint: [Automating the creation of CyberRangeCZ Platform scenarios.mp4](#)

The combined contribution of the Learning Modules and the cyber ranges is therefore greater than either part alone. The Learning Modules provide the curriculum, concepts, standards, terminology and assessment logic. The cyber ranges provide the operational setting, tools, evidence and practical tasks. Together, they support a training model in which learners first understand the principles of cybersecurity practice and then apply them in controlled environments that reproduce relevant SOC, CSIRT, CTI, SOAR, risk management, vulnerability assessment and reporting workflows.

Future enhancements should address both dimensions in a balanced way. For the Learning Modules, the next step should be to harmonise learning outcomes, prerequisites, assessment criteria and links to practical activities across all modules. A common template for module objectives, target roles, estimated duration, prior knowledge, associated standards and assessment types would make the curriculum easier to navigate and reuse.

A second enhancement is stronger cross-referencing between theory and practice. Where a cyber range implements a concept introduced in a Learning Module, this relationship should be made explicit. Risk management theory should link to the LM2 cyber range, incident handling and forensics content should link to LM8 scenarios, and vulnerability assessment concepts should link to LM5 exercises. This would help learners understand the continuity between Open edX content, classroom delivery and hands-on CyberRangeCZ activities.

For the cyber ranges, future work should focus on completing the validation and execution testing of scenarios that are not yet marked as fully done. This includes confirming that each topology deploys reliably, provisioning completes without manual intervention, learner-facing URLs and credentials are correct, scoring and reporting components work as expected, and each exercise can be completed by following the provided instructions.

Further work should also standardise repository structure and documentation. A common template for all KYPO/CyberRangeCZ scenarios should include a minimum viable deployment guide, tool inventory, learner prerequisites, instructor checklist, expected outputs, assessment rubric, known limitations, security warnings and troubleshooting section. This would make the scenarios easier to maintain and easier for external instructors to adopt.

Finally, stronger automation should be developed across the validation pipeline. Automated checks for JSON training definitions, YAML topology references, Ansible syntax, role dependencies, hostname resolution, secrets placeholders, exposed services and post-provisioning smoke tests would improve reliability. The QA Agent for Cyber Range also represents a promising direction for semi-automated scenario validation, reducing instructor workload and supporting faster iteration of training content.

In conclusion, D5.3 demonstrates that NG-SOC has produced a strong foundation for open cybersecurity training and exercise scenarios. The deliverable combines structured Learning Modules with practical cyber range

environments, supports multiple SOC-relevant roles and workflows, and introduces automation approaches that can improve repeatability and validation. The next phase should consolidate this work through final validation, standardised packaging, stronger links between modules and exercises, richer assessment, continued automation and alignment with the broader NG-SOC capability roadmap.

Appendix A – Asset Specification

Table 30 OpenEDx Asset Specification

Asset Overview	
Asset(s) name(s):	OpenEDx Self Paced Education Platform
Created by:	ED
Document version:	1.0
Asset Description	The continuous training, education and awareness module aims to train, educate and up-skill the involved within security domain, personnel. The module comprises a platform that provides self-paced training courses and a Cyber range platform for hands-on training scenarios without the risk of compromising systems in production. Open edX GitHub: https://github.com/openedx Opened/edx-platform GitHub: https://github.com/openedx/edx-platform Open edX info and community: https://openedx.atlassian.net/wiki/spaces/COMM/overview?mode=global
Asset Requirements	
Hardware requirements:	VM 2+ Cores 8+ GB RAM 50+ GB Storage
Locality	ED Premises
Distributed environment	-
Type and size of input data	OpenEDx uses APIs for access to OpenEDx information OpenEDx uses data in .csv (comma-separated values) file format Users can input data in OpenEDx using XML code using OLX Users can format equations, you can use MathJax The maximum size for each file is 10 MB
Data processing	Real-time
Type and size of output data	OpenEDx uses MySQL™ 5.1 relational database system with InnoDB storage engine Output files are stored as UTF-8. OpenEDx also uses the Django® Python Web framework OpenEDx uses LMS, or learning management system, is a software tool that allows you to create, deliver, and report on training courses and programs A blank Tutor-based installation uses 341 MB in the data/ folder – this includes MySQL database (283 MB), MongoDB (17 MB) and the Android app (21 MB). The amount of space that you need depends on how many students your platform

	will have, how frequently they will have to upload files, how big these files will be, how much videos your staff will upload, how large they are, etc. It could end up being anywhere between 100 MB and 100 TB	
Interfacing (I/O)	Input: Devstack Interface	Output: Open edX feature toggles used in edx-platform
Interactions	Interaction with edX REST APIs The OAuthAPIClient uses the Tiered Cache internally for caching SAML 2.0 (Security Assertion Markup Language) and OAuth 2.0	
Software dependencies/libraries required:	MYSQL, Memcache, MongoDB, nginx, docker, Ansible, python3	
Software license:	Open source	
User Interaction:	Open edX provides a user interface	
Additional Information		
Relevant blocks from conceptual architecture	Continuous training, education and awareness	
Functionalities for MVP (M30)	A trainer will construct self-paced courses. These courses will be consumed by the trainees, to test and enhance their Cybersecurity related knowledge. Feedback will be available both to the trainer and to the trainees.	
Notes and Issues:	None.	

REFERENCES

- [1] European Parliament and Council (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. Retrieved on 22 June 2026 from <https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng>.
- [2] European Parliament and Council (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data. Retrieved on 22 June 2026 from <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.
- [3] National Institute of Standards and Technology (2024). The NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved on 22 June 2026 from <https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final>.
- [4] Joint Task Force Transformation Initiative (2012). Guide for Conducting Risk Assessments. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved on 22 June 2026 from <https://csrc.nist.gov/pubs/sp/800/30/r1/final>.
- [5] Nelson, A., Rekhi, S., Souppaya, M., & Scarfone, K. (2025). Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved on 22 June 2026 from <https://doi.org/10.6028/NIST.SP.800-61r3>.
- [6] Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to Integrating Forensic Techniques into Incident Response. Gaithersburg, MD: National Institute of Standards and Technology. Retrieved on 22 June 2026 from <https://csrc.nist.gov/pubs/sp/800/86/final>.
- [7] International Organization for Standardization and International Electrotechnical Commission (2022). ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Geneva: ISO. Retrieved on 22 June 2026 from <https://www.iso.org/standard/27001>.
- [8] International Organization for Standardization and International Electrotechnical Commission (2022). ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. Geneva: ISO. Retrieved on 22 June 2026 from <https://www.iso.org/standard/75652.html>.
- [9] International Organization for Standardization (2018). ISO 31000:2018 Risk management — Guidelines. Geneva: ISO. Retrieved on 22 June 2026 from <https://www.iso.org/standard/65694.html>.
- [10] European Union Agency for Cybersecurity (2022). European Cybersecurity Skills Framework (ECSF): User Manual. Athens: ENISA. Retrieved on 22 June 2026 from <https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf>.
- [11] FIRST (2020). Computer Security Incident Response Team (CSIRT) Services Framework, Version 2.1. Retrieved on 22 June 2026 from https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1.
- [12] MITRE Corporation (n.d.). MITRE ATT&CK®. Retrieved on 22 June 2026 from <https://attack.mitre.org/>.

- [13] OASIS Open (2023). CACAO Security Playbooks Version 2.0. Retrieved on 22 June 2026 from <https://docs.oasis-open.org/cacao/security-playbooks/v2.0/security-playbooks-v2.0.html>.
- [14] CyberRangeCZ (n.d.). CyberRangeCZ Platform Documentation. Retrieved on 22 June 2026 from <https://docs.platform.cyberrange.cz/>.
- [15] KYPO Cyber Range Platform (n.d.). KYPO Cyber Range Platform. Retrieved on 22 June 2026 from <https://crp.kypo.muni.cz/>.
- [16] Open edX (n.d.). Open edX Documentation. Retrieved on 22 June 2026 from <https://docs.openedx.org/en/latest/index.html>.
- [17] Wazuh, Inc. (n.d.). Wazuh Documentation. Retrieved on 22 June 2026 from <https://documentation.wazuh.com/current/index.html>.
- [18] MISP Project (n.d.). MISP Documentation and Support. Retrieved on 22 June 2026 from <https://www.misp-project.org/documentation/>.
- [19] National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper No. 29). U.S. Department of Commerce. Retrieved on 29 June 2026 from <https://doi.org/10.6028/NIST.CSWP.29>
- [20] European Parliament and Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1792, and repealing Directive (EU) 2016/1148 (NIS 2 Directive). Official Journal of the European Union, L 333, 80–152. <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
- [21] European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- [22] European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011. Official Journal of the European Union, L 333, 1–79. <https://eur-lex.europa.eu/eli/reg/2022/2554/oj>
- [23] European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). Official Journal of the European Union, L 2024/2847. <https://eur-lex.europa.eu/eli/reg/2024/2847/oj>
- [24] European Commission. (2021). Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts (COM/2021/206 final). EUR-Lex. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>

- [25] de Mast, J., & Lokkerbol, J. (2012). An analysis of the Six Sigma DMAIC method from the perspective of problem solving. *International Journal of Production Economics*, 139(2), 604–614. <https://doi.org/10.1016/j.ijpe.2012.05.035>
- [26] Cloudian. (n.d.). What is data protection and privacy? Cloudian. Retrieved June 29, 2026, from <https://cloudian.com/guides/data-protection/data-protection-and-privacy-7-ways-to-protect-user-data/>
- [27] Bing, C., Menn, J., & Lynch, S. N. (2021, June 8). One password allowed hackers to disrupt Colonial Pipeline, CEO tells senators. Reuters. <https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/>



NGSOC

Next Generation Security Operations Centres



Co-funded by
the European Union



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

This project has received funding from the European Union's Digital Europe Programme (DIGITAL) under grant agreement No 101145874

