Harmonizing People, Processes, and Technology for Robust Cybersecurity

D6.6 Gamified Training Modules v2

Document Summary Information

Grant Agreement No	101158555	**Acronym**	CYberSynchrony
Full Title	Harmonizing People, Processes, and Technology for Robust Cybersecurity		
Start Date	01/06/2024	**Duration**	36 months
Project URL	https://www.cybersynchrony.eu/		
Deliverable	D6.2 Gamified Training Modules v2		
Work Package	WP6 Cybersecurity Consciousness: Empowering Society Through Awareness (CYBERWISE and Cybersecurity Standardization and Compliance Reinforcement (CYBERGOPLUS)		
Contractual due date	31/08/2026	**Actual submission date**	25/08/2026
Type	R -Document, report	**Dissemination Level**	Public
Lead Beneficiary	Focal Point (FP)		
Responsible Author	Koutras Dimitris (FP), Malamas Vangelis (FP)		
Contributions from	Kitty Kioskli (TRUST), Andrea Purificato (MER)		

Funded by the European Union

Funded by the European Union under Grant Agreement no. 101158555. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the granting authority can be held responsible for them.

Revision history

Version	Issue Date	Changes	Contributor(s)
0.1	17.05.2026	Initial Deliverable structure	Koutras Dimitris (FP)
0.2	02.06.2026	Deliverable Structure Finalization	Malamas Evangelos (FP)
0.3	09.06.2026	First contribution	Koutras Dimitris, Malamas Evangelos (FP)
0.4	20.06.2026	Contribution	Malamas Evangelos, Koutras Dimitris (FP)
0.5	25.07.2026	Final draft ready for internal review	Koutras Dimitris(FP)
0.6	30.07.2026	Peer review	Andrea Purificato(MER)
0.6	31.07.2026	Peer review	Kitty Kioskli(TRUST)
0.7	03.08.2026	Final draft addressing comments from internal review	Koutras Dimitris(FP)
0.8	20.08.2026	Final quality check	Eleni Keliri (eBOS)
1.0	25.08.2026	Final version ready for submission	Violeta Vasileva (MAG)

Disclaimer

The content of the document herein is the sole responsibility of the publishers, and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the CYberSynchrony consortium make no warranty of any kind with regard to this material including but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the CYberSynchrony consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© CYberSynchrony Consortium This Deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

[1] According to CYberSynchrony's Quality Assurance Process for reports:

- 3 months before Deliverable's Due Date: Table of Contents ready to be reviewed by WP leader/ Technical Manager/ Quality Manager
- 2 months before Deliverable's Due Date: 50% should be complete. Review by the Quality Manager (& Technical Manager for software).
- 1 month before Deliverable's Due Date:100% should be complete. Review by the Quality Manager and Peer Reviewers.
- M: Sent to PC for Submission to the EC after addressing all comments by Quality Manager and Peer Reviewers

Table of Contents

Executive Summary 5
1 Introduction 6
1.1 Mapping CYberSynchrony Outputs 7
1.2 Linkage to other project outputs 7
1.3 Deliverable Structure 8
2 Mission Content Management System (MCMS) 9
2.1 Overview and Purpose 9
2.2 Cyber Technique Library Management 9
2.3 Defense Library Management 10
2.4 Mission Library and Authoring 10
2.5 Attack Chain and Stage Management 11
2.6 Asset and Defense Assignment 11
2.7 Configuration and Scoring Parameters 12
2.8 Deployed Mission Catalogue 13
3 Cybergate Engine and Editor Enhancements 15
3.1 Live Backend Data Integration 15
3.2 Dedicated Mission Authoring Executable 16
3.3 Backend Infrastructure 17
4 Integration with the CYberSynchrony Platform 19
4.1 Integration Architecture 19
4.2 Data Flow and Synchronization 20
4.3 Adaptability to EU Project Needs 21
5 Conclusions 23
6 References 24

List of Figures

Figure 1: Review baseline and requirements addressed in the v2 development cycle 6
Figure 2: MCMS Cyber Technique Library - technique metadata and publishing controls 9
Figure 3: Defense mapping and multiplier configuration by attack technique 12
Figure 4: MCMS Mission Library - mission selection, metadata, and publishing workflow 15
Figure 5: Dedicated authoring interface - general mission configuration 16
Figure 6: Technique authoring. minigame mapping and log content 17
Figure 7: Corporate-environment point-of-interest and asset assignment 20
Figure 8: Industrial/OT point-of-interest and asset assignment 21

List of Tables

Table 1: Adherence to CYberSynchrony's GA 7
Table 2: Links to other Project Outputs/Work 8
Table 3. Missions & Primary Learning focus 13

© CYberSynchorny, 2024

Acronyms and abbreviations

Abbreviation / Term	Description
AD	Active Directory
API	Application Programming Interface
ATT&CK	Adversarial Tactics, Techniques & Common Knowledge
CI/CD	Continuous Integration / Continuous Deployment
ECCC	European Cybersecurity Competence Centre
EDR	Endpoint Detection and Response
EU	European Union
FP	Focal Point
GA	Grant Agreement
ICS	Industrial Control Systems
IoT	Internet of Things
JSON	JavaScript Object Notation
MCMS	Mission Content Management System
MITRE	MITRE Corporation
MFA	Multi-Factor Authentication
OT	Operational Technology
PHP	PHP: Hypertext Preprocessor
REST	Representational State Transfer
SFTP	SSH File Transfer Protocol
SIEM	Security Information and Event Management
SOC	Security Operations Center
TLS	Transport Layer Security
TTPs	Tactics, Techniques, and Procedures
VM	Virtual Machine
WP	Work Package

© CYberSynchorny, 2024

Executive Summary

D6.6 *"Gamified Training Modules v2"* is the second and final operational release of the Cybergate gamified cybersecurity training platform within the CYberSynchrony project (Grant Agreement no. 101158555). It is delivered under Work Package 6 (WP6) "Cybersecurity Consciousness: Empowering Society Through Awareness", led by Focal Point (FP), and fulfils the GA commitment to provide a mature, fully integrated gamified training environment in support of Task T6.4 (Immersive Gamified Cybersecurity) and the broader WP6 objectives.

Building directly upon D6.2 "Gamified Training Modules v1", this deliverable advances the Cybergate platform along three interconnected dimensions. First, it introduces the Mission Content Management System (MCMS): a comprehensive administrative backend that empowers trainers and administrators to manage the full lifecycle of training content — including cyber attack technique libraries, defense mappings, mission structures, narrative contexts, attack chain stages, asset assignments, and scoring configurations — without requiring access to the underlying codebase. This capability is the cornerstone of the platform's adaptability, as it enables mission content to be updated, extended, and tailored to specific organizational or sector needs in response to evolving threat landscapes.

Second, the Unity-based Cybergate editor engine has been significantly enhanced to retrieve live data directly from the backend during both development and runtime. Custom Unity editor modules facilitate real-time communication with the backend API, ensuring that mission authors always work with current content. In its final form, the editor is available as a standalone executable (.exe), making mission authoring accessible to trainers and content experts without software development expertise.

Third, Cybergate has been prepared for integration with the broader CYberSynchrony platform, with interfaces designed to support shared authentication, cross-module analytics, and alignment with threat intelligence outputs from WP3 and WP4. This integration is particularly significant in the context of the EU project's mission: the MCMS allows mission content to be continuously updated to reflect the specific cybersecurity challenges facing European Member States, national authorities, and critical infrastructure operators, keeping the training environment relevant, timely, and aligned with Europe's evolving cybersecurity needs.

Together, the developments in D6.6 transform Cybergate from a structured training prototype into a operationally integrated, dynamically adaptable training environment. The platform is positioned to support the CYberSynchrony project's overarching goal of equipping European society with the awareness, skills, and resilience needed to face modern cyber resilience.

© CYberSynchorny, 2024

1 Introduction

Work Package 6 (WP6) of CYberSynchrony pursues a set of ambitious objectives that span the full spectrum of cybersecurity consciousness: engaging diverse societal segments with awareness campaigns, utilizing gamification to make learning impactful, measuring campaign effectiveness through data analytics, cultivating a culture of secure online behaviour, supporting cybersecurity policy implementation, and ensuring industry-wide compliance with established standards. Deliverable D6.6 “Gamified Training Modules v2” sits at the heart of these objectives, providing the second operational version of the Cybergate immersive training platform.

The CYberSynchrony project, funded under the European Commission’s DIGITAL-ECCC-2023-DEPLOY-CYBER-04 call, brings together twelve beneficiaries from across Europe to deliver a holistic modular cybersecurity framework. The project places particular emphasis on the human dimension of cybersecurity, recognizing that technology alone is insufficient without an informed, prepared, and cyber-resilient society. Cybergate directly embodies this philosophy by placing learners at the center of immersive, scenario-driven training that mirrors real-world adversarial behavior.

While D6.2 established the foundational architecture, mission design methodology, and four-phase gameplay cycle of Cybergate, D6.6 focuses on the capabilities that make the platform genuinely operational at scale. The most consequential of these is the Mission Content Management System (MCMS), which provides the mechanism through which Cybergate achieves its defining adaptive capability: the ability to update, customize, and extend mission content without touching the game engine. This means that as new threats emerge, as project needs evolve, and as different Member States or sectors require tailored scenarios, the platform can adapt, rapidly and without technical overhead.

This adaptability is not incidental but central to the EU project’s value proposition. CYberSynchrony is designed to serve national cybersecurity authorities, competence centres, coordination centres, and relevant stakeholders across Europe. The ability to bring training scenarios closer to the specific threat environments and policy contexts of these varied audiences is precisely what the MCMS enables. Cybergate’s missions can be updated to simulate the latest attack patterns, aligned with the threat intelligence produced by WP3, and configured to reflect the defensive priorities and regulatory requirements relevant to each deployment context.

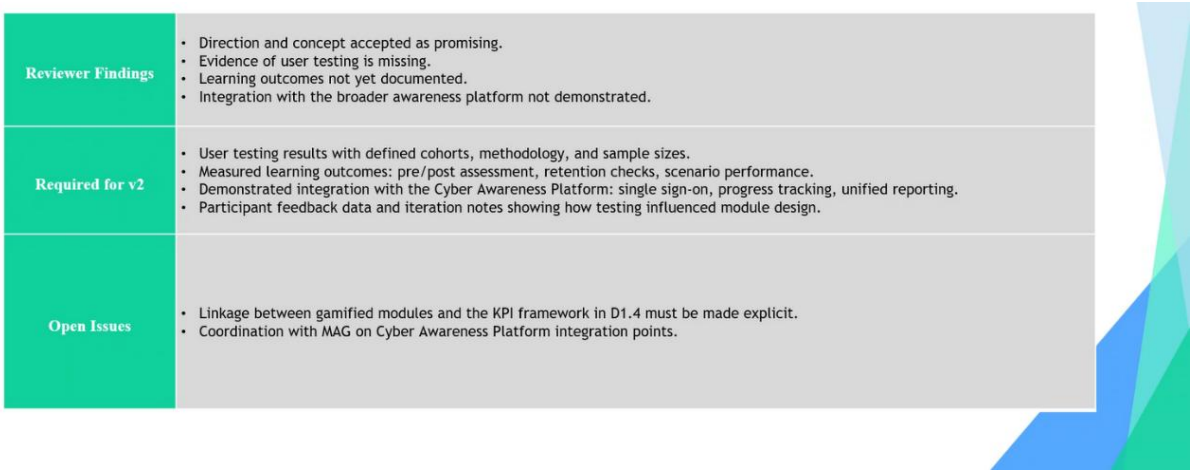

Figure 1: Review baseline and requirements addressed in the v2 development cycle

© CYberSynchorny, 2024

1.1 Mapping CYberSynchrony Outputs

This section maps the CYberSynchrony Grant Agreement commitments relevant to D6.6 to the corresponding document chapters.

Table 1: Adherence to CYberSynchrony's GA

Component no	Component title	Respective Document Chapter(s)	Justification
DELIVERABLE			
D6.6	Gamified Training Modules v2	Chapters 1–4	The deliverable extends the Cybergate platform with a Mission Content Management System, engine upgrades, and full CYberSynchrony platform integration — directly fulfilling the GA commitment for an operational v2 gamified training environment.
TASKS			
T6.4	Immersive Gamified Cybersecurity (Leader: FP; Participant: ALL)	Chapters 2, 3, 4	The MCMS and backend architecture directly advance T6.4 by providing a dynamically configurable simulation environment where missions can be updated to reflect real threats relevant to EU member states.
T6.1	CYberSynchrony Platform and Pervasive Cybersecurity Awareness Platform	Chapter 4	Platform integration ensures Cybergate operates as a connected module within the broader CYberSynchrony ecosystem, supporting the cross-module architecture envisioned in T6.1.
T6.3	CYberSynchrony Training Planning	Chapters 2, 3	Backend-driven content management and the dedicated editor executable support the structured, scalable training planning approach required by T6.3, including online and in-person deployment modes.

1.2 Linkage to other project outputs

D6.6 is embedded within a network of cross-WP dependencies and contributions that reinforce the coherence of the CYberSynchrony ecosystem.

© CYberSynchorny, 2024

Table 2: Links to other Project Outputs/Work

WP Number	Task Number	Deliverable Number related	Content
WP3	T3.3	D3.3 – Personalized Risk Assessment Tools	Risk outputs from WP3 directly feed into the MCMS mission design layer, ensuring attack technique libraries and scenario parameters reflect realistic, organization-specific threat profiles.
WP3	T3.4	D3.4 – Dynamic Risk Parameter Refinement	Dynamic risk parameters generated in WP3 can be injected into mission configurations through the MCMS, enabling real-time adaptation of training difficulty and scenario relevance.
WP4	T4.3	D4.2 – Automated Response Toolkit	Detection-response logic from WP4 informs the defensive action mappings within the MCMS defense library, ensuring consistency between operational response tools and training scenarios.
WP5	T5.2	D5.2 – Incident Response Collaboration Framework	Platform integration connects Cybergate training outcomes with WP5 collaborative incident response exercises, strengthening the link between skills training and operational readiness.
WP6	T6.1–T6.4	D6.2 – Gamified Training Modules v1	D6.6 directly extends D6.2, building upon the mission architecture, four-phase gameplay cycle, and validation framework while introducing the content management and integration capabilities that transform v1 into a production-ready ecosystem.

1.3 Deliverable Structure

This deliverable is organized into four substantive chapters:

Chapter 2: Mission Content Management System (MCMS): Describes the MCMS architecture and its functional modules, from technique and defense library management to mission authoring, attack-chain construction, asset assignment, scoring configuration, and the ten-mission content catalogue.

Chapter 3: Cybergate Engine and Editor Enhancements: Documents the upgrades to the Unity editor and game engine, including live backend data integration, the standalone authoring executable, and the PHP+SFTP backend infrastructure.

Chapter 4: Integration with the CYberSynchrony Platform: Outlines the integration architecture connecting Cybergate to the broader project ecosystem, including data flows, shared services, and the platform's adaptability to EU project and Member State needs.

Chapter 5: Conclusions: Summarizes the achievements of D6.6 and sets out the path for future platform enhancements.

© CYberSynchorny, 2024

2 Mission Content Management System (MCMS)

2.1 Overview and Purpose

The Mission Content Management System (MCMS) is the central new capability introduced in D6.6. It is a purpose-built administrative backend that provides a structured, role-based interface for managing all training content within the Cybergate platform. The MCMS represents the practical realization of a design principle that was architectural in D6.2 but is now fully operational: the complete separation of content from code.

In D6.2, the modular mission architecture established that "mission logic, attack techniques, defensive options, and scenario parameters are defined as data-driven components, enabling rapid updates, new content creation, and sector-specific customization." The MCMS is the system that operationalizes this principle. It provides the tools through which trainers, mission designers, and administrators can exercise full control over the platform's content without requiring software development expertise or access to the Unity game engine.

The importance of this capability for the CYberSynchrony project cannot be overstated. The EU project's mandate requires that training tools remain relevant across a diverse and evolving landscape of cyber threats, regulatory frameworks, and organizational contexts. National cybersecurity authorities in different Member States face different threat priorities. Critical infrastructure operators in the energy, healthcare, and transport sectors have distinct attack surfaces. The MCMS is what allows Cybergate to serve all of these audiences, by enabling mission content to be tailored, updated, and extended as needed, without rebuilding the game engine.

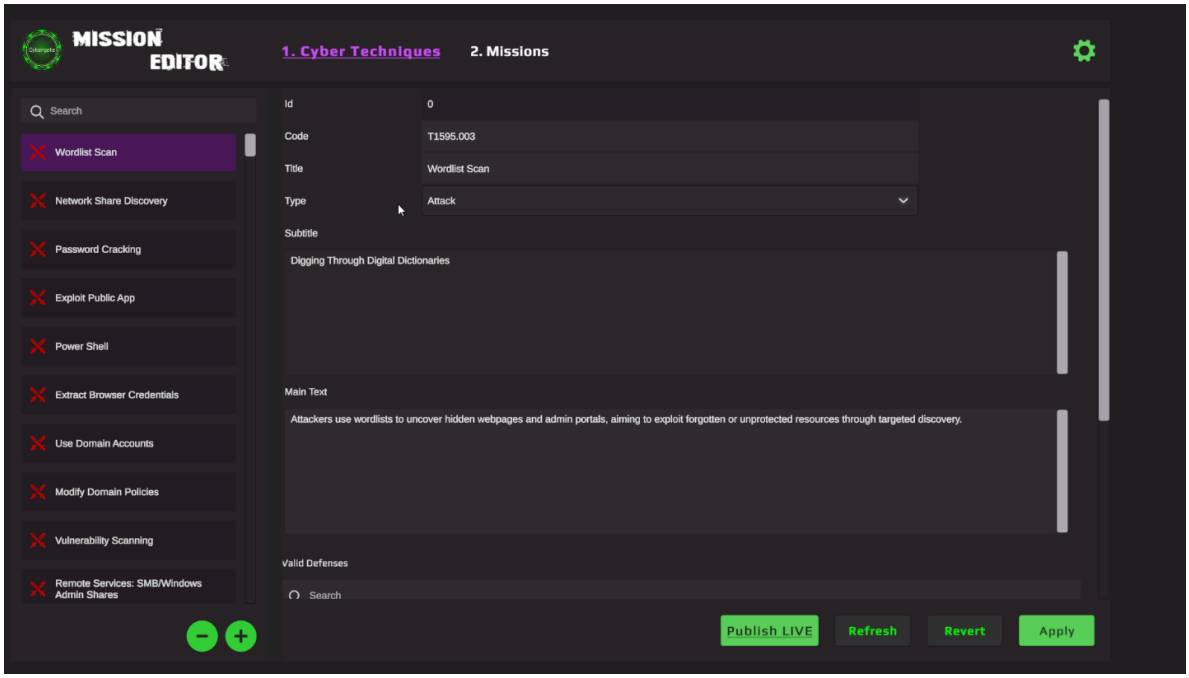

Figure 2: MCMS Cyber Technique Library - technique metadata and publishing controls

2.2 Cyber Technique Library Management

The Cyber Technique Library is the authoritative repository for all attack techniques available within the Cybergate platform. Administrators can manage this library through the MCMS, with full create, read, update, and delete capabilities for each technique entry.

© CYberSynchorny, 2024

Each technique entry in the library captures the following attributes:

- Technique identifier and name (aligned with MITRE ATT&CK nomenclature, e.g., T1110 for Brute Force)
- Tactic category (e.g., Initial Access, Credential Access, Lateral Movement, Impact)
- Technique description and educational context
- Difficulty rating and expected player engagement duration
- Associated mini-game mechanic type (e.g., password cracking, phishing simulation, lateral movement puzzle)
- Sector applicability flags (enterprise IT, industrial/OT, hybrid environments)

By maintaining a centralized, manageable technique library, the MCMS ensures that new MITRE ATT&CK techniques can be incorporated into the platform as they are published, keeping training content current with the evolving threat landscape. For the CYberSynchrony context, this means that techniques specifically relevant to the European threat environment, such as those targeting EU critical infrastructure sectors or exploiting regulatory compliance gaps, can be prioritized and brought into training missions without delay.

2.3 Defense Library Management

Parallel to the technique library, the MCMS provides a complete defense library management interface. This library catalogs all defensive controls available during the Defense and Dome phases of Cybergate gameplay, maintaining their mappings to the attack techniques they mitigate.

Each defense entry includes:

- Defense name and identifier (aligned with MITRE D3FEND mitigations)
- Description of the defensive control and its real-world implementation context
- Technique mitigation mappings: which MITRE ATT&CK techniques this defense counters
- Resource cost configuration: the defensive budget units required to deploy this control
- Defense multiplier: a configurable weight determining the effectiveness of this defense against specific techniques
- Applicability context: whether the defense applies to enterprise IT, OT environments, or both

The ability to manage defense multipliers is particularly significant from a pedagogical standpoint. By adjusting the relative effectiveness of different defenses, MCMS administrators can tune the platform to reflect the specific defensive posture and resource constraints of target organizations. For example, a mission designed for a national health authority might assign higher effectiveness to patient data segmentation controls, while a mission for an energy sector operator might weight OT network isolation more heavily. This configurability ensures that Cybergate trains decision-making skills that are directly applicable to each learner's real-world context.

2.4 Mission Library and Authoring

The mission library module provides the complete mission authoring environment within the MCMS. Trainers can create new missions from scratch or clone existing missions to create variants, using a structured authoring workflow that guides them through each dimension of mission configuration.

Mission authoring encompasses:

- Basic metadata: mission title, version, difficulty tier, target sector, and narrative framing
- Technique selection: choosing from the technique library to populate the attack chain
- Defense configuration: selecting available defensive controls and configuring resource constraints

© CYberSynchorny, 2024

- Narrative assignment: linking briefing texts, contextual backgrounds, and attacker personas to the mission
- Stage and objective definition: structuring the mission into phases aligned with the Mandiant attack lifecycle
- Asset mapping: assigning techniques to specific simulated infrastructure components
- Scoring calibration: setting point values, time allocations, and defense multipliers for the mission

The mission authoring interface is designed to be accessible to content experts who understand cybersecurity but are not software developers. The workflow is guided and validates configurations in real time, preventing the creation of incomplete or inconsistent missions. Completed missions are published directly to the backend, where they become immediately available to the game engine without requiring a software release cycle.

This frictionless content pipeline is central to the platform's adaptability. When a new threat campaign targeting European infrastructure is identified — whether a ransomware wave affecting healthcare, a supply chain attack on EU institutions, or a phishing campaign targeting public servants — a new mission can be authored, validated, and deployed to active training sessions within hours, not weeks.

2.5 Attack Chain and Stage Management

The attack chain manager is one of the most technically sophisticated modules within the MCMS. It provides granular control over the construction of the mission's adversarial narrative, ensuring that each mission models a realistic, coherent intrusion progression rather than an arbitrary collection of techniques.

The attack chain is organized into distinct stages corresponding to phases of the Mandiant Attack Lifecycle, as established in D6.2: Initial Reconnaissance, Initial Compromise, Establish Foothold, Escalate Privileges, Internal Reconnaissance, and Complete Mission. Within each stage, administrators can:

- Add and sequence specific MITRE ATT&CK techniques from the library
- Define attacker objectives for the stage (what the attacker is trying to achieve)
- Configure per-technique log entries that are revealed to players during gameplay, providing contextual clues and educational narration
- Set notepad entries per technique: brief, in-game reference cards that help players understand the technique's significance
- Adjust stage timing and point allocation to control mission pacing and difficulty

The staged structure is critical for pedagogical effectiveness. By experiencing the attack chain stage by stage, first as an attacker executing each technique, then as a defender analyzing the resulting chain, learners develop an intuitive understanding of how isolated techniques combine into a coherent intrusion. This understanding, of how reconnaissance enables initial access, how credential theft enables lateral movement, and how lateral movement enables ransomware impact, is the kind of operational situational awareness that distinguishes effective defenders from those who respond to symptoms rather than root causes.

2.6 Asset and Defense Assignment

The asset and defense assignment modules provide the spatial and relational structure that anchors the attack chain to a realistic infrastructure context. Rather than experiencing techniques in the abstract, players interact with a simulated environment in which each technique targets a specific infrastructure component.

The asset assignment module allows techniques within a mission to be associated with specific system assets such as:

- End-user workstations and laptops

© CYberSynchorny, 2024

- Domain controllers and authentication servers
- File servers and data repositories
- Network devices (routers, firewalls, switches)
- OT controllers and SCADA systems (for industrial missions)
- Cloud-hosted services and APIs

This mapping provides the visual and contextual grounding that makes Cybergate's gameplay feel operationally realistic rather than abstract. When a player executes a lateral movement technique, they see it propagate from a workstation to a domain controller; when they deploy network segmentation as a defense, they see the lateral movement path interrupted.

The defense assignment module establishes the mitigation relationships: which defensive controls neutralize which attack techniques, and with what multiplier weighting. These assignments are the computational foundation of the Defense Phase scoring engine. Administrators can configure defense assignments at the mission level, overriding library defaults to create scenario-specific defensive landscapes that reflect the constraints and capabilities of target organizations.

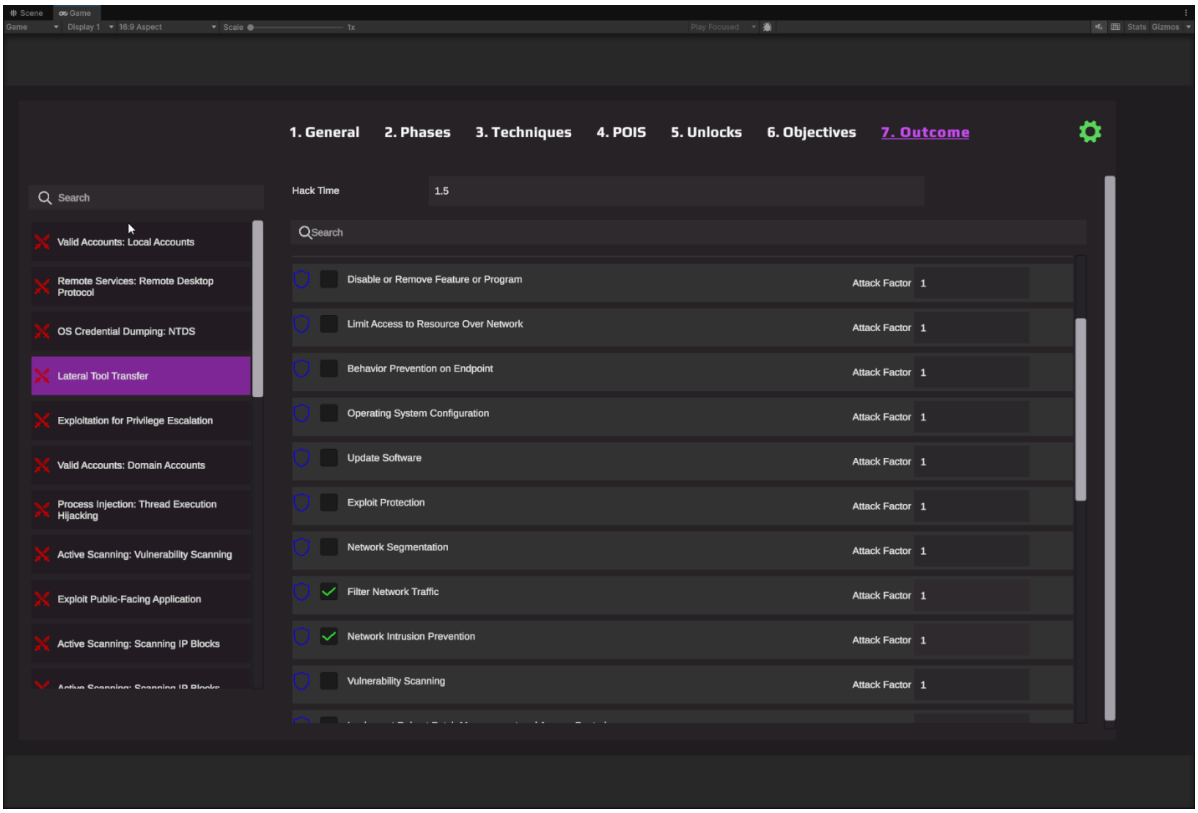

Figure 3: Defense mapping and multiplier configuration by attack technique

2.7 Configuration and Scoring Parameters

The final MCMS module provides the quantitative configuration layer that governs how missions play out in terms of time, points, and difficulty. Administrators can configure the following parameters for each technique and defense within a mission:

© CYberSynchorny, 2024

- Time allocation per technique: the duration available to players to complete each mini-game during the Attack Phase
- Points awarded per technique: the score value of successfully executing each attack step
- Defense multiplier per defense technique: the effectiveness weight of each defensive control against the techniques it counters
- Resource budget: the total defensive resources available to the defender team during the Defense Phase
- Dome action effects: the impact weight of the mission's strategic keystone defense option

These parameters collectively determine the mission's difficulty profile, its pacing, and the scoring dynamics that drive the Outcome Phase evaluation. By making all of these parameters configurable through the MCMS, the platform allows training administrators to calibrate mission difficulty progressively across a learning cohort, ensuring that early missions build foundational confidence while later missions challenge experienced practitioners with realistic resource constraints and multi-vector threat scenarios.

2.8 Deployed Mission Catalogue

The v2 content package comprises ten mission briefs arranged as three progressive campaign arcs. Each brief defines the threat actor, expected duration, difficulty, attack path, infrastructure, defensive concepts, learning objectives, and MITRE ATT&CK-aligned reference material. This content demonstrates how the MCMS data model is populated with concrete, reusable training scenarios.

Table 3. Missions & Primary Learning focus

Mission	Threat actor / campaign arc	Duration / difficulty	Primary learning focus
Mission 1: Initial Breach	Generic APT 1 — Corporate Network Compromise	90 minutes Foundational	neglect that an attacker is patient enough to find
Mission 2: The Lateral Move	Generic APT (post-compromise) 1 — Corporate Network Compromise	120 minutes Intermediate	once attackers have any credential, every credential is at risk
Mission 3: Domain Exploitation	Generic APT (advanced persistence) 1 — Corporate Network Compromise	150 minutes Advanced	once an attacker can forge tickets, they no longer need to compromise users
Mission 4: The Impact	Generic APT / Ransomware operator 1 — Corporate Network Compromise	180 minutes Advanced (Crisis Response)	by the time the attacker presses the button, almost every option you wish you had is gone
Mission 5: Breaking Into the Factory	Industrial APT 2 — Industrial Compromise	90 minutes Intermediate	OT security begins long before the OT network. By the time the attacker reaches the factory floor, the battle has usually already been lost on the desk of someone in HR
Mission 6: Manipulating the Machines	Industrial APT (OT-capable) 2 — Industrial Compromise	120 minutes Advanced	the IT/OT boundary is not a network design choice. It is the difference between an incident and a disaster
Mission 7: Shutdown Sequence	Industrial APT (Impact Phase) 2 — Industrial Compromise	150 minutes Advanced (Crisis Response)	industrial cyberattacks are no longer measured in megabytes of data lost; they are measured in production stoppages, equipment damage, and safety incidents

© CYberSynchorny, 2024

Mission 8: TA577 — Initial Access Broker	TA577 3 — The Multi-Actor Attack Chain	90–120 minutes Advanced	modern cybercrime is not a single attacker against a single victim. It is a marketplace, with specialization, division of labor, and a clearinghouse for compromised access
Mission 9: APT29 — Cloud and Active Directory Compromise	APT29 (Cozy Bear / NOBELIUM / The Dukes) 3 — The Multi-Actor Attack Chain	120–180 minutes Expert	the most dangerous intrusions don't look like intrusions. They look like trusted users behaving normally
Mission 10: LockBit — Ransomware Deployment	LockBit (Ransomware-as-a-Service) 3 — The Multi-Actor Attack Chain	90–150 minutes Expert (Crisis Response)	the same access, the same credentials, the same network — and a completely different attack, because the threat actors' goals are completely different

The catalogue progresses from foundational corporate compromise (Missions 1-4), through industrial IT/OT intrusion and impact (Missions 5-7), to a multi-actor chain in which TA577 brokers access that is subsequently exploited by APT29 for espionage and LockBit for ransomware (Missions 8-10). This progression supports increasing difficulty while showing how early control failures compound across later stages.

© CYberSynchorny, 2024

3 Cybergate Engine and Editor Enhancements

3.1 Live Backend Data Integration

The most consequential enhancement to the Cybergate Unity engine in D6.6 is the introduction of live backend data retrieval. The game engine now communicates directly with the MCMS backend API to fetch mission content at runtime, replacing the static, pre-packaged content approach used in the D6.2 prototype.

Custom Unity editor modules were developed specifically to handle this backend communication. These modules provide development-time tooling for browsing the technique library, previewing mission structures, and loading backend content directly into the Unity editor environment. During development, mission authors can inspect the full MCMS content catalog from within Unity, select missions for testing, and observe how backend-defined parameters are reflected in the game engine's behavior.

At runtime, the game engine retrieves the active mission's complete data package from the backend at session initialization: attack chain definition, technique mini-game parameters, defense options, asset mappings, scoring configuration, and narrative content. This live retrieval ensures that players always experience the most current version of each mission, incorporating any updates or corrections applied through the MCMS since the previous session.

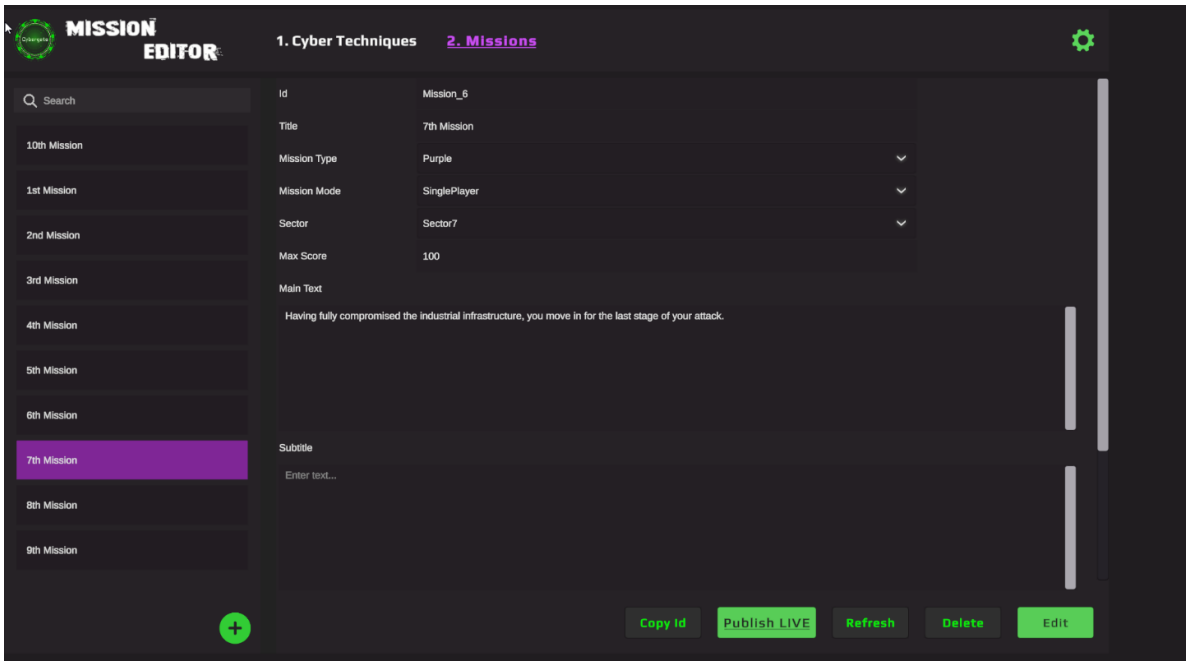

Figure 4: MCMS Mission Library - mission selection, metadata, and publishing workflow

This architecture eliminates the synchronization overhead that was a known limitation of the prototype system. In D6.2, any change to mission content required a coordinated update between content teams and developers, followed by a software release. With live backend integration, content teams operate entirely through the MCMS; changes are immediately available to the engine without any developer involvement. This separation of concerns is fundamental to the platform's long-term maintainability and its ability to serve an active, evolving training program across the CYberSynchrony project's deployment lifetime.

© CYberSynchorny, 2024

3.2 Dedicated Mission Authoring Executable

In the final version of the Cybergate platform, the MCMS editor interface is made available as a standalone executable (.exe) file, independent of the full Unity development environment. This represents a significant step in making mission authoring accessible to the full range of stakeholders involved in the CYberSynchrony training program.

The standalone executable packages the MCMS interface in a self-contained application that can be installed and operated on standard workstations without Unity licensing requirements or technical onboarding. Target users include:

- Cybersecurity trainers and educators who design mission content based on domain expertise rather than software skills
- WP6 task leaders and training coordinators who need to review and approve mission content before deployment
- Partner organization representatives who wish to contribute sector-specific mission scenarios reflecting their operational context
- Project management staff responsible for aligning training content with GA deliverable requirements

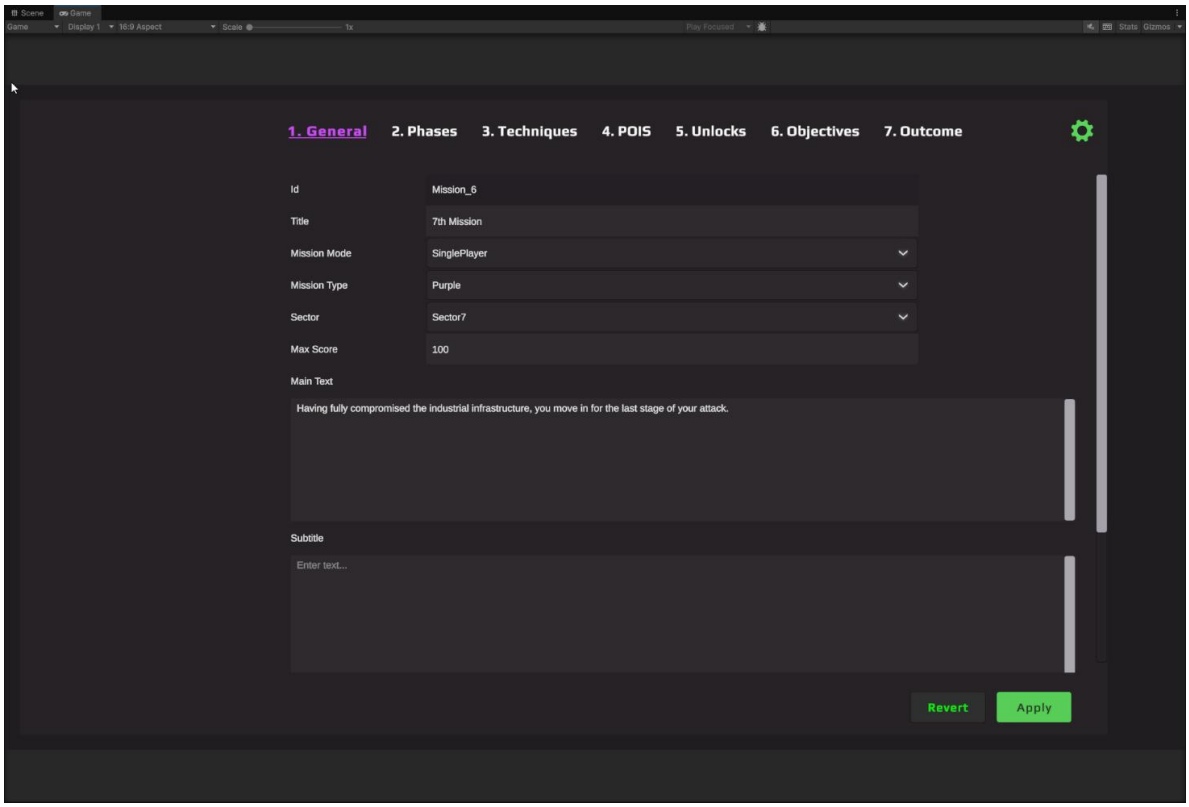

Figure 5: Dedicated authoring interface - general mission configuration

The executable connects to the MCMS backend via standard HTTPS, with role-based authentication ensuring that only authorized users can access content management functions. Changes made through the executable are immediately propagated to the backend and become available to active game engine instances without any intermediary steps.

This tool is a critical enabler for the project's broader ambition of making Cybergate adaptable to EU partner needs. Partners across the CYberSynchrony consortium, national authorities, academic institutions, and industry

© CYberSynchorny, 2024

partners, can contribute mission content reflecting their specific threat environments and organizational contexts, using a tool that requires no technical background beyond cybersecurity expertise.

3.3 Backend Infrastructure

The backend infrastructure supporting D6.6 combines a PHP-based REST API server with SFTP-based file management for large binary assets, deployed in a cloud-ready architecture designed for reliability and scalability.

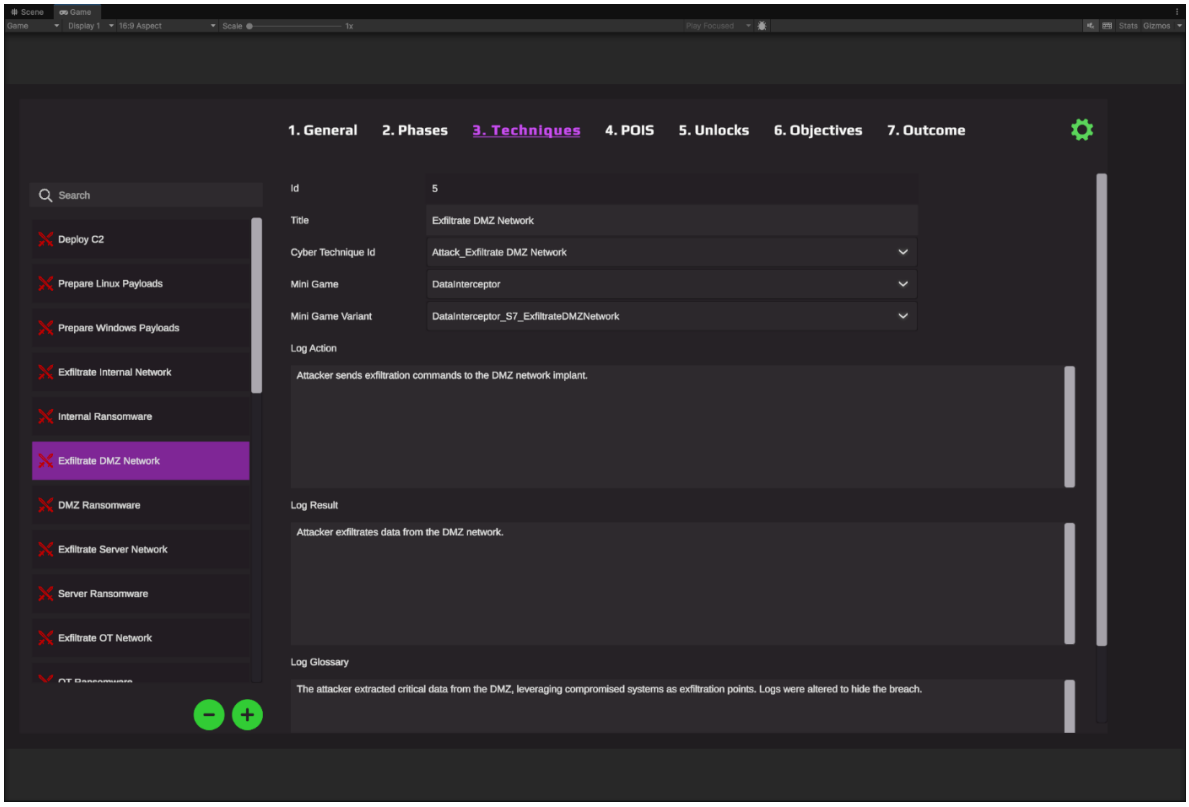

Figure 6: Technique authoring. minigame mapping and log content

The PHP API provides RESTful endpoints for all MCMS operations: creating and updating technique and defense library entries, publishing missions, fetching mission data for game engine initialization, and submitting player outcome analytics. PHP was selected for its broad hosting compatibility, straightforward deployment, and established security model with appropriate hardening.

For large binary assets, game graphics, environmental textures, audio files, and scenario media, the backend uses SFTP-based file transfer. This hybrid approach combines the flexibility of a web API for structured data with the throughput characteristics required for media-heavy content. Asset files are referenced by identifier within the API's JSON responses and fetched separately by the game engine during session initialization.

A dedicated development backend environment mirrors the production architecture, providing a safe sandbox for testing new missions and validating backend integrations before rollout. The dual-environment model, consistent with the operational and simulation environments described in D6.2, ensures that development and testing activities never impact live training sessions.

The backend is designed for cloud hosting with stateless API architecture enabling horizontal scaling. Role-based access controls restrict content management capabilities to authorized users, while all API

© CYberSynchorny, 2024

communications are encrypted via TLS. Audit logging captures all content modification operations, providing accountability and traceability for mission content changes.

© CYberSynchorny, 2024

4 Integration with the CYberSynchrony Platform

4.1 Integration Architecture

The planned integration of Cybergate with the CYberSynchrony platform is an important step that transforms the game from a standalone training tool into a connected component of the project's modular cybersecurity framework. This transition is directly aligned with the architectural vision expressed in the GA: a cohesive, modular platform through which users can "access and purchase the various modules of the Modular framework" (T6.1), with Cybergate serving as the gamified training module within that ecosystem.

From an operational perspective, participants first log in to the CYberSynchrony platform using their assigned user accounts. Following the instructions provided by the responsible trainer or training coordinator, authorized participants then enter the Cybergate game environment for the relevant training session. Access to the game is controlled according to the approved training schedule: the environment is activated only during the predefined dates and time windows in which training activities are conducted. Outside these scheduled periods, the game environment remains unavailable to participants. This operating model supports supervised access, cohort coordination, and consistent delivery of each training session.

The integration architecture is loosely coupled, ensuring that Cybergate remains independently operable for organizations that deploy it in standalone contexts, while enabling the richer, integrated experience available within the full CYberSynchrony ecosystem. Key integration touchpoints include:

- Platform-based participant access: learners log in to CYberSynchrony and enter the Cybergate environment only when instructed by the responsible trainer and while the scheduled training window is active
- Learner analytics pipeline, enabling Cybergate outcome data (mission scores, technique recognition rates, defense choices, team coordination patterns) to feed into the project's unified learning analytics infrastructure
- Threat intelligence ingest, connecting WP3's risk assessment and dynamic parameter refinement outputs to the MCMS, enabling threat intelligence to directly inform mission content updates
- Training planning coordination, linking Cybergate session scheduling and progress tracking to the T6.3 training planning framework

© CYberSynchorny, 2024

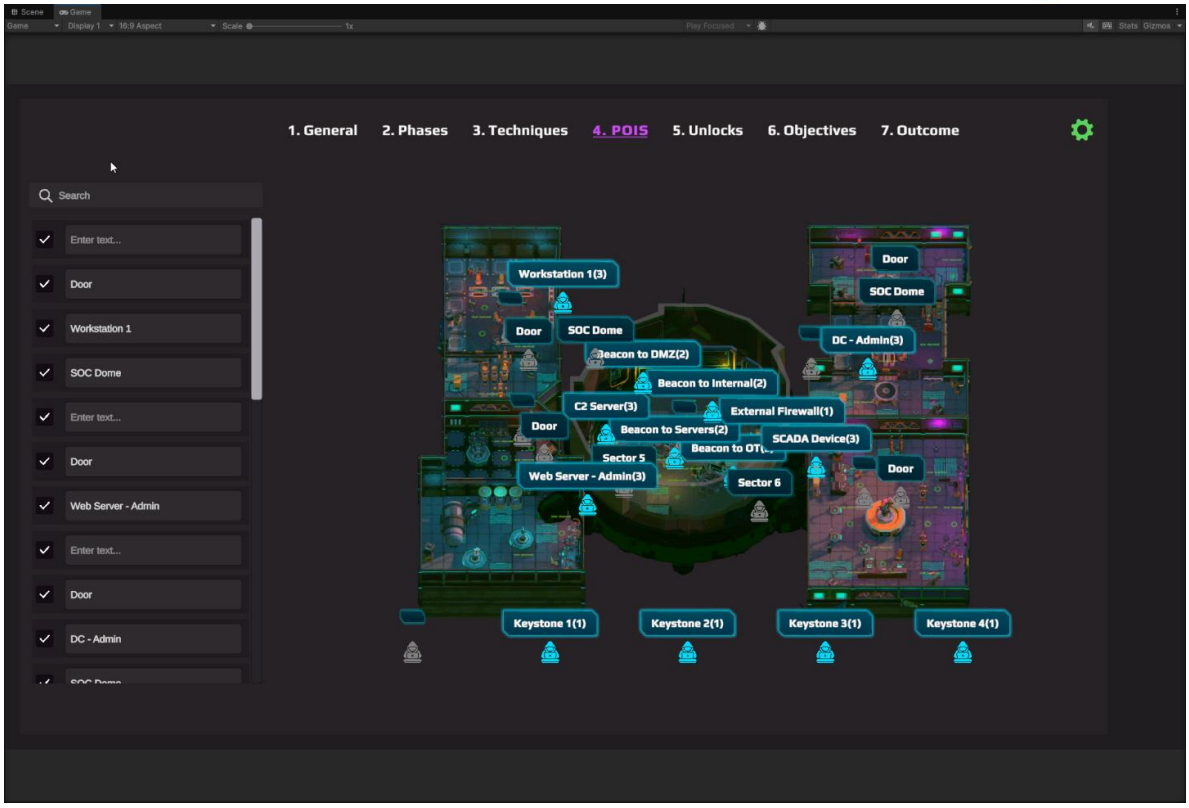

Figure 7: Corporate-environment point-of-interest and asset assignment

4.2 Data Flow and Synchronization

Data flows between Cybergate and the CYberSynchrony platform operate bidirectionally, with different synchronization cadences appropriate to each data type.

Outbound flows from Cybergate to the platform include:

- Real-time learner session data: mission starts, phase transitions, technique execution outcomes, defense selections, and Dome choices
- Post-session analytics packages: mission completion records, team scores, individual performance breakdowns, and outcome replay data
- Aggregated skill gap indicators: patterns of consistently failed defenses or misidentified techniques that signal training needs
- Mission utilization metrics: which missions are deployed most frequently, by which organizations, and with what outcomes

Inbound flows from the platform to Cybergate include:

- User profile and role data: learner identities, cohort assignments, and training history for personalization
- Threat intelligence updates from WP3: new risk parameters, updated threat profiles, and emerging technique identifiers for MCMS incorporation
- Defense mapping updates from WP4: refined mitigation relationships as the automated response toolkit evolves
- Training schedule and cohort assignments from T6.3: which groups should experience which missions, in what sequence

© CYberSynchorny, 2024

Synchronization is managed through a combination of scheduled batch synchronization for historical analytics and event-driven updates for real-time flows. All integration interfaces use TLS encryption, token-based API authentication, and audit logging, meeting the security standards appropriate for a project operating within Europe's cybersecurity landscape.

4.3 Adaptability to EU Project Needs

The combination of the MCMS and platform integration gives Cybergate a capability that is uniquely aligned with the CYberSynchrony project's EU mandate: the ability to adapt training scenarios continuously to reflect the specific cybersecurity challenges facing European institutions, Member States, and critical infrastructure operators.

This adaptability operates through a well-defined workflow that connects the EU threat environment to deployed training missions:

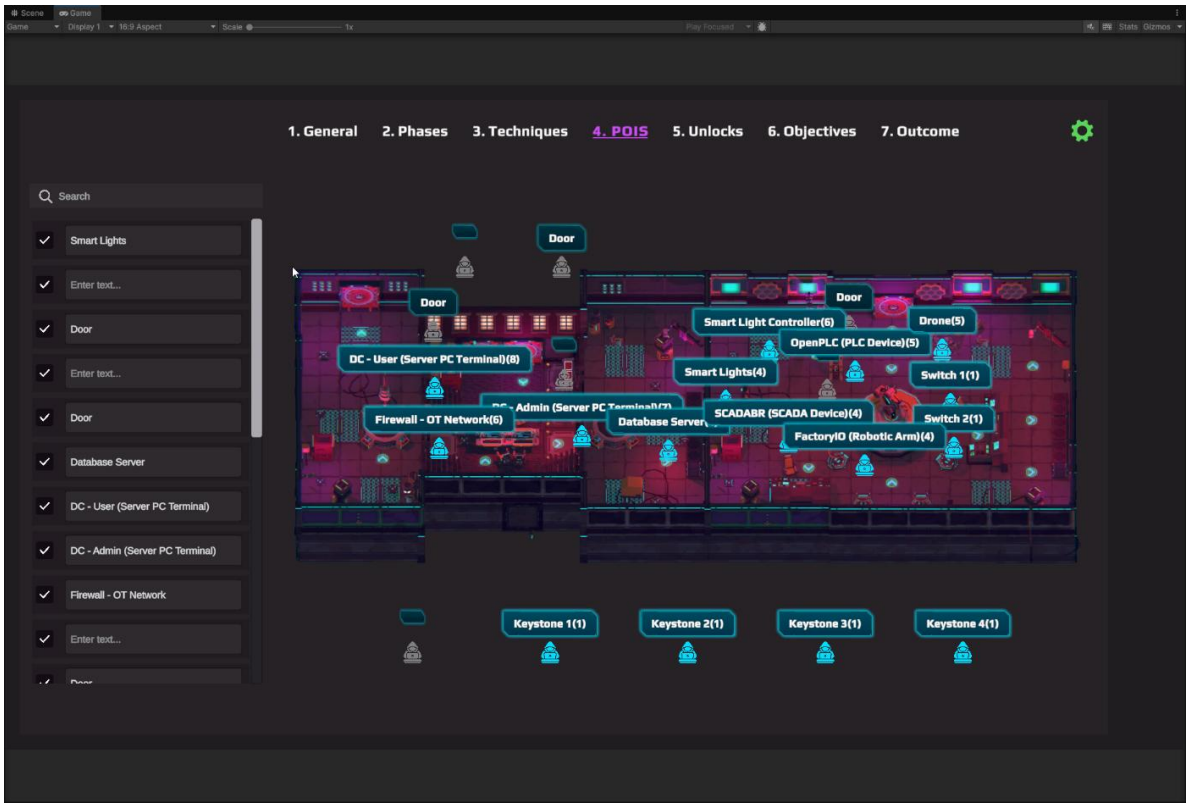

Figure 8: Industrial/OT point-of-interest and asset assignment

Concretely, this means that:

- When ENISA publishes updated threat landscape reports identifying new attack vectors targeting EU critical infrastructure, those techniques can be added to the Cybergate technique library via the MCMS and incorporated into new or updated missions within days.
- When a partner organization such as a national cybersecurity authority identifies a sector-specific threat pattern, their staff can use the standalone .exe to author a mission reflecting that scenario without waiting for developer support.
- When the WP3 risk assessment tools identify elevated risk profiles for specific attack techniques in a target organization's context, those techniques can be weighted more heavily in the missions deployed to that organization's training cohort.

© CYberSynchorny, 2024

- When new NIS2 compliance requirements or sector-specific regulations create new defensive priorities, those can be reflected in the defense library and incorporated into training scenarios that teach compliance-aligned defensive decision-making.

This adaptive capability is what distinguishes Cybergate v2 from a conventional fixed training product. Rather than delivering a static set of scenarios, it provides a living training environment whose content evolves alongside the threat landscape it models. In the context of the CYberSynchrony project's goal of equipping European society with effective cybersecurity training mechanisms, this adaptability is not a feature — it is the foundational capability upon which long-term relevance and impact depend.

© CYberSynchorny, 2024

5 Conclusions

D6.6 delivers the second and final operational version of the Cybergate gamified cybersecurity training platform, fulfilling the Grant Agreement commitment for Gamified Training Modules v2 under WP6 of the CYberSynchrony project. The deliverable advances the platform across three interconnected dimensions that collectively transform it from a structured prototype into a operationally integrated, dynamically adaptable training environment.

The Mission Content Management System is the deliverable's most consequential contribution. By providing a comprehensive, role-based administrative interface for managing the full lifecycle of training content, from technique and defense libraries to mission authoring, attack chain construction, asset assignment, and scoring configuration, the MCMS gives the platform its defining adaptive capability. Mission content can be updated, extended, and tailored to specific organizational or sector needs without touching the game engine. This is the mechanism through which Cybergate remains relevant as threats evolve, as project contexts change, and as different Member States and critical infrastructure sectors require tailored training scenarios. The MCMS is what makes the EU project's investment in Cybergate a durable one.

The engine and editor enhancements documented in Chapter 3 provide the technical foundation for this adaptability. Live backend data integration ensures that every training session draws on the most current mission content, while the standalone authoring executable democratizes mission creation by making it accessible to domain experts without software development backgrounds. Together, these capabilities close the loop between content design and gameplay delivery, eliminating the coordination overhead that would otherwise impede rapid content iteration.

Platform integration, documented in Chapter 4, anchors Cybergate within the broader CYberSynchrony ecosystem. Shared authentication, cross-module analytics, and threat intelligence ingest from WP3 and WP4 ensure that the training environment is connected to the project's operational infrastructure and can benefit from the outputs of other work packages. The EU-aligned mission adaptation workflow described in Section 4.3 provides a concrete model for how the platform's adaptability can be exercised in practice, from ENISA threat reports to deployed training missions.

Looking forward, the Cybergate platform established by D6.6 provides a strong foundation for future development. Areas for continued investment include adaptive learning pathways informed by the analytics pipeline, expanded mission libraries covering emerging threat vectors such as AI-assisted attacks and cloud-native intrusions, deeper integration with the project's collaborative incident response tools from WP5, and the development of sector-specific mission packs tailored to the EU's critical infrastructure protection priorities.

In conclusion, D6.6 delivers a gamified training system that is technically robust, pedagogically grounded, and strategically positioned to serve the CYberSynchrony project's mission of equipping European society with the awareness, skills, and resilience needed to face modern cyber threats. The platform's adaptability, its ability to bring training scenarios continuously closer to the specific threats and needs of its users, is its most important quality, and it is the quality that will determine its long-term impact.

© CYberSynchorny, 2024

6 References

Accessible Rich Internet Applications (WAI-ARIA) Authoring Practices, W3C. (n.d.). Retrieved from https://www.w3.org/WAI/ARIA/apg/

https://d3fend.mitre.org/

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 (NIS2 Directive). (n.d.). Retrieved from https://nis2directive.eu/

European Cybersecurity Skills Framework (ECSF), ENISA. (n.d.). Retrieved from https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf

Keycloak – Open Source Identity and Access Management. (n.d.). Retrieved from https://www.keycloak.org/

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). (n.d.). Retrieved from https://gdpr-info.eu/

Web Content Accessibility Guidelines (WCAG) 2.1, World Wide Web Consortium (W3C). (n.d.). Retrieved from https://www.w3.org/TR/WCAG21/

© CYberSynchorny, 2024