Harmonizing People, Processes, and Technology for Robust Cybersecurity

D6.2 Gamified Training Modules v1

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 v1		
Work Package	WP6 Cybersecurity Consciousness: Empowering Society Through Awareness (CYBERWISE and Cybersecurity Standardization and Compliance Reinforcement (CYBERGOPLUS)		
Contractual due date	31.12.2025	**Actual submission date**	15.12.2025
Type	R -Document, report	**Dissemination Level**	Public
Lead Beneficiary	Focal Point (FP)		
Responsible Author	Koutras Dimitris (FP)		
Contributions from	Malamas Vangelis (FP)		

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	17.07.2025	Initial Deliverable structure	Koutras Dimitris (FP)
0.2	02.08.2025	Deliverable Structure Finalization	Malamas Evangelos (FP)
0.3	09.09.2025	First contribution	Koutras Dimitris, Malamas Evangelos (FP)
0.4	20.10.2025	Contribution	Malamas Evangelos, Koutras DImitris (FP)
0.5	01.12.2025	Final draft ready for internal review	Koutras Dimitris, Malamas Evangelos (FP)
0.6	05.12.2025	Peer review 1	Leandros Maglaras (TRUST)
0.6	06.12.2025	Peer review 2	Evangelos Michos (IANUS)
0.7	09.12.2025	Final draft addressing comments from internal review	Koutras Dimitris, Malamas Evangelos (FP)
0.8	11.12.2025	Final quality check	Eleni Keliri (EBOS)
1.0	12.12.2025	Final version ready for submission	Koutras Dimitris (FP)

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 6
1.2 Linkage to other project outputs 7
1.3 Deliverable Structure 8
2 Architecture of the Gamified Training Environment 9
2.1 Overview of the Cybergate Architecture 9
2.2 Diagram Representation 10
2.3 Mission Architecture & Game Flow 11
2.4 Technical Infrastructure 11
3 Design of Gamified Training Modules 13
3.1 Methodology for Mission and Module Design 13
3.2 Playbook-Inspired Module Execution Flow 15
3.3 Case Studies – Mission Structure and Examples 16
3.4 Mechanics of Learning Through Progression 18
4 Deployment Strategy and Validation 20
4.1 Deployment Environment 20
4.2 Testing & Validation of Gamified Modules 21
4.3 Summary of Deployment and Validation Approach 23
5 Conclusions 24
6 References 25

List of Figures

Figure 1 Main tactic 12
Figure 2 Attack succeeded 14
Figure 3 Attack no result 14
Figure 4 Game graphics 16
Figure 5 Mitre 17
Figure 6 Game example 18
Figure 7 Game example 20
Figure 8 Game example 22

List of Tables

Table 1: Adherence to CYberSynchrony's GA 6
Table 2: Links to other Project Outputs/Work 7

© 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
C&C	Command and Control
DCO	Defensive Cyber Operations
DLP	Data Loss Prevention
EDR	Endpoint Detection and Response
FP	Focal Point
IaC	Infrastructure as Code
IDS	Intrusion Detection System
IOC	Indicator of Compromise
JSON	JavaScript Object Notation
KQL	Kusto Query Language
MITRE	MITRE Corporation
MFA	Multi-Factor Authentication
POI	Point of Interest
REST	Representational State Transfer
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
Sysmon	System Monitor
TTPs	Tactics, Techniques, and Procedures
UEBA	User and Entity Behaviour Analytics
UPN	User Principal Name
VM	Virtual Machine
YAML	YAML Isn’t Markup Language

© CYberSynchorny, 2024

Executive Summary

D6.2 titled "*Gamified Training Modules v1"* is part of Work Package 6 (WP6), which focuses on strengthening cybersecurity awareness, skill development, and institutional readiness across society through interactive, engaging, and technically grounded learning experiences. This deliverable contributes to that objective by designing and implementing Cybergate. Cybergate is an immersive, game-based cybersecurity training platform that integrates offensive and defensive cyber concepts using established threat-intelligence frameworks and realistic adversary behaviors. It provides a structured, repeatable, and scalable method for training users in cyber incident detection, decision-making, and coordinated response.

The work carried out under this deliverable includes the development of a comprehensive set of gamified training missions, each modeled on real cyber intrusion patterns aligned with the MITRE ATT&CK and MITRE D3FEND frameworks. These missions simulate full-spectrum attack lifecycles, from reconnaissance and initial compromise to lateral movement, impact, and recovery inhibition. Participants engage first as attackers through interactive mini-games and then as defenders applying resource-limited countermeasures, thus reinforcing the principle that understanding adversary tactics directly improves defensive posture. This offense-to-defense model is strengthened by the platform's structured four-phase mission flow: Attack, Defense, Dome, and Outcome, which mirrors the Mandiant intrusion lifecycle and provides learners with a realistic operational context.

The gamified training modules developed in D6.2 are underpinned by a modular technical architecture that separates mission content from the core engine, enabling rapid updates, scenario customization, and seamless expansion to additional sectors. The system supports multiplayer coordination, real-time state synchronization, and secure sandboxed simulation environments, ensuring that training can scale from small teams to large organizational cohorts. This architecture also integrates detailed analytics that allow trainers to monitor participant performance, identify persistent skill gaps, and iteratively refine mission difficulty and defensive learning objectives.

Findings from the development and early testing of the Cybergate modules show significant improvements in learner engagement, situational awareness, and the ability to recognize and prioritize critical threat indicators. The combination of interactive challenges, structured reflection, and mission-specific scoring reinforces technical understanding while also improving decision-making under pressure—an essential capability for modern security teams. The platform's mission progression model ensures that trainees are guided from foundational concepts to advanced attack-defense scenarios, gradually building confidence and practical skill.

The purpose of this deliverable is to provide the first operational version of CYberSynchrony's gamified training environment, establishing the foundation for broader deployment across WP6 cybersecurity awareness initiatives. This version forms the basis for future enhancements, including expanded mission libraries, adaptive learning pathways informed by gameplay analytics, and deeper integration with the project's collaborative training tools. The work completed in D6.2 directly supports the long-term objective of CYberSynchrony: equipping citizens, professionals, and organizations with engaging and effective training mechanisms that strengthen Europe's collective cyber resilience.

© CYberSynchorny, 2024

1 Introduction

Work Package 6 (WP6) of the CYberSynchrony project focuses on strengthening cybersecurity awareness, building resilient digital skills, and enabling users across society to better understand, anticipate, and mitigate cyber threats. Deliverable D6.2 *"Gamified Training Modules v1"* provides the first operational version of an interactive, game-based training environment designed to improve cybersecurity readiness through immersive, scenario-driven learning. The development of this deliverable is based on the Cybergate platform, which combines threat-informed content, mission-based learning, and a technically grounded simulation architecture to enhance both individual and team-based defensive capabilities.

Cybergate integrates offensive and defensive cyber concepts within a unified, gamified environment, allowing trainees to experience the full lifecycle of a cyber intrusion in a controlled and educational format. By aligning its missions with industry-standard frameworks such as **MITRE ATT&CK**, **MITRE D3FEND**, and the **Mandiant Attack Lifecycle**, the training modules expose users to realistic adversary tactics, techniques, and procedures (TTPs), while simultaneously teaching the defensive strategies necessary to counter them. This dual perspective (first experiencing the attacker's path, then executing the defender's response), provides a comprehensive and intuitive understanding of cyber operations that traditional training approaches often fail to deliver.

The gamified modules developed for D6.2 cover the complete spectrum of a targeted attack, enabling participants to observe how seemingly minor early-stage intrusions evolve into significant operational impacts if not properly mitigated. Missions are organized into multi-phase cycles (Attack, Defense, Dome, Outcome) that correspond to real-world intrusion patterns. The platform's progression system gradually increases mission complexity, ensuring that participants evolve from foundational understanding to advanced decision-making in later stages of gameplay. Through interactive mini-games, scenario-based defensive planning, and structured after-action reviews, learners develop both technical knowledge and critical thinking skills.

Complementing its educational design, Cybergate is built upon a scalable and modular technical infrastructure. 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 system supports multiplayer interaction, real-time synchronization, and secure sandboxed simulations, ensuring that users can safely engage with realistic threat environments without risk to actual infrastructure. These characteristics make the platform suitable for corporate training, national-level cyber exercises, academic programs, and cross-sector awareness efforts.

1.1 Mapping CYberSynchrony Outputs

This section presents the CYberSynchrony Grant Agreement (GA) commitments relevant to the development of D6.2 and maps them to the corresponding document chapters where these commitments are addressed.

Table 1: Adherence to CYberSynchrony's GA

Component no	Component title	Respective Document Chapter(s)	Justification
DELIVERABLE			
D6.2	Gamified Training Modules v1	Chapters 1, 2, 3, 4	The deliverable designs and implements interactive gamified training missions for cybersecurity awareness and skill-building, aligned with real threat behavior via MITRE

			ATT&CK, MITRE D3FEND, and Mandiant models.
TASKS			
T6.1	Cybersecurity Awareness & Training	Chapters 2, 3	T6.1 focuses on developing awareness resources and training materials. D6.2 contributes by providing a fully functional game-based learning system grounded in threat-informed content and scenario-driven missions.
T6.2	Development of Training Modules and Digital Learning Paths	Chapters 2, 3, 4	D6.2 delivers structured missions, progression systems, and outcome-based learning flows designed to serve as reusable digital training modules suitable for multiple user groups.
T6.3	Gamification and Simulation Environments	Chapters 2, 3, 4	The Cybergate platform directly supports T6.3 by offering a complete simulation and gamification engine, including mini-games, multiplayer coordination, defense planning, and real-time mission analytics.
T6.4	Evaluation, Feedback & Learning Analytics	Chapters 3, 4	D6.2 includes scoring systems, outcome replays, and data-driven analytics to assess learner performance and provide measurable insight into skill development.

1.2 Linkage to other project outputs

D6.2 is closely connected to several deliverables and tasks throughout CYberSynchrony, ensuring that the training modules are technically aligned, threat-informed, and compatible with the project's broader ecosystem.

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	Outputs from WP3 inform the threat scenarios used in Cybergate missions, ensuring training aligns with realistic organizational risks.
WP3	T3.4	D3.4 – Dynamic Risk Parameter Refinement	Risk intelligence produced by WP3 supports the adaptive difficulty and threat modeling within training missions.

© CYberSynchorny, 2024

WP4	T4.3	D4.2 – Automated Response Toolkit	Detection-response logic from WP4 informs the defensive actions available in the Defense and Dome phases, reinforcing consistency across training and operational tools.
WP5	T5.2	D5.2 – Incident Response Collaboration Framework	D6.2 contributes complementary skills-based training that strengthens collaborative decision-making during cyber incidents.
WP6	T6.1, T6.2, T6.3	D6.1 – Cybersecurity Awareness & Training	D6.2 builds on D6.1 by providing actionable, interactive modules that translate awareness concepts into experiential learning.

1.3 Deliverable Structure

This deliverable is organized into four chapters, each addressing a different layer of the design, content, and implementation of the gamified training modules developed in CYberSynchrony:

Chapter 1 – Introduction
Provides an overview of the deliverable's objectives, its alignment with the Grant Agreement, and its linkage to other project outputs.

Chapter 2 – Architecture of the Gamified Training Environment
Describes the technical and pedagogical architecture underlying the Cybergate platform, including mission structuring, mini-game logic, four-phase gameplay flow, and the integration of ATT&CK/D3FEND frameworks.

Chapter 3 – Design of Gamified Training Modules
Presents the methodology for mission development, the conceptual alignment with real-world attack lifecycles, and detailed descriptions of the mission progression systems, learning mechanics, scoring, and outcome evaluation.

Chapter 4 – Deployment Strategy and Validation
Outlines the practical steps required for implementing the gamified training modules across various environments, including organizational pilots, feedback analysis, performance metrics, and roadmap for future enhancements.

© CYberSynchorny, 2024

2 Architecture of the Gamified Training Environment

The architecture of the gamified training modules delivered under D6.2 is designed to create an immersive, scalable, and technically realistic environment for cybersecurity learning. It integrates mission logic, adversary simulation, defensive decision-making, multiplayer collaboration, and structured after-action review, all within a secure, sandboxed framework. This architecture ensures that participants can safely experience the full lifecycle of cyber intrusions and practice defense strategies that reflect real-world conditions [9].

The system is built on the principle that **effective cybersecurity training requires both operational realism and pedagogical structure**. To enable this, the environment combines:

1. **Threat-informed content** aligned with MITRE ATT&CK, MITRE D3FEND, and Mandiant attack lifecycle models.
2. **Modular, data-driven mission definitions**, allowing rapid updates and sector-specific customization.
3. **Interactive gameplay mechanics** that simulate attacker and defender behavior.
4. **A multi-phase scenario engine** (Attack → Defense → Dome → Outcome) grounded in adversarial progression.
5. **Secure, scalable backend infrastructure** for multiplayer interaction and analytics.
6. **A continuous learning feedback loop** integrated into mission scoring and outcome visualizations.

This chapter provides a detailed description of the Cybergate architecture, outlining how its components work together to deliver a coherent, realistic, and pedagogically effective gamified training experience.

2.1 Overview of the Cybergate Architecture

The Cybergate platform is designed as an **end-to-end training ecosystem** that connects offensive simulation, defensive strategy, and structured reflection. Its architecture is intentionally modular to support extensibility, interoperability, and reuse across multiple training contexts.

Core Architectural Components

1. Scenario & Mission Engine

The heart of the environment is a configurable mission engine that loads mission data like attack techniques, defense options, objectives, resource limits, and scoring rules, from structured datasets. Missions are defined in editable formats (e.g., JSON, spreadsheets), enabling trainers to modify or expand content without altering core code.

2. Attack Simulation Layer

During the Attack Phase, players engage with mini-games representing MITRE ATT&CK techniques (e.g., brute force, phishing, lateral movement). These interactions unlock adversary actions that form the attack chain, which the defender team must later counter. This layer exposes learners to attacker behavior in a controlled, pedagogically safe way.

3. Defense Decision Layer

© CYberSynchorny, 2024

The Defense Phase is a collaborative environment where teams select defensive controls mapped to MITRE D3FEND mitigations. Limited resources force prioritization, mirroring real-world incident response constraints. The system calculates mitigation effects against the ATT&CK chain defined in the attack phase.

4. Dome (Strategic Defense) Layer

A distinct "keystone defense" system applies a high-impact, campaign-level defensive action. This layer introduces strategic thinking and translates local incident response into sector-wide or organizational-level interventions.

5. Outcome Replay & Analytics Engine

After defenses are locked in, the system replays the entire attack sequence, displaying which techniques succeeded or failed, how defenses performed, and the team's overall score relative to a realistic maximum. Analytics are logged for instructor review and learner feedback.

6. Multiplayer Networking & Real-Time Synchronization

Cybergate supports team-based play. The architecture includes real-time communication channels to ensure that team actions, defense selections, and mission states are instantly synchronized for all participants.

7. Secure Sandboxed Execution Environment

All attack simulations are virtual and symbolic; no real malicious code is executed. This protects users, organizations, and networks while preserving instructional accuracy.

2.2 Diagram Representation

The system architecture for the gamified training environment is described below.

- **Mission Content Repository** (containing attack techniques, missions, defense mappings);
- **Scenario Engine**, which orchestrates the four-phase gameplay cycle;
- **Attack Simulation Layer** connected to interactive mini-games;
- **Defense & Dome Modules**, responsible for strategic and tactical defensive actions;
- **Outcome Replay Engine**, generating post-mission feedback;
- **User Interface Layer**, presenting gameplay to trainees;
- **Real-Time Collaboration Layer**, enabling multiplayer functionality;
- **Data Logging and Analytics Module**, which records player actions;
- **Secure Backend Infrastructure**, hosting the entire simulation environment.

The architecture emphasizes modularity, enabling updates to mission logic, defense mappings, or threat models without modifying the core execution engine.

© CYberSynchorny, 2024

2.3 Mission Architecture & Game Flow

The mission architecture follows a **four-phase gameplay cycle**, ensuring a consistent, pedagogically sound flow across all missions. This cycle mirrors the structure of real-world intrusion analysis and the logic of adversarial kill chains [4][7].

Attack Phase — Simulating Adversary Behavior

Players simulate attacker actions through mini-games that represent ATT&CK techniques such as credential access (T1110), spearphishing (T1566), lateral movement (T1021), or privilege escalation (T1003). Each successful mini-game unlocks corresponding attack steps that build the threat chain the defender must face later. This exposes learners to adversary intent, progression, and methodology in a safe, controlled format.

Defense Phase — Tactical Decision-Making Under Constraints

Defenders evaluate the discovered ATT&CK chain and select D3FEND-aligned defensive measures (e.g., MFA, segmentation, endpoint hardening). Limited resources enforce prioritization, simulating the realities of operational cybersecurity where budget, time, and personnel are finite.

Dome Phase — Strategic, High-Impact Defense Selection

Teams choose one “keystone defense” that affects the broader scenario or sector environment. These actions represent large-scale mitigations such as system-wide containment, cross-sector information sharing, or coordinated incident response campaigns.

Outcome Phase — Replay, Scoring, and Learning Feedback

The system replays the full attack chain step-by-step, showing which defenses succeeded or failed. A realistic scoring method compares team performance against a best-case achievable defense posture. This structured after-action review reinforces learning through reflection and highlights areas for improvement.

2.4 Technical Infrastructure

The technical infrastructure of Cybergate is engineered to support reliable, secure, and scalable deployment for diverse training contexts.

Modular Content Architecture

- Mission definitions, ATT&CK techniques, D3FEND defenses, and narrative elements are all stored as structured data (e.g., JSON, spreadsheets).
- Trainers can introduce new missions or modify existing scenarios without code changes.

Client–Server Delivery Model

- The client (browser or dedicated app) handles user interface, graphics, and mini-games.
- The server manages mission progression, scoring logic, database storage, and analytics.

Real-Time Multiplayer Support

- Teams collaborate through synchronized actions.
- Web sockets or similar protocols ensure low latency in state updates.

Security & Isolation

© CYberSynchorny, 2024

- No real malware or harmful code is executed.
- All simulations occur within a closed environment, preventing risk to training networks.

Scalability & Deployability

- Cloud-ready backend capable of supporting concurrent training sessions.
- Microservice architecture allows independent scaling of game logic, analytics, and user management.

Analytics & Telemetry

- Every action (attack performed, defense selected, outcome achieved) is logged.
- Trainers can view learner performance patterns and identify skill gaps.
- Data informs future mission tuning and personalized learning paths.

This infrastructure enables Cybergate to operate as a flexible, high-fidelity training platform suitable for organizations, education providers, and national cybersecurity capacity-building.

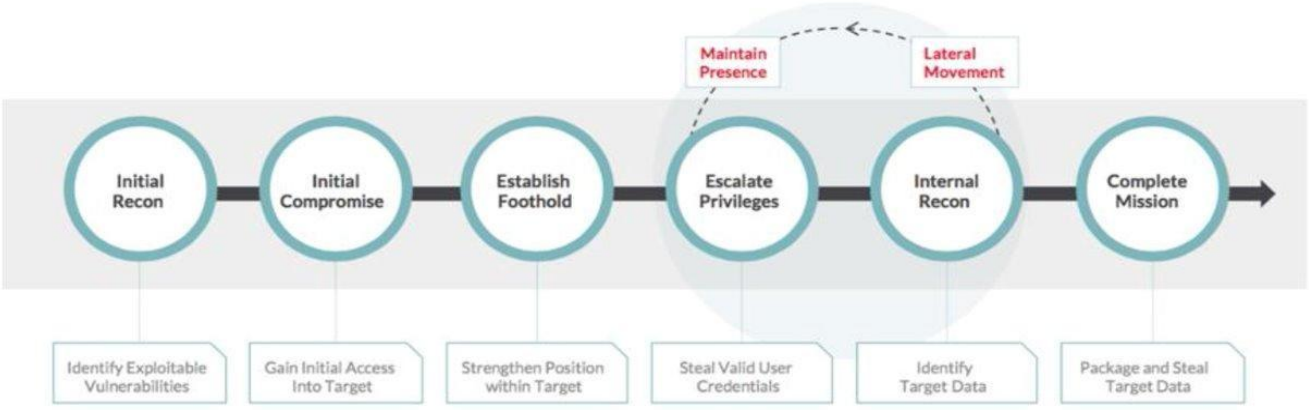

Figure 1 Main tactic

© CYberSynchorny, 2024

3 Design of Gamified Training Modules

The design of the gamified training modules developed in D6.2 follows a structured methodology grounded in real-world cyber threat behavior, pedagogical principles, and scenario-based experiential learning. Each module is conceptualized as a self-contained mission that exposes participants to adversary tactics and then challenges them to deploy appropriate defensive strategies under realistic constraints. The design philosophy treats **offense and defense as interdependent learning dimensions**, reinforcing the core WP6 objective of enhancing cybersecurity skills through active, intuitive, and technically accurate training experiences.

Cybergate's training modules are built on three foundations:

1. **Threat-informed mission design**, using MITRE ATT&CK, MITRE D3FEND, and the Mandiant Attack Lifecycle as reference models;
2. **Interactive gameplay mechanics**, including mini-games, decision-making exercises, and collaborative defense planning;
3. **Progressive learning architecture**, where mission complexity increases over time to guide users from basic concepts to advanced defense scenarios.

This chapter presents the methodology, structure, and implementation of these modules.

3.1 Methodology for Mission and Module Design

The methodology used to develop the gamified training modules blends cyber threat intelligence, educational design, and game mechanics to create realistic and engaging learning experiences [1].

Threat-Informed Model

Cybergate integrates key cybersecurity frameworks to ensure technical accuracy and real-world relevance [2]:

- **MITRE ATT&CK** provides the offensive techniques simulated during the Attack Phase (e.g., brute force T1110, credential dumping T1003, spearphishing T1566).
- **MITRE D3FEND** informs the available defensive actions (e.g., MFA, segmentation, process isolation).
- **Mandiant Attack Lifecycle** provides the overarching structural progression of missions, from reconnaissance to impact.

This alignment guarantees that each mission is mapped to authentic adversarial behavior and defensive best practices [3].

© CYberSynchorny, 2024

Figure 2 Attack succeeded

Dual-Phase Learning (Offense → Defense)

Each mission requires the learner to experience both:

1. **Attacker Perspective** – unlocking and executing simulated adversarial techniques via interactive mini-games.
2. **Defender Perspective** – assessing the resulting threat chain and deploying strategic defenses under time and resource constraints.

This intentional pairing reinforces the pedagogical concept that understanding offensive behavior enhances defensive capability.

Figure 3 Attack no result

Resource-Limited Decision Making

Defenders are given a **limited defensive budget** and must prioritize controls. This mirrors real-world SOC scenarios where time, personnel, and tools are finite. It also teaches strategic prioritization such as:

- selecting MFA over less effective mitigations
- deploying segmentation to restrict lateral movement
- isolating critical assets before secondary ones

Reflection Through Outcome Replay

© CYberSynchorny, 2024

The Outcome Phase visually replays the entire adversarial chain alongside the defenses deployed. It highlights:

- which attack steps succeeded or failed
- which defenses were effective
- what could have been done differently

This reflective loop strengthens long-term retention and supports evidence-based learning.

3.2 Playbook-Inspired Module Execution Flow

Although D6.2 focuses on training rather than automated SOAR workflows, the modules intentionally mirror the logic of incident response playbooks. This ensures consistency across WP4 and WP6 and prepares learners for operational environments [3].

The modules follow a deterministic flow that corresponds to the four-phase Cybergate gameplay cycle:

1. Attack Phase – Simulated Adversary Execution

Players activate ATT&CK techniques through mini-games representing:

- password cracking
- spearphishing
- lateral movement
- privilege escalation
- reconnaissance
- endpoint compromise

These actions form the “attack chain” that defenders must later mitigate.

2. Defense Phase – Collaborative Mitigation Planning

Based on the attack chain:

- Teams select D3FEND-mapped defenses
- Each defense mitigates one or more ATT&CK techniques
- Resource constraints enforce strategic thinking

This structure resembles a human-in-the-loop incident response playbook.

3. Dome Phase – Keystone Strategic Defense

Teams select a single high-impact defensive action with sector-wide or systemic implications. Examples include:

- shutting down a vulnerable service across all hosts
- issuing cross-organization threat intelligence reports
- activating a network-wide containment policy

© CYberSynchorny, 2024

4. Outcome Phase – Automated Replay and Scoring

The module engine:

- replays the attack sequence
- evaluates mitigation success
- provides realistic scoring
- benchmarks performance against the maximum achievable defense

This acts as the functional equivalent of a post-incident review process.

Figure 4 Game graphics

3.3 Case Studies – Mission Structure and Examples

The Cybergate training modules include **seven missions** organized into **two chapters**, each representing a full attack lifecycle. Every mission introduces new ATT&CK techniques and corresponding defensive options [10].

© CYberSynchorny, 2024

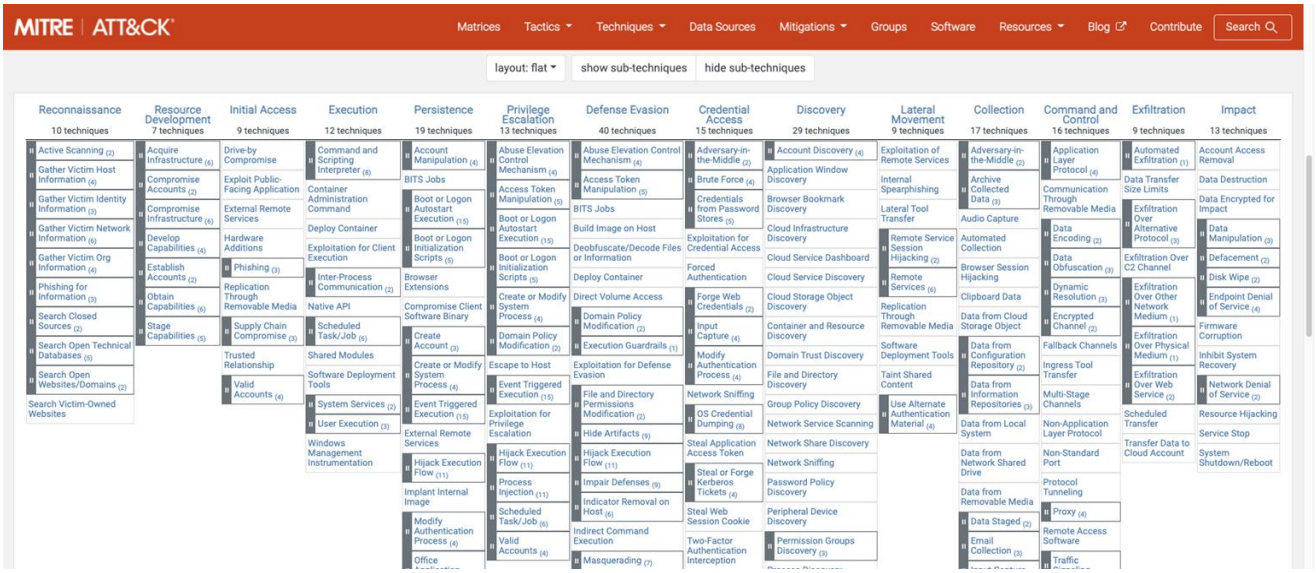

Figure 5 Mitre

3.3.1 Chapter 1: Corporate Breach (Missions 1–4)

This chapter focuses on enterprise IT environments, beginning with reconnaissance and escalating toward ransomware deployment [4][7].

Mission 1 – Reconnaissance & Initial Access
Simulated techniques include wordlist scanning (T1595.003) and network share enumeration (T1135).
Players learn foundational concepts such as exposure, weak endpoints, and perimeter scanning.

Mission 2 – Credential Theft & Internal Reconnaissance
Techniques: LSASS memory dumping (T1003.001), RDP hijacking (T1563.002).
Learners experience the danger of stolen credentials and uncontrolled privilege escalation.

Mission 3 – Lateral Movement & Discovery
Techniques: Kerberoasting (T1558.003), domain account discovery (T1087.002).
This emphasizes the need for segmentation, account hygiene, and identity protection.

Mission 4 – Ransomware Impact
Simulated impact: coordinated ransomware deployment and C2 infrastructure setup.
Defenses focus on backups, endpoint hardening, and kill-chain disruption.

© CYberSynchorny, 2024

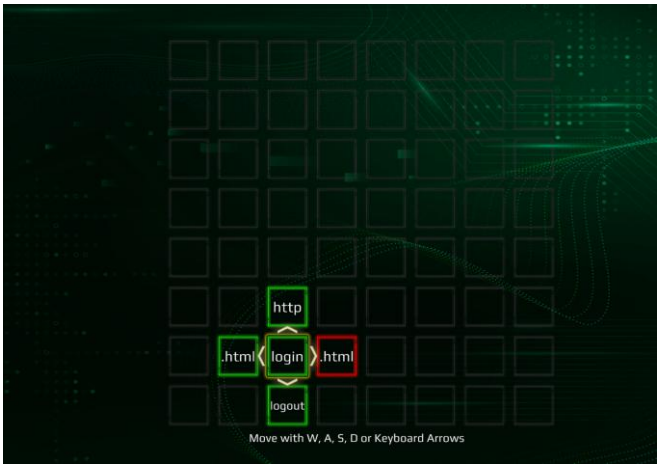

Figure 6 Game example

3.3.2 Chapter 2: Industrial Intrusion (Missions 5–7)

This chapter expands the training to an industrial ecosystem with IoT, ICS, and operational technology components [8][12].

Mission 5 – Perimeter Breach at IT/OT Boundary
Techniques: user execution (T1204), initial foothold in DMZ assets.
Learners explore weaknesses in hybrid IT/OT environments.

Mission 6 – Compromise of ICS Infrastructure
Techniques: SMB-based device access (T1021.002), manipulation of I/O modules (T0847).
Highlights include device isolation and OT segmentation.

Mission 7 – Impact & Recovery Inhibition
Techniques: data encryption for impact (T1486), recovery inhibition (T1490).
Critical lesson: operational continuity and disaster readiness.

3.4 Mechanics of Learning Through Progression

The modules use a strategic progression model to ensure increasing difficulty and deeper learning [11]:

Progressive Technical Complexity

- Mission 1 introduces isolated attacker techniques
- Missions 3–4 require handling multi-vector threats
- Mission 7 simulates worst-case ICS compromise scenarios

Cumulative Knowledge Reuse

Techniques and defenses reappear in later missions in new contexts, reinforcing recognition and transfer of learning.

© CYberSynchorny, 2024

Team Coordination and Role Specialization

As difficulty increases, teams organically develop roles such as:

- analyst
- strategist
- threat mapper
- defense coordinator

This mirrors real SOC collaboration.

Feedback-Driven Improvement

The interplay between replay analytics and team reflection drives measurable skill gains.

© CYberSynchorny, 2024

4 Deployment Strategy and Validation

The deployment of the gamified training modules developed in D6.2 focuses on ensuring that the Cybergate platform can operate reliably across multiple environments, support scalable training scenarios, and deliver consistent learning outcomes. The deployment strategy emphasizes modularity, interoperability, and alignment with the broader CYberSynchrony architecture, while the validation process ensures that each mission meets technical, educational, and experiential quality criteria.

The Cybergate platform is designed to function both as an operational training tool for organizations and as an educational environment for structured cybersecurity curricula. Therefore, deployment must accommodate diverse operational needs, ranging from single-team training exercises to multi-organization simulations and cross-sector cybersecurity awareness events.

Figure 7 Game example

4.1 Deployment Environment

The deployment of Cybergate consists of two complementary environments [9]:

1. **Operational Training Environment**
2. **Simulation & Development Environment**

Together, these enable seamless integration of training modules into different settings while ensuring continuous improvement through iterative testing.

Operational Training Environment

This environment is designed for actual training sessions delivered to end-users, including cybersecurity professionals, students, and organizational personnel.

Key characteristics include:

- **Browser-based or client-based access**, ensuring minimal setup requirements for trainees.
- **Backend infrastructure hosted in a secure cloud environment**, enabling high availability and low-latency multiplayer interactions.
- **Role-based user authentication**, ensuring that only authorized trainees and trainers access the system.
- **Dynamic content loading**, allowing new missions, techniques, or narrative elements to be introduced without system downtime.

© CYberSynchorny, 2024

- **Telemetry collection**, capturing all user decisions, attack sequences, and defense selections for later analysis.

This environment allows organizations to deploy Cybergate for internal exercises, red-team simulations, upskilling programs, or periodic awareness training.

Simulation & Development Environment

This environment is used by trainers, mission designers, and developers to test new missions and refine existing ones before rolling them into the operational environment. It supports:

- **Sandboxed execution**, ensuring that experimentation never impacts production training.
- **Hot-swappable mission content**, including ATT&CK techniques, D3FEND mappings, and dome actions.
- **Automated scenario testing**, verifying that missions load and execute correctly.
- **Instructor tools** for scenario walkthroughs and difficulty calibration.

The dual environment structure ensures that Cybergate remains stable for end-users while maintaining flexibility for rapid content updates and mission innovation.

4.2 Testing & Validation of Gamified Modules

Validation of the Cybergate modules follows a rigorous multi-stage process that ensures accuracy, learning effectiveness, and technical robustness. The validation approach combines functional testing, performance assessment, gameplay evaluation, and learning outcome analysis.

a. Functional Accuracy

Each mission undergoes step-by-step functional validation to ensure that:

- Attack mini-games correctly map to MITRE ATT&CK techniques.
- Defense selections correctly mitigate the associated ATT&CK steps using D3FEND principles.
- Dome actions apply the intended strategic effects on mission outcomes.
- Attack chains are generated dynamically and replay accurately.
- Scoring logic reflects realistic defense potential.

This ensures that the learning mechanics remain consistent with the underlying threat-intelligence foundations.

b. Performance Metrics

The system is evaluated using quantifiable performance indicators, including:

- **Response latency** between player actions and UI state changes.
- **Mini-game execution speed** and responsiveness under load.
- **Multiplayer synchronization accuracy**, ensuring real-time collaboration.
- **Mission load times** from content repository to active gameplay.
- **Scoring engine performance**, validating that outcome computation scales to simultaneous sessions.

© CYberSynchorny, 2024

These metrics help guarantee smooth and reliable gameplay even in large training deployments.

c. Scenario-Based Validation

Scenario-based validation tests the fidelity of each mission against expected threat progression patterns. For each mission:

- The attack chain is checked against MITRE ATT&CK mappings.
- Defensive decisions are compared to real-world best practices.
- The mission's narrative progression is validated against the Mandiant attack lifecycle stages
- Outcome replay is inspected to ensure accurate representation of attack-defense interactions.

This process verifies that missions accurately model realistic cyber incidents rather than isolated or arbitrary challenges.

Figure 8 Game example

d. Gameplay Usability and Engagement

Testing includes human-centered evaluations focusing on:

- player comprehension of mission objectives
- effectiveness of visual cues and interface layout
- clarity of defense selection menus
- pacing of missions and cognitive load
- collaborative communication flow among team members

© CYberSynchorny, 2024

This ensures that the training environment is intuitive, engaging, and accessible to both technical and non-technical participants.

e. Learning Impact Assessment

To validate the educational value of Cybergate missions, instructors assess:

- whether players show improved recognition of ATT&CK techniques
- whether defensive choices become more strategic over time
- team coordination patterns
- the degree to which players understand threat progression
- retention of knowledge across multiple missions

Outcome Phase analytics are especially important — they show which defenses consistently succeed or fail, highlighting areas where participants may require additional training.

f. Security and Access Control Validation

Since Cybergate operates in environments where cybersecurity is paramount, the platform undergoes checks for:

- secure authentication
- encrypted data handling
- sandbox integrity
- role-based access for mission deployment and content editing
- absence of real malicious code execution

These safeguards ensure that training never risks the security of organizational infrastructure.

4.3 Summary of Deployment and Validation Approach

The deployment and validation framework in D6.2 ensures that Cybergate delivers [5][6]:

- **Operational reliability** in real-world training environments
- **Pedagogical soundness** through mission-by-mission learning validation
- **Threat intelligence accuracy** via ATT&CK, D3FEND, and Mandiant lifecycle alignment
- **Scalability** through modular mission design and cloud-ready infrastructure
- **Consistent user experience** through performance benchmarking
- **Actionable training analytics** to guide learner progression.

This structured approach guarantees that the gamified modules are stable, engaging, technically precise, and ready for large-scale adoption within WP6 and beyond.

© CYberSynchorny, 2024

5 Conclusions

This deliverable represents a major milestone in the advancement of CYberSynchrony's mission to strengthen cybersecurity awareness, readiness, and capability across society. Through the design and implementation of the Cybergate platform, this deliverable provides a technically accurate, threat-informed, and pedagogically robust training system that addresses the evolving challenges posed by modern cyber threats. The integration of MITRE ATT&CK, MITRE D3FEND, and the Mandiant Attack Lifecycle ensures that the training content not only reflects real adversary behaviour but also reinforces defensive best practices across the entire attack continuum.

The gamified modules introduce an innovative combination of offensive simulation and defensive strategy, enabling learners to experience the attacker's perspective and then immediately practice countermeasures in realistic, time-pressured environments. This dual perspective significantly enhances situational awareness, threat anticipation, and critical decision-making — skills that are essential for cybersecurity professionals and broader user groups alike. The structured four-phase mission flow (Attack, Defense, Dome, Outcome) provides a cohesive and repeatable framework that builds technical knowledge while strengthening collaborative abilities and strategic thinking.

The technical architecture of Cybergate — including its modular mission engine, secure sandboxed execution environment, real-time multiplayer synchronization, and extensive analytics — ensures that the platform is scalable, extensible, and suitable for both organizational and educational contexts. The modularity allows rapid adaptation to new threat vectors, emerging techniques, and sector-specific scenarios, ensuring the platform remains relevant as the threat landscape evolves. The inclusion of analytics and performance tracking further supports trainers and organizations in identifying skill gaps, evaluating progress, and tailoring future training.

Validation activities conducted as part of this deliverable demonstrate the reliability, educational value, and operational readiness of the Cybergate modules. Functional testing, scenario-based assessment, gameplay evaluation, and learning impact studies confirm that the modules deliver consistent results, realistic outcomes, and measurable improvements in learner competency. The replay and scoring system reinforce reflective learning and provides actionable insights that support iterative skill development.

This first version of the gamified training modules forms the foundation for the continued evolution of the Cybergate platform within WP6. Future iterations will build on the work presented here by expanding mission libraries, enhancing adaptive learning features, incorporating additional sectors such as cloud and mobile security, and integrating lessons learned from ongoing training deployments. These developments will further reinforce CYberSynchrony's objective of creating dynamic, engaging, and effective cybersecurity training environments that build long-term resilience across Europe.

In conclusion, D6.2 delivers a robust, validated, and scalable gamified training system that contributes directly to strengthening cyber awareness, skills, and preparedness. It provides a strong basis for future enhancements and plays a central role in achieving CYberSynchrony's overarching goal of empowering society through innovative cybersecurity education.

© CYberSynchorny, 2024

6 References

[1] What Are MITRE ATT&CK and MITRE D3FEND? | D3 Security
https://d3security.com/blog/mitre-attack-defend-explained/

[2] Targeted attack life cycle | Google Cloud
https://cloud.google.com/security/resources/insights/targeted-attack-lifecycle

[3] Cyber Kill Chain, MITRE ATT&CK, and Purple Team | SANS Institute
https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team

[4] Brute Force - T1110 - Offensive Technique Details | MITRE D3FEND™
https://d3fend.mitre.org/offensive-technique/attack/T1110/

[5] Jin, G., Tu, M., Kim, T. H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. Journal of Education and Learning (EduLearn), 12(1), 150-158.

[6] Khan, M. A., Merabet, A., Alkaabi, S., & Sayed, H. E. (2022). Game-based learning platform to enhance cybersecurity education. *Education and Information Technologies*, *27*(4), 5153-5177.

[7] ATT&CK Technique T1566 - Mappings Explorer - GitHub Pages
https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-9.0/domain-enterprise/techniques/T1566/

[8] Valid Accounts - T1078 - MITRE D3FEND
https://d3fend.mitre.org/offensive-technique/attack/T1078/

[9] Donekal Chandrashekar, N., Lee, A., Azab, M., & Gracanin, D. (2024). Understanding user behavior for enhancing cybersecurity training with immersive gamified platforms. *Information*, *15*(12), 814.

[10] Khan, M. A., Merabet, A., Alkaabi, S., & Sayed, H. E. (2022). Game-based learning platform to enhance cybersecurity education. *Education and Information Technologies*, *27*(4), 5153-5177.

[11] ATT&CK Technique T1592 - Mappings Explorer
https://center-for-threat-informed-defense.github.io/mappings-explorer/attack/attack-9.0/domain-enterprise/techniques/T1592/

[12] User Execution, Technique T1204 - Enterprise - MITRE ATT&CK®
https://attack.mitre.org/techniques/T1204/

© CYberSynchorny, 2024