

DIGITAL-ECCC-2022-CYBER-B-03-
CYBER-RESILIENCE



This project has received funding from the European Union's DIGITAL-ECCC-2022-CYBER-B-03-CYBER-RESILIENCE programme under grant agreement No 101145872.

Connected 5G-IoT Cyber Range for Training and Secure Operations



WP4– Scoring System and Gamification

Deliverable D4.1 “NITRO scoring and gamification system - first version”

Editor(s):	IURC
Author(s):	Angeliki Panou (UPRC), Christos Xenakis (UPRC), Aikaterini Poupouza (UPRC), Nikitas Sgouros (UPRC), Anna Politi (UPRC), Georgios Eftymoglou (UPRC), Christoforos Ntantogian (IURC), Emmanouil Magkos (IURC), Aggeliki Tsohou (IURC), Andreas Athanasoulas (UNIGR), Styliani Tsitsoula (HCSI), Anastasis Tzoumpas (UBI), Stavros Ketseas (UBI), Anna Naouni (UBI), Malekas Pantelis (UBI).
Dissemination Level:	P
Type:	R
Version:	1.4

Project Profile

Contract Number	101145872
Acronym	NITRO
Title	Connected 5G-IoT Cyber Range for Training and Secure Operations
Start Date	Jan 1 st , 2024
Duration	36 Months

Partners



University of Piraeus Research Center

Greece



UNISYSTEMS LUXEMBOURG SARL

Luxembourg



ONIAN UNIVERSITY

Cyprus



HELLENIC CYBERSECURITY INSTITUTE

Greece



UBITECH LIMITED

Greece

Document History

VERSIONS

Table 1 Document history

Version	Date	Author	Remarks
0.2	28.02.2025	IURC/UPRC	Table of Contents
0.4	05.03.2025	IURC/UBI/UNIGR	Initial version
0.6	19.03.2025	UBI/HCSI/UNILU	Inputs
0.8	13.05.2025	IURC	Revision
1	14.05.2025	UPRC/UBI/HCSI	Inputs and Revision
1.2	19.05.2025	UPRC/UNIGR	Revision
1.4	30.06.2025	IURC	Final Version

Executive Summary

Deliverable D4.1 is dedicated to the documentation of the work in Task 4.1 and Task 4.2 presenting the scoring methodology and the gamification solution that will be used in NITRO. Particularly, T4.1 "Scoring and feedback mechanism" includes the design and development of a novel scoring system for trainees that will provide feedback regarding the technical skills and capabilities of the trainees to defend successfully the system under attack. Scoring systems for defenders are not popular and one of the NITRO's key objectives is to provide an intuitive scoring system so that trainees not only participate in exercises but also comprehend and identify their knowledge gaps, inefficiencies with the goal to self-improve and enhance their skills. To this end, visual elements, layout, and overall structure of the scoring and feedback mechanism will be created. This includes designing intuitive navigation menus, interactive components, and visually appealing data visualizations to provide a comprehensive view of the participants activities and progress cyber range activities. On the other hand, T4.2 involves activities for the application of game design principles, mechanics, and elements to enhance the learning and engagement experience within the cyber range environment. In particular, this task includes designing and developing game-like features such as challenges, levels, achievements, leaderboards, and rewards systems that align with the training objectives of the NITRO 5G-IoT Cyber Range. Moreover, collaboration and teamwork mechanisms will be developed to allow participants to develop cooperative strategies to overcome cybersecurity threats.

Table of Contents

Executive Summary	4
Table of Figures	6
Table of Tables	7
1 Introduction	8
1.1 Scope	8
1.2 Connection to other deliverables	8
1.3 Document structure	8
2. Gamification Design of the Exercises.....	8
2.1 High-Level Design of the Scoring and Gamification System.....	9
2.2 Learning Curve.....	11
2.3 Storytelling.....	12
2.4 Supportive Educational Material.....	14
3. Scoring System Design	14
3.1 Flags	14
3.2 Leaderboards	15
3.3 Badges/Certification.....	15
3.6 Visual Elements and Data Visualization	17
4. Intelligent Scoring.....	19
4.1 Integration with Threat Intelligence and SIEM Logs	19
4.2 Incorporating Indicators of Compromise (IOC) and Attack Actors.....	22
4.3 Metrics for Blue Teaming	22
4.4 Dynamics (Automated Scripts / CRON jobs - check load file)	24
5. Conclusion	25
References	25

Table of Figures

Figure 1. Adaptive Difficulty and Progression.....	10
Figure 2 Adaptive Learning Path	11
Figure 3 Storytelling and Progression	13
Figure 4. Badges and Certifications.....	16
Figure 5. Visualization and User Engagement	18
Figure 6. Intelligent Scoring System.....	20
Figure 7. Continuous Monitoring and Metrics for Blue Teaming	22
Figure 8. Dynamics of Automated Scoring and Evaluation.....	24



Table of Tables

Table 1 Document history.....	3
-------------------------------	---

1 Introduction

1.1 Scope

The role of this deliverable is to present the scoring methodology and the gamification solution that will be used in NITRO. Particularly, this deliverable describes the gamification design used in the NITRO exercises together with example on how to achieve the enhanced gamified mechanics within the cyber range.

1.2 Connection to other deliverables

The corresponding deliverable D4.1 is directly related to the following technical deliverables:

- **D2.2 NITRO cyber range architecture, testing and validation plans - first version:** Gamification and scoring system of NITRO have been designed under the approach that is defined in D2.1.
- **D2.3 Technical, legal, policy requirements and use case scenarios - second version:** D2.3 will include the latest updated that will arise from the gamification features of D4.1.
- **D2.4 NITRO cyber range architecture, testing and validation plans - second version:** The final NITRO architecture will be based on the parameters and features of gamification and scoring system of the NITRO exercises mentioned in this deliverable.
- **D3.3 NITRO security training exercises design and development - second version:** D3.3 will include the implementation and a walkthrough of the exercises together with the gamification and scoring approach of the NITRO coming from this deliverable.
- **D4.2 NITRO Infrastructure Integration - first version:** First integration plan in D4.2 will be based on technical features stemming from D4.1.

1.3 Document structure

The rest of the document is organized as follows. Section 2 describes the gamification design that characterizes the NITRO exercises. Next, Section 3 depicts the scoring system while Section 4 presents the NITRO’s intelligence system. Finally, Section 5 concludes the deliverable.

2. Gamification Design of the Exercises

The gamification design of the NITRO 5G cyber range aims to create an engaging, educational, and rewarding environment for participants to develop cybersecurity skills. The scoring and gamification system is an important factor on interactive training environments, driving engagement while reinforcing learning outcomes [JAY, DAG]. For example, a point-based system tracks achievements, with participants earning points for tasks like identifying vulnerabilities or mitigating attacks [DDK]. Adaptive difficulty adjusts challenges to maintain a state of flow, ensuring participants are neither overwhelmed nor understimulated [JTM]. Various achievement milestones are introduced, such as badges for completing tasks without errors, further motivate participants [FBS], while real-time leaderboards foster competition [LOP]. The design includes the following building blocks that are considered as important factors:

1. **Scoring and Gamification System:** Participants earn points by completing tasks such as detecting and mitigating attacks. Points contribute to leveling up or unlocking more complex challenges. Achievements and badges are awarded for milestones, and a real-time leaderboard fosters competition. Time-based challenges and dynamic difficulty adjustment ensure that players are consistently challenged and rewarded for their efficiency.
2. **Learning Curve:** The exercises are designed to cater to different skill levels. Starting with basic tasks, participants progress through intermediate and advanced scenarios. The learning curve is adaptive, allowing participants to focus on weaker areas while continually building their skills. Feedback is provided throughout, ensuring participants receive guidance without feeling overwhelmed.
3. **Storytelling:** A compelling narrative immerses participants in a high-stakes cyberattack scenario. As part of a cybersecurity team defending critical 5G infrastructure, participants complete missions to thwart various types of attacks. The story evolves based on participants' actions, with NPC mentors offering guidance and feedback. The plot changes dynamically depending on the outcomes of the exercises.
4. **Supportive Educational Material:** To enhance learning, interactive tutorials, documentation, and video explanations are available to help participants understand the technical aspects of each task. A hint system provides assistance when needed, and post-exercise reports offer detailed feedback and suggestions for improvement. This ensures participants gain both practical skills and theoretical knowledge.

2.1 High-Level Design of the Scoring and Gamification System

The scoring and gamification system is at the core of any interactive training environment, driving engagement while reinforcing learning outcomes. The system is designed to effectively motivate participants by providing tangible rewards and real-time feedback, encouraging participants to keep progressing through the exercises. As participants accumulate points, they are capable to unlock new levels, representing a deeper understanding and mastery of complex concepts in cybersecurity. For example, a beginner might earn points by completing basic configurations, while an expert could earn higher points for tackling more challenging problems, such as defending against coordinated attacks.

Modern game design incorporates several key elements (Figure 1) to create engaging and dynamic player experiences. One of the most important is adaptive difficulty, which ensures the game remains challenging yet fair by automatically adjusting obstacles, enemy strength, or puzzle complexity based on the player's skill level [JTM]. This system not only keeps players in a state of "flow" but also influences unlock criteria, ensuring that new levels, abilities, or content become available only when the player is ready. Additionally, adaptive difficulty can affect ranking systems and special challenges, tailoring competitive or timed events to match individual performance, making leaderboards more meaningful and inclusive.

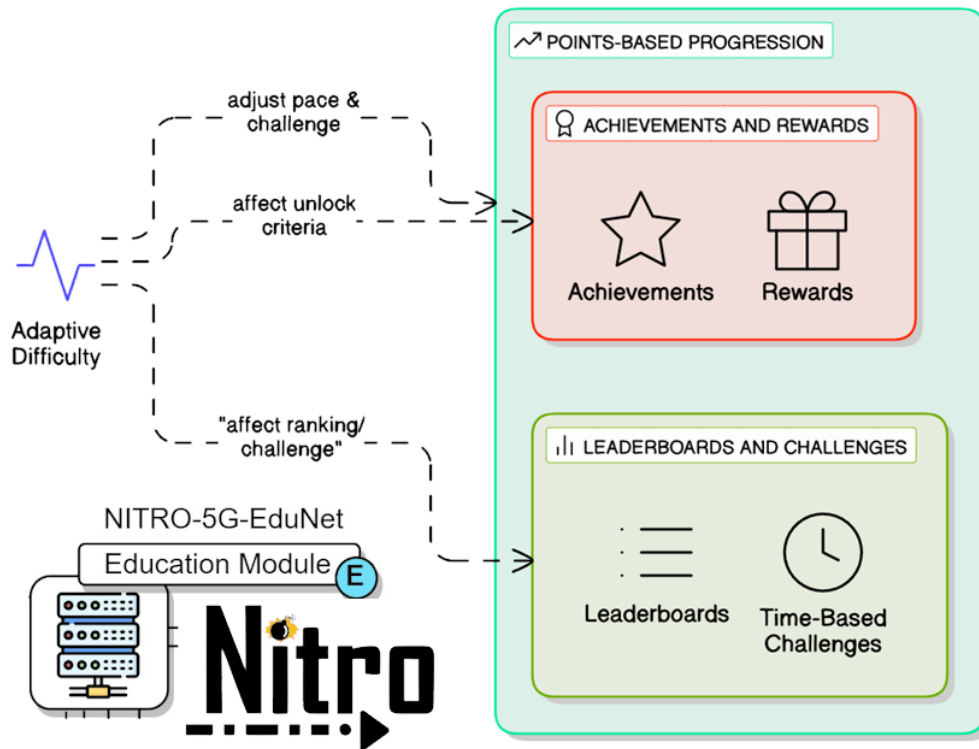


Figure 1. Adaptive Difficulty and Progression

Figure 1 illustrates the gamification system that integrates adaptive difficulty, points-based progression, achievements and rewards, and leaderboards with time-based challenges. Adaptive Difficulty influences the system in two primary ways. First, it adjusts the pace and challenge unlock criteria within the Points-Based Progression framework. This ensures that as users earn points, the difficulty and speed of unlocking new challenges are tailored to their skill level and progress, promoting a personalized learning or gaming experience. Achievements are earned based on meeting specific milestones or completing tasks, while rewards are incentives provided to motivate continued engagement.

Another core concept is point-based progression, which provides players with a clear sense of growth and accomplishment. By earning experience points, in-game currency, or other measurable rewards, players can track their advancement and work toward specific goals [JAY]. This system often ties into achievements and rewards, where completing predefined challenges, such as defeating a boss under certain conditions or exploring hidden areas, grants badges, trophies, or exclusive items. These incentives not only validate player effort but also encourage experimentation and replayability. To foster competition and community engagement, many games implement leaderboards and challenges. Leaderboards rank players based on high scores, speedrun times, or other metrics, creating a sense of rivalry and motivation to improve [ZAF]. Meanwhile, time-based challenges, such as limited-time events or daily missions, add urgency and variety, ensuring players return regularly. Together, these mechanics create a balanced ecosystem where personal progression, skill adaptation, and social competition keep the experience fresh and rewarding for all types of players.

The inclusion of achievements such as badges or titles will further motivate participants. These achievements could be awarded for specific milestones, such as completing a task without errors,

solving a complex attack, or achieving a certain number of points within a session. To maintain engagement and foster competition, a leaderboard can display real-time rankings based on points, showcasing top performers. This introduces an element of friendly rivalry, encouraging participants to strive for higher rankings. Furthermore, the time-based challenges could be incorporated into the scoring system, where participants earn bonus points for completing tasks within a specified time frame, promoting efficiency and the ability to perform under pressure. Dynamic difficulty adjustment is also crucial; as participants advance through the exercises, the difficulty should scale accordingly, ensuring that they are consistently challenged without feeling overwhelmed.

2.2 Learning Curve

The learning curve within the gamified system (**Error! Reference source not found.**) needs to be carefully designed to accommodate a wide range of participants, from beginners to advanced users. The system should start with beginner-level exercises that introduce participants to the fundamental concepts of cybersecurity in a 5G network. These could include tasks like basic network configurations, understanding simple attack vectors, and recognizing security weaknesses. As participants demonstrate competence, they progress to intermediate-level challenges that require a deeper understanding of network security principles, such as defending against Distributed Denial-of-Service (DDoS) attacks or implementing encryption protocols. The ultimate goal is to engage participants in advanced-level exercises where they tackle sophisticated scenarios, such as defending an entire 5G infrastructure from coordinated, multi-vector attacks or performing real-time threat analysis during a high-stakes breach.

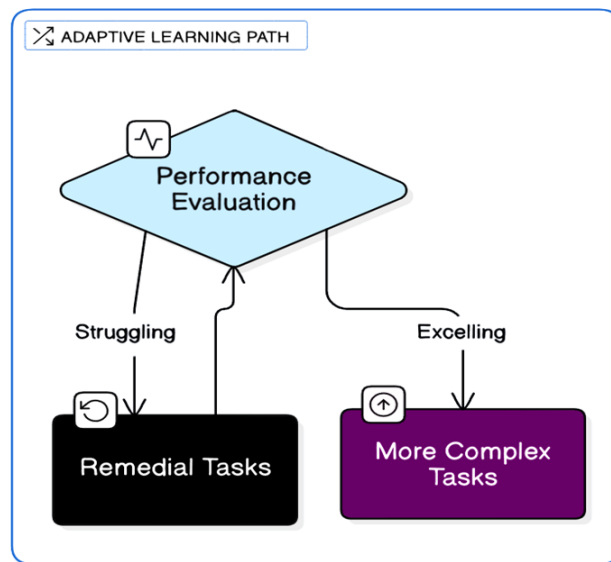


Figure 2 Adaptive Learning Path

A well-designed adaptive learning path dynamically adjusts to a learner’s performance, ensuring that the educational experience remains engaging, efficient, and appropriately challenging [SED]. At its core, this system relies on continuous performance evaluation, where the learner’s interactions, response accuracy, and problem-solving speed are analyzed in real time. Based on this assessment, the system identifies whether the learner is struggling with the material or excelling beyond

expectations.

For learners who are struggling, the system provides remedial tasks, targeted exercises that reinforce foundational concepts through repetition, simplified explanations, or alternative teaching methods. This scaffolding prevents frustration and helps bridge knowledge gaps before progressing further. Conversely, learners who demonstrate mastery are presented with more complex challenges to prevent boredom and stimulate deeper cognitive engagement. These advanced tasks may include higher-level applications, critical-thinking problems, or exploratory activities that extend beyond the standard curriculum.

The advantage of an adaptive learning path lies in its ability to personalize the learning curve for each individual. That is, the system adapts the difficulty and pacing to match the skill level of learners, instead of forcing them to progress in a rigid manner by following the same learning path. This approach gives better retention of knowledge and promotes motivation because it ensures that learners are neither overwhelmed nor underwhelmed. The adjustment of content using real-time feedback in adaptive learning, creates the appropriate educational path that increases both efficiency and long-term understanding.

The progression from simple to complex scenarios (Figure 2) allows for a progressive learning path, where participants build confidence as they successfully complete tasks [JTM]. To support this, the system can include adaptive learning paths, where the challenges adjust based on performance. If a participant excels in one area, the system might present more complex challenges, while if a participant struggles, the system can suggest more basic tasks to help reinforce concepts. Feedback should be a vital part of the system, with real-time guidance offered when a participant encounters difficulties. This keeps learners engaged and ensures they are not stuck in one area for too long. Each completed task should unlock additional content and progressively harder challenges, providing a sense of accomplishment while avoiding frustration or disengagement.

2.3 Storytelling

Integrating storytelling into the gamification system is a powerful way to enhance the immersive experience for participants. A well-crafted narrative can make the training feel like a dynamic and high-stakes mission rather than a series of isolated exercises [TOC]. The scenario begins with alerts signaling an ongoing attack on a 5G network, which serves as the backbone for IoT devices, smart cities, and emergency communications. As participants work through lab exercises, their actions determine whether the network is defended or suffers a data breach as follows:

- Successfully mitigating a DDoS attack could reinforce network resilience, leading to a partial compromise where some systems remain functional.
- Failing to detect a malware infiltration might trigger a network failure, escalating the crisis and requiring emergency recovery protocols.

Each mission within the narrative aligns with real-world cyber threats, such as:

- Securing 5G core networks against man-in-the-middle attacks.
- Preventing IoT device hijacking to stop adversaries from intercepting sensitive data.
- Identifying and neutralizing APTs (Advanced Persistent Threats) before they exfiltrate critical

intelligence.

Incorporating story progression into cybersecurity training (**Error! Reference source not found.**) transforms technical exercises into an immersive, high-stakes experience. By framing hands-on labs within a compelling narrative, such as defending critical 5G infrastructure against a sophisticated cyberattack, participants become more engaged, emotionally invested, and motivated to apply their skills effectively. The story could follow an elite cybersecurity team responding to escalating threats, where each decision directly impacts the plot's outcome, leading to either a positive story path (successful defense) or a negative story path (catastrophic failure).

By embedding training within a story, learners experience cause-and-effect consequences, reinforcing the real-world impact of cybersecurity failures [COE]. A positive resolution (network defended) rewards participants with a sense of accomplishment, while a negative outcome (network collapses) underscores the urgency of proper defense strategies. This method not only enhances technical retention but also sharpens decision-making under pressure, an essential skill for cybersecurity professionals.

The storytelling elements involve information around a cyberattack scenario where participants are part of an elite team of cybersecurity experts tasked with defending critical 5G infrastructure against sophisticated adversaries. The overarching plot could involve various cyberattacks attempting to destabilize the 5G network, such as malware infiltrations, DDoS attacks, and attempts at intercepting IoT communications. As participants progress through the challenges, the story unfolds, and their actions could directly influence the plot's direction.

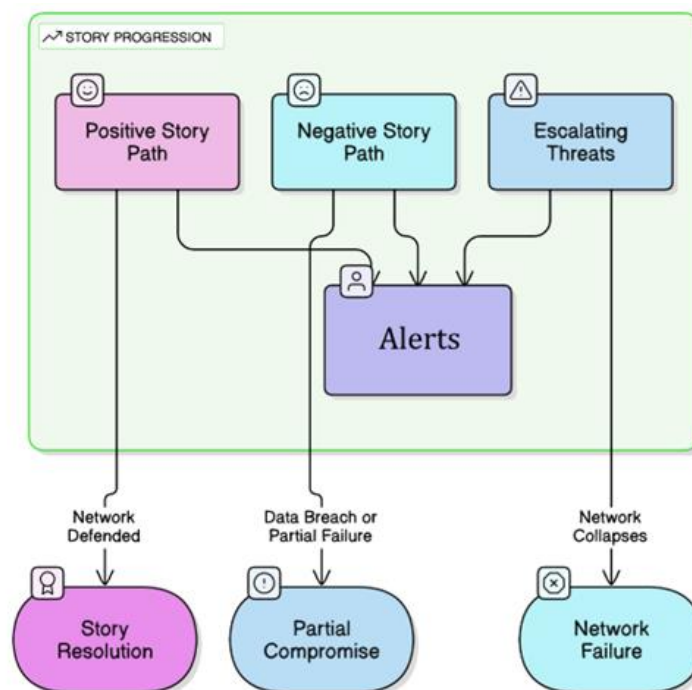


Figure 3 Storytelling and Progression

Each exercise could be framed as a specific mission within the larger narrative, with participants working to prevent or mitigate certain types of attacks. For example, one mission could focus on

protecting a 5G network's backbone infrastructure from a DDoS attack, while another might require participants to secure communication between connected IoT devices. The storyline should evolve based on participants' decisions and actions, with multiple possible outcomes depending on how well they complete their tasks. If a participant fails a mission or makes a poor decision, the story could take a darker turn, showing the consequences of those actions, such as the breach of sensitive data or the collapse of part of the network. Non-player characters (NPCs) could also be integrated into the story, acting as virtual mentors or team members who provide guidance, offer feedback, and react to the participant's progress.

2.4 Supportive Educational Material

To ensure that the gamification system of NITRO is not only engaging but also educational, it's crucial to provide comprehensive, supportive educational material. This material will help participants understand the technical aspects of the tasks they are undertaking and reinforce the learning objectives. Educational resources can come in many forms, such as interactive tutorials that introduce new concepts before each mission [KKM]. For example, before a task on securing 5G communication, a short tutorial might explain the basics of 5G architecture, its security requirements, and common vulnerabilities. This helps set the context for the task at hand and ensures participants are adequately prepared.

Additionally, documentation on various cybersecurity topics, such as cryptography, network protocols, and attack detection techniques, should be readily available within the platform. These documents would provide deeper insights into the concepts being applied in the NITRO platform exercises, allowing participants to consult them when they need a refresher or are uncertain about specific aspects of the challenge. The system could also include a hint system, which provides contextual suggestions when participants are struggling with a particular task [MAR]. This can be integrated into the narrative, where an NPC mentor provides helpful hints, ensuring that participants are not left feeling lost but are still encouraged to find their own solutions.

3. Scoring System Design

The Scoring System Design for the NITRO 5G Cyber Range is central to motivating participants and ensuring that the exercises are both engaging and educational. The system is structured to track progress, reward achievement, and encourage continuous improvement.

3.1 Flags

Flags are integral to the scoring system, acting as milestones and rewards for completing tasks or solving challenges within the cybersecurity exercises. Each flag represents a significant accomplishment, such as detecting a specific attack vector, defending a critical system, or solving a complex security issue. Flags are captured when participants successfully identify and mitigate threats, secure vulnerabilities, or complete scenario-based tasks. Flags are categorized by the complexity and significance of the task, allowing participants to see their progress and track their expertise. Flags serve as both incentives and performance indicators, providing participants with tangible evidence of

their achievements.

3.2 Leaderboards

The Leaderboard is a core feature of the gamification design, creating a competitive environment that encourages participants to engage more deeply with the training. The leaderboard displays real-time rankings based on the total score accumulated by participants. Points are awarded for completing exercises, capturing flags, and meeting specific performance milestones (such as time-based challenges or achieving a particular level of task complexity). Key aspects of the leaderboard include:

- **Global Rankings:** The overall leaderboard displays the top performers across all participants, fostering global competition.
- **Weekly/Monthly Leaderboards:** For shorter timeframes, allowing participants to compete in periodic challenges and earn recognition for their performance over a limited duration.
- **Team Leaderboards:** Encourages collaboration by allowing participants to form teams and work together to complete challenges. This leaderboard ranks teams based on their combined performance.

Leaderboards also integrate **dynamic difficulty** adjustments. As a participant progresses, the tasks become more challenging, ensuring that the participant is always striving for improvement while staying motivated by their position on the leaderboard.

3.3 Badges/Certification

Badges and certifications are a vital part of the scoring system, providing participants with recognition for specific accomplishments. These rewards not only serve as a form of motivation but also as proof of skills acquired, which can be valuable for professional development.

Badges and certifications (Figure 4) are very powerful tools in modern learning ecosystems, offering participants tangible proof of their achievements and enhancing their motivation and engagement. These digital assets act also as a reward and can be used as micro-credentials, validating specific skills, competencies, or milestones within a structured program. Integrating the badges with scoring and rewarding system, the NITRO 5G-IoT Cyber Range can transform the hard exercise into a sense of accomplishment, encourage continuous learning, and provide participants with assets that enhance their professional credibility.

Badges - Milestones and Skills: Embedding badges and certifications into training programs, particularly in fields like cybersecurity where hands-on skills are essential, can help bridge the gap between theoretical and technical concepts in a real-world context within the NITRO 5G-IoT Cyber Range. Including badges as digital media not only acknowledges the efforts of the participants but also equips them with micro-credentials that can be used for boosting their scientific and professional profile. In addition, badges can help educators and employers to create a structured pathway for skill development and career advancement within NITRO. Furthermore, badges serve as a dynamic way to reward participants for achieving specific goals within the cyber range and training program. They act

as tangible markers of progress, motivating learners to stay engaged while highlighting their growing expertise. Examples of badges include:

- **Completion Badges:** Used as a reward of finishing a specific module or exercise, recognizing the persistence of the participants to complete the modules.
- **Skill-Based Badges:** Used for demonstrating the participants' proficiency in specific topics and scientific areas, for example "5G Vulnerability Expert" for mastering the vulnerability techniques used within the NITRO or "DDoS Defender Mastery" as an expertise in mitigating distributed denial-of-service attacks.
- **Efficiency Badges:** Those are special badges that are rewarded in a designated time frame or with exceptional accuracy, emphasizing both speed and precision in the attack or defensive action milestones.

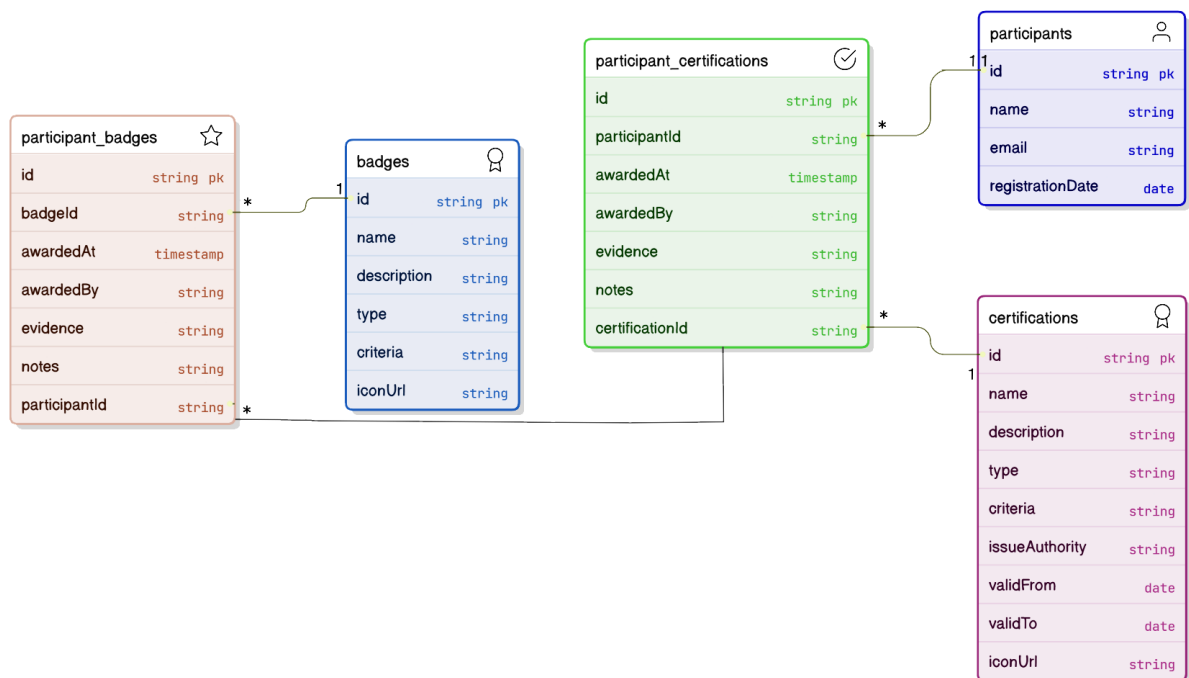


Figure 4. Badges and Certifications

The psychological impact of badges and certifications should not be underestimated. They tap into intrinsic and extrinsic motivators:

- **Progress Tracking:** Participants can visualize their growth through a collection of badges, creating a compelling narrative of their learning journey.
- **Competitive Edge:** In job applications, certifications differentiate candidates by providing third-party validation of their skills.
- **Employer Trust:** Organizations increasingly use these credentials to assess candidates' practical abilities, reducing reliance on resumes alone.

The NITRO 5G-IoT Cyber Range provides evidence for badges through detailed, verifiable records of participants' performance in simulated cybersecurity scenarios. For instance, badges like "5G Network

Defender" or "IoT Security Specialist" are earned by completing tasks such as mitigating a DDoS attack or securing IoT devices. Evidence includes logs, performance reports, and metrics like attack mitigation success, configuration changes, or vulnerability analysis, all tied to predefined criteria for transparency.

Certifications - Validating Expertise: Unlike badges, which often represent smaller milestones, certifications typically signify broader competency and are frequently tied to industry-recognized standards. These credentials often have expiration dates, requiring periodic renewal to ensure holders remain up-to-date with evolving best practices. For participants who demonstrate consistent excellence, certifications offer a higher level of validation for their cybersecurity skills. These credentials are particularly valuable for showcasing expertise to employers and industry peers. Types of certifications include:

- **Course Completion Certificate:** Awarded to participants who successfully complete an entire series of training modules or exercises, signifying comprehensive knowledge of the program's content.
- **Competency Certificates:** Granted to those who excel in advanced topics, such as intrusion detection, incident response, or vulnerability management, demonstrating specialized proficiency.

Certifications provide formal recognition of a participant's capabilities, enhancing their professional portfolio and credibility in the cybersecurity field. Key aspects include:

- **Issue Authority:** Certifications granted by reputable organizations carry significant weight in the cybersecurity field.
- **Validity Periods:** Time-bound certifications (e.g., validFrom and validTo dates) emphasize the need for ongoing education.
- **Professional Utility:** Certifications like "Certified 5G Security Analyst" can directly impact career advancement, serving as prerequisites for specialized roles.

By incorporating badges and certifications, training programs create a clear framework for recognizing both incremental progress and advanced mastery. These credentials not only celebrate personal achievements but also serve as valuable assets in the job market, signaling to employers that participants possess practical, in-demand skills. This system ultimately empowers learners to translate their training into meaningful career opportunities.

3.6 Visual Elements and Data Visualization

The visual elements and data visualizations are integrated into the NITRO scoring system to provide users with clear feedback and monitor their performance.

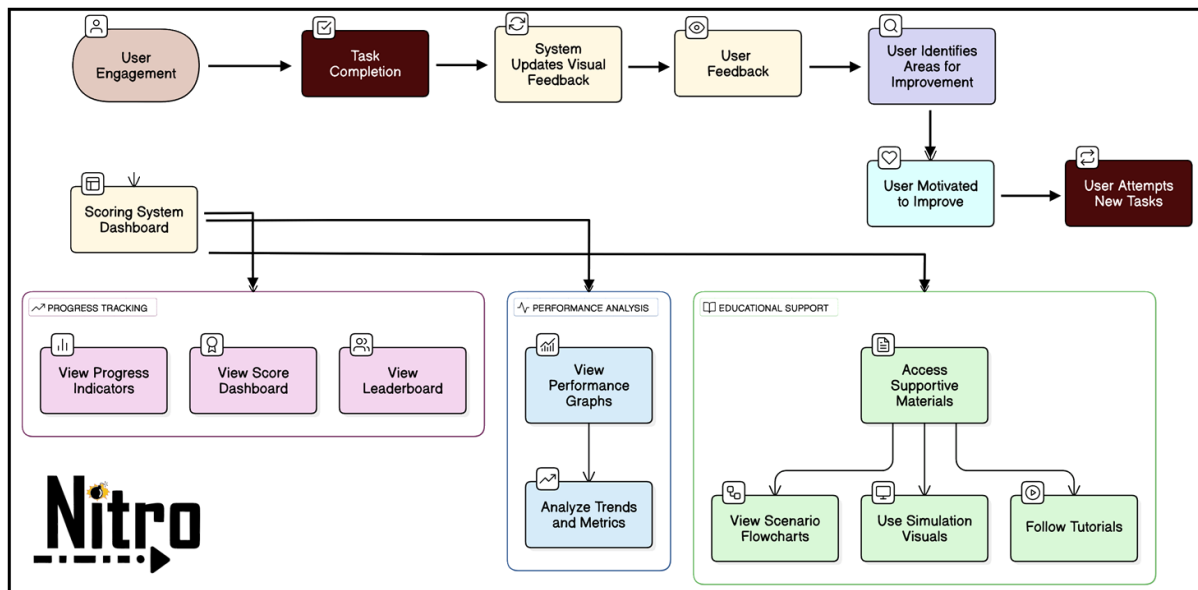


Figure 5. Visualization and User Engagement

Effective user engagement in learning and training systems is based on the strategic use of visual elements and data visualization to create an intuitive and motivating environment. The dynamic feedback mechanisms can be used as progress tracking tools, and visuals can enhance the learning experience. These systems can assist the guidance of the users through complex tasks.

Real-Time Feedback and Motivation: Visual feedback is key to keeping users engaged. Features like progress bars, achievement pop-ups, or color-coded alerts provide instant recognition of completed tasks. For example, A system dashboard will be used to show real-time metrics, highlighting the actions of the users and their progress. Performance graphs will also help users to understand their progress and highlight areas for improvement, encouraging them to try new challenges. This immediate feedback makes accomplishments feel tangible and actionable, boosting the users’ motivation. Score dashboards or leaderboards add a sense of competition or collaboration, further driving their engagement.

Progress Tracking and Performance Analysis: Progress tracking transforms abstract goals into clear, achievable milestones, making the learning journey more tangible. Visual tools such as progress bars for module completion, dashboards comparing performance over time, or flowcharts outlining the next steps of the exercise help users understand where they stand. These tools not only provide clarity but also create a sense of accomplishment, motivating users to continue their efforts.

Educational Support Through Visual Learning Aids: Complex concepts become more accessible through well-crafted visual aids, which reduce mental effort and enhance understanding. Interactive elements, such as open attack vectors in the NITRO 5G-IoT Cyber Range, tutorials with clear annotated diagrams, or flowcharts mapping decision paths in network defense scenarios, make learning more intuitive. These actions ensure users not only complete tasks but also grasp and apply key concepts, leading to deeper knowledge retention and practical skill development. As a result, the cognitive load is reduced, which helps accelerate comprehension. These tools ensure users not only complete tasks but also understand the underlying principles, leading to deeper retention and practical application.

In conclusion, the following are important to be integrated to support the data visualization.

- **Progress Indicators:** Visual elements like progress bars are used to show the completion level of tasks or missions. For instance, the scoreboard displays the percentage of challenges completed within a given exercise.
- **Supportive educational materials:** Scenario-based flowcharts, simulation visuals, and tutorials can complement the visual elements, enhancing the learning process. These materials provide clear guidance, step-by-step instructions, and context to help participants understand complex tasks and cybersecurity concepts.
- **Score Dashboards:** The participant's score and performance stats are displayed on a personalized dashboard, showing the total points earned, badges collected, flags captured, and the current leaderboard rank. This provides users with a comprehensive view of their achievements.
- **Performance:** Graphs from the scoreboard show how performance evolves over time, visualizing trends in scores, task completion rates, and other metrics such as the number of successful defenses or incidents mitigated. These insights allow participants to identify areas where they need improvement and adjust their strategies accordingly.
- **Leaderboard:** The leaderboard is designed with dynamic updates and interactive elements, where participants can view their position in real-time, track their progress against others, and see detailed statistics on their performance compared to peers.

By combining these visual elements with data-driven insights, the scoring system enhances participants' engagement, motivates them to improve, and provides them with a clear understanding of their cybersecurity training journey.

4. Intelligent Scoring

Intelligent scoring can be enhanced by integrating logs, SIEM (Security Information and Event Management) systems, and IDS (Intrusion Detection System) alerts to provide real-time, data-driven feedback. By utilizing these sources, scoring can be dynamically tied to the actions taken by participants, offering a more accurate and comprehensive reflection of their performance.

4.1 Integration with Threat Intelligence and SIEM Logs

The integration of SIEM logs and Threat Intelligence sources (e.g., MITRE TTPs) into the scoring system allows for dynamic, real-time feedback on participant actions. This can be used to track and score responses to specific tactics, techniques, and procedures (TTPs) that adversaries typically use in cyber-attacks. As participants engage in the exercise, actions such as identifying or mitigating these techniques can be automatically scored and reflected in real time.

Integrating SIEM logs and Threat Intelligence sources, including frameworks like MITRE ATT&CK TTPs (Tactics, Techniques, and Procedures), into the scoring system allows the participant's responses to be dynamically scored based on real-world adversary tactics. MITRE TTPs are well-documented

methods that adversaries use in cyber-attacks, and integrating them helps create a more realistic, contextual environment for learning. The system automatically scores actions, such as detecting or neutralizing a TTP used by attackers, based on the real-time information from SIEM and IDS logs [KAR]. The key advantages of this integration are:

- **Real-time feedback:** Participants receive immediate scoring updates based on actions they take during the exercise.
- **Relevance to real-world threats:** The scoring is tied to actual attack techniques used in cybersecurity, ensuring that training is aligned with real-world scenarios.

Scoring based on actions: Rather than solely completing predefined tasks, participants are scored based on their response to actual simulated attacks that occur during the exercise.

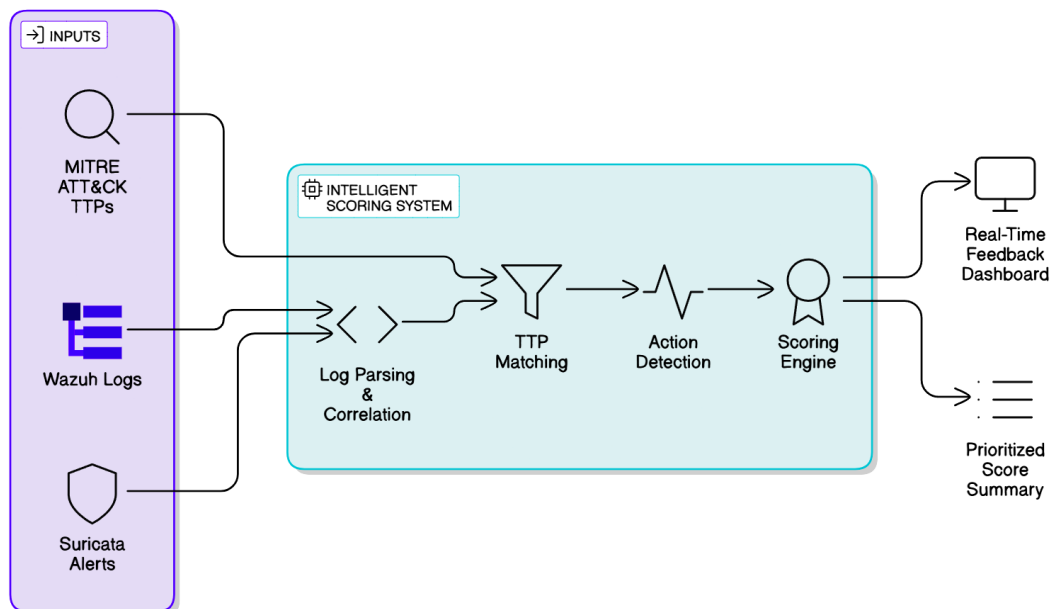


Figure 6. Intelligent Scoring System

Modern cybersecurity training platforms leverage intelligent scoring systems to evaluate participants' performance in real-world threat detection and response scenarios. By integrating MITRE ATT&CK TTPs (Tactics, Techniques, and Procedures) and SIEM (Security Information and Event Management) logs (e.g., Wazuh), these systems provide dynamic, context-aware scoring that reflects real-world security operations.

1. **Key Components of an Intelligent Scoring System**
2. **MITRE ATT&CK Framework Integration** – Maps adversary behaviors to training exercises.
3. **SIEM Log Parsing & Correlation** – Aggregates and analyzes security events for scoring.
4. **Real-Time Feedback & Prioritized Scoring** – Ensures immediate performance insights.

The **MITRE ATT&CK framework** serves as the backbone for intelligent scoring by defining adversary behaviors. In training scenarios:

- **TTP Matching:** The system checks if participants correctly identify and mitigate techniques like Lateral Movement (Tactic TA0008) or Credential Dumping (Technique T1003).

- **Weighted Scoring:** High-risk techniques (e.g., Ransomware Deployment) carry more points than low-risk ones.
- **Adaptive Difficulty:** If a participant repeatedly misses a specific TTP (e.g., Phishing Detection), the system introduces more exercises on that technique.

Intelligent Scoring Through Log Parsing and Correlation: At the core of the intelligent scoring system lies robust log parsing and correlation powered by Wazuh, which aggregates and analyzes security logs from endpoints, firewalls, and intrusion detection/prevention systems (IDS/IPS). The scoring engine meticulously processes these logs to identify key threat indicators, such as malicious command executions (e.g., reconnaissance attempts), suspicious process injections (aligned with MITRE technique T1055), and patterns of failed login attempts indicative of brute-forcing (T1110). By correlating these events with known adversary behaviors from the MITRE ATT&CK framework, the system provides a contextual scoring mechanism that reflects real-world detection and response capabilities.

MITRE Technique	Detection Accuracy	Points Awarded
Spearphishing (T1566)	Correctly blocked	+50
Privilege Escalation (T1068)	Missed	-30

Action-Based Scoring and Real-Time Feedback: The system dynamically evaluates participant actions, rewarding points for correct responses, such as isolating a compromised host, while deducting points for errors like misconfigured firewall rules. It also accounts for the precision of threat detection, penalizing both false negatives (missed threats) and excessive false positives (over-alerting). This granular scoring is complemented by a real-time feedback dashboard, which highlights critical metrics like top detected threats (e.g., "Stopped 3/5 Brute Force Attempts"), skill gaps (e.g., weaknesses in identifying persistence techniques), and competitive leaderboard rankings. This immediate feedback loop not only reinforces learning but also fosters a sense of achievement and healthy competition among participants.

Whether Suricata identifies a DoS attack or similar, the platform will generate a specific alert with details such as the source IP address, destination IP, and a brief description of the attack. Similarly, Wazuh logs might report related suspicious activities, such as a failed login attempt or system resource anomalies that could be indicative of the DoS attack's impact. These logs are then parsed, and the system assigns points for the DoS category based on the Suricata alert. In the event that Wazuh logs also show evidence of additional attacks, such as exploitation or reconnaissance, additional score points will be assigned accordingly. The total score, derived from summing the points for all unique attack categories, helps security analysts prioritize responses based on the diversity and intensity of the threats.

Post-Exercise Analysis and Continuous Improvement: After each exercise, participants receive a prioritized score summary that breaks down their performance across MITRE ATT&CK tactics, helping them identify strengths and areas needing improvement. Trend graphs visualize progress over time, enabling learners to track their development and adjust their focus accordingly. High performers may

earn credentials like "Advanced Threat Hunter" badges, while recurring skill gaps trigger personalized training recommendations. Beyond individual growth, these analytics serve organizational goals: SOC teams leverage the data for performance evaluations, and red/blue team drills use the insights to refine overall security readiness. By merging log-driven scoring with actionable feedback and certification pathways, the system bridges training and real-world cybersecurity operations, ensuring skills are both measurable and applicable.

4.2 Incorporating Indicators of Compromise (IOC) and Attack Actors

Incorporating Indicators of Compromise (IOC) and Attack Actors enhances scoring by using **IOCs** (e.g., IP addresses, file hashes, URLs) and **attack actor profiles** to track and score participant responses. Participants can be awarded points for identifying and mitigating threats based on **real-world attack patterns**. These indicators can be embedded in the challenges, and their detection and neutralization can contribute directly to scoring, ensuring a more practical, threat-driven learning experience.

4.3 Metrics for Blue Teaming

Metrics for blue teaming (Figure 7) focus on assessing the effectiveness of defensive actions. Metrics such as incident response times, the number of successful defenses, and the identification of vulnerabilities are used to evaluate how well the blue team (defenders) performs. The scoring can adapt to the complexity of tasks and how well participants protect the network, encouraging them to enhance their skills in real-world defense scenarios.

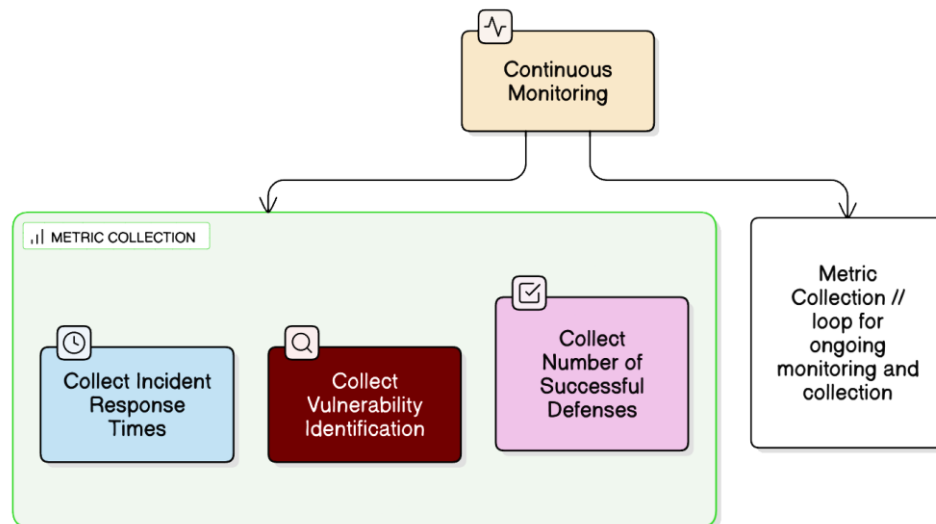


Figure 7. Continuous Monitoring and Metrics for Blue Teaming

Continuous Monitoring and Blue Teaming in 5G Networks: This exercise regards the continuous monitoring of the 5G core and the relevant subcomponents, encompassing tasks like collecting incident response times, vulnerability identification, and successful defenses, directly aligns with the role of blue teams in cybersecurity. Blue teaming involves proactive defense strategies, including real-time monitoring, threat detection, and incident response, to protect organizational assets. In the context of 5G networks, which are characterized by high data throughput, low latency, and massive

device connectivity (e.g., IoT devices), these principles become even more critical.

5G networks introduce unique security challenges due to their complexity, including increased attack surfaces from billions of connected devices and vulnerabilities in millimeter-wave communications. The metric collection tasks (Figure 7), help blue teams measure how quickly they can detect and mitigate threats in 5G environments, where rapid response is essential to prevent widespread disruption. Vulnerability assessments are important to identify any weaknesses in 5G infrastructure, such as misconfigured cloud assets or unpatched software. The effectiveness of security controls is also very important to consider that include firewall configurations or enabling and refer to intrusion detection systems to discover advanced threats like Distributed Denial of Service (DDoS) attacks, which are amplified in 5G due to its capacity.

The feedback loop in Figure 7 ensures ongoing improvement, a key aspect of blue teaming. As 5G networks evolve, blue teams must adapt to new threats, such as those exploiting high-frequency channels or cloud integration, by refining their monitoring and defense strategies. This aligns with the proactive threat hunting and continuous monitoring emphasized in blue Team operations, ensuring 5G networks remain resilient against sophisticated cyberattacks.

Blue Teaming and Education in Cybersecurity: The relationship between the diagram and education becomes evident when considering how continuous monitoring and blue teaming principles are taught and applied in cybersecurity education programs. The diagram serves as a practical model for educating students and professionals about defensive security strategies. Collect Incident Response Times introduces learners to the importance of measuring and optimizing response efficiency, a skill critical for members of the blue team. This can be taught through simulated exercises where students analyze response times to mock incidents, fostering hands-on experience.

Exercises that involve vulnerability identification and assessments educate individuals on identifying and prioritizing risks, a core competency for blue teams. In educational settings, this might involve vulnerability assessments on simulated networks, teaching students to use tools like Security Information and Event Management (SIEM) systems to detect weaknesses. Collect Number of Successful Defenses highlights the need to evaluate security controls, which can be integrated into curricula through red team-blue team exercises. These simulations allow students to defend against mock attacks, reinforcing the iterative learning process reflected in the diagram's feedback loop.

Integrating 5G, Blue Teaming, and Education: 5G's deployment has heightened the need for skilled blue team professionals, driving demand for specialized education. The diagram's focus on metric collection and feedback loops mirrors the training methodologies used to prepare individuals for 5G security roles. In practice, blue teams in 5G environments rely on educated professionals who understand both the technology and defensive strategies. The diagram's emphasis on continuous monitoring aligns with 5G security requirements, such as real-time threat detection in high-traffic networks, which require trained analysts to interpret metrics effectively. Education programs can incorporate case studies (e.g., resolving log collection issues during 5G backups) to teach problem-solving skills tailored to 5G's operational challenges.

Moreover, the feedback loop encourages lifelong learning, a necessity in the fast-evolving 5G

landscape. Educational initiatives, such as certifications or workshops, can use this model to train blue teams to adapt to emerging 5G threats, like those from increased IoT connectivity or misconfigured network elements. This integration ensures that education not only imparts current knowledge but also fosters the adaptability needed to secure 5G networks, creating a pipeline of skilled defenders to meet industry demands.

4.4 Dynamics (Automated Scripts / CRON jobs - check load file)

Dynamics (Automated Scripts / CRON Jobs) automate aspects of the scoring and evaluation process. Through scripts and CRON jobs (Figure 8), the system can process logs, generate updated attack data, and load new files automatically, ensuring real-time feedback and consistent challenge progression.

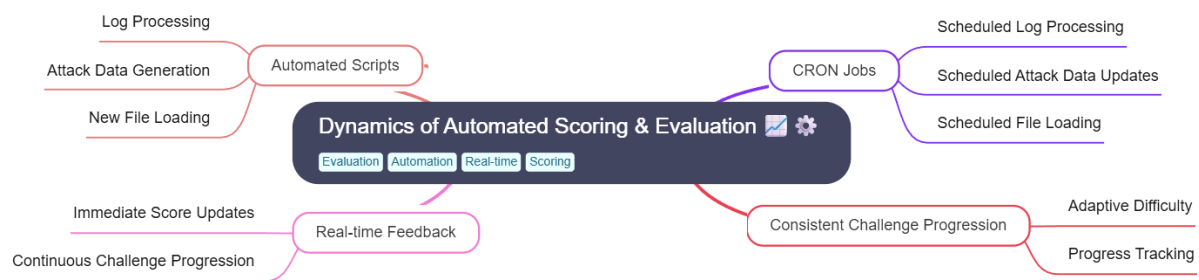


Figure 8. Dynamics of Automated Scoring and Evaluation

Figure 8 illustrates a framework centered on the Dynamics of Automated Scoring & Evaluation, a process designed to automate and enhance the assessment of cybersecurity challenges, likely in training or simulation environments. This framework integrates log processing, automated scripts, scheduled tasks (via CRON jobs), and adaptive evaluation mechanisms. Below, I’ll explain the diagram in detail and relate it to blue teaming in 5G networks and education across three conceptual pages, aligning with your request for a three-page explanation.

Figure 8 presents the details on the dynamics of the automated scoring and evaluation, an important aspect that automates the evaluation of cybersecurity scenarios through real-time scoring, evaluation, and automation. This process is supported by several components: Log Processing, Automated Scripts, and CRON Jobs, which handle scheduled tasks like Scheduled Log Processing, Scheduled Attack Data Updates, and Scheduled File Loading. These elements feed into the evaluation system, which then provides Immediate Score Updates, Real-time Feedback, Consistent Challenge Progression, Adaptive Difficulty, and Progress Tracking (in pink and red boxes).

In this educational context, CRON Jobs generating flags and points are invaluable for teaching blue teaming skills, particularly in simulated environments like Capture the Flag (CTF) exercises or red team-blue team scenarios [YOO]. The second diagram’s framework, with its focus on automated scoring, is well-suited for cybersecurity training programs. CRON Jobs can be programmed to run challenges at set intervals, evaluate student actions, and provide feedback through flags and points, fostering hands-on learning.

For example, CRON jobs can be used to automate tasks such as the scheduled deployment of challenge

files that simulate real-world scenarios, such as a 5G network vulnerability caused by a misconfigured IoT device. Students, acting as Blue Team members, must investigate the system, identify the vulnerability, and take appropriate action, such as applying a security patch. At a later scheduled time, another CRON job triggers log analysis to verify whether the student's actions align with the expected solution. If the system detects a correct response, it automatically generates a flag, awards points (e.g., 50 points), and updates the student's progress through an integrated tracking system. This approach simulates realistic incident response workflows while reinforcing learning through automation, feedback, and gamified elements.

This automated system enhances education by providing consistent, objective evaluation, as outlined in the diagram's Consistent Challenge Progression and Adaptive Difficulty. In 5G-specific training, CRON Jobs can simulate real-world scenarios like scheduled updates to attack data, teaching students to defend against 5G threats such as unauthorized access to base stations. The immediate feedback from flags and points motivates learners, while the structured progression ensures they build skills incrementally, preparing them for blue team roles in 5G security.

In the context of blue teaming, the defensive cybersecurity practice focused on monitoring, detecting, and responding to threats, this framework is highly relevant to 5G networks. 5G's high-speed, low-latency, and massive device connectivity create a complex attack surface, requiring blue teams to simulate and evaluate defenses continuously. CRON Jobs ensure scheduled updates to attack data and file loading, reflecting the need to keep 5G security simulations current with evolving threats, such as those targeting cloud-integrated 5G infrastructure.

This dynamic system allows for continuous updates to the scoring system, ensuring it reflects current network conditions and attack activities as they evolve during exercises.

5. Conclusion

The modules and exercises provide a well-rounded approach to master 5G in details and overall understand and get practice on attack and defensive mechanisms that are deployed within the NITRO 5G-IoT Cyber Range. The modules offer a balance of theoretical knowledge and practical application. Each module built progressively upon the last, ensuring that learners could develop their understanding step by step. Through carefully designed exercises, it provides an opportunity to exercise in real-world scenarios, enhancing the problem-solving abilities and understand the main software components that should be considered when securing 5G. The hands-on nature of the exercises helped reinforce key concepts, making the learning process both engaging and effective.

References

- [DDK] Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: Defining "gamification". *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, 9-15. <https://doi.org/10.1145/2181037.2181040>
- [FBS] Fleming, T. M., Bavin, L., Stasiak, K., Hermansson-Webb, E., Merry, S. N., Cheek, C., Lucassen, M., Lau, H. M., Polson, B., & Hetrick, S. (2017). Serious games and gamification for mental health:

- Current status and promising directions. *Frontiers in Psychiatry*, 7, 215. <https://doi.org/10.3389/fpsyt.2016.00215>
- [COE] Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games. *Simulation & Gaming*, 51(5), 586-611.
- [DAG] Daghestani, L. F., Ibrahim, L. F., Al-Towirgi, R. S., & Salman, H. A. (2020). Adapting gamified learning systems using educational data mining techniques. *Computer Applications in Engineering Education*, 28(3), 568-589.
- [JAY] Jayalath, J., & Esichaikul, V. (2022). Gamification to enhance motivation and engagement in blended eLearning for technical and vocational education and training. *Technology, Knowledge and Learning*, 27(1), 91-118.
- [JTM] Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Game based cybersecurity training for high school students. *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 68-73. <https://doi.org/10.1145/3159450.3159461>
- [KAR] Karagiannis, S., Ntantogian, C., Magkos, E., Ribeiro, L. L., & Campos, L. (2021). PocketCTF: a fully featured approach for hosting portable attack and defense cybersecurity exercises. *Information*, 12(8), 318.
- [KKM] Kapp, K. M. (2012). *The gamification of learning and instruction: Game-based methods and strategies for training and education*. Pfeiffer.
- [LOP] López-Pernas, S., Gordillo, A., Barra, E., & Quemada, J. (2021). Escapp: A web platform for conducting educational escape rooms. *IEEE Access*, 9, 38062-38077.
- [MAR] Martou, P., Mens, K., Duhoux, B., & Legay, A. (2022, June). Generating virtual scenarios for cyber ranges from feature-based context-oriented models: a case study. In *Proceedings of the 14th ACM International Workshop on Context-Oriented Programming and Advanced Modularity* (pp. 35-43).
- [SED] Seda, P., Vykopal, J., Švábenský, V., & Čeleda, P. (2021, October). Reinforcing cybersecurity hands-on training with adaptive learning. In *2021 IEEE Frontiers in Education Conference (FIE)* (pp. 1-9). IEEE.
- [TOC] Toccafondi, N., Bilancini, E., & Boncinelli, L. (2023, September). Learning CyberSecurity with Story-Driven CTF Challenges: CyberTrials 2023. In *International Conference on Higher Education Learning Methodologies and Technologies Online* (pp. 307-322). Cham: Springer Nature Switzerland.
- [YOO] Yoo, J. D., Park, E., Lee, G., Ahn, M. K., Kim, D., Seo, S., & Kim, H. K. (2020). Cyber attack and defense emulation agents. *Applied Sciences*, 10(6), 2140.
- [ZAF] Zafar, A., Yamin, M. M., Katt, B., & Torseth, E. (2024). All flags are not created equal: A deep look into CTF Scoring Algorithms. *Expert Systems with Applications*, 254, 124436.