T1GER: An Instructional Re-Design of a Cyber Range Exercise in a Commercial Security Operations Center

Magdalena Glas
Faculty of Informatics and Data Science
University of Regensburg
Regensburg, Germany
magdalena.glas@ur.de

Leon Kersten
Department of Mathematics and Computer Science
Eindhoven University of Technology
Eindhoven, Noord-Brabant
Netherlands
l.kersten.1@tue.nl

Tom Mulders
Department of Mathematics and Computer Science
Einhoven University of Technology
Eindhoven, Noord-Brabant
Netherlands
t.r.j.mulders@tue.nl

Günther Pernul
Faculty of Informatics and Data Science
University of Regensburg
Regensburg, Germany
guenther.pernul@ur.de

Luca Allodi
Department of Mathematics and Computer Science
Einhoven University of Technology
Eindhoven, Noord-Brabant
Netherlands
l.allodi@tue.nl

Abstract

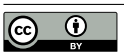
The workforce shortage in Security Operation Centers (SOCs) increases the need for effective training methods for aspiring cybersecurity analysts. Cyber ranges provide realistic environments for such training, yet many designs prioritize technical infrastructure while overlooking how trainees actually learn. Building on established instructional design principles, this study investigates how to improve learning in cyber range exercises. In collaboration with a commercial SOC, we enhanced an existing exercise for training Tier 1 analysts by integrating T1GER, a cyber range Learning Management System (LMS) that provides structured feedback, scaffolding, and competitive elements. We evaluated the approach in a randomized controlled trial with $N = 144$ participants from cybersecurity courses at two European universities, who were randomly assigned to either the original LMS (control group) or the T1GER LMS (treatment group). Results showed that using T1GER led to significantly better learning experiences and shorter training times, while maintaining equivalent knowledge outcomes.

CCS Concepts

• **Security and privacy** → **Human and societal aspects of security and privacy**; **Intrusion/anomaly detection and malware mitigation**; • **Human-centered computing** → *Empirical studies in HCI*; • **Social and professional topics** → **Computing education**.

Keywords

Cyber Range, Security Operations Center, Learning, Cybersecurity Exercise, Instructional Design



CHI '26, Barcelona, Spain

ACM ISBN 979-8-4007-2278-3/26/04
https://doi.org/10.1145/3772318.3791226

ACM Reference Format:
Magdalena Glas, Leon Kersten, Tom Mulders, Günther Pernul, and Luca Allodi. 2026. T1GER: An Instructional Re-Design of a Cyber Range Exercise in a Commercial Security Operations Center. In *Proceedings of the 2026 CHI Conference on Human Factors in Computing Systems (CHI '26), April 13–17, 2026, Barcelona, Spain.* ACM, New York, NY, USA, 22 pages. https://doi.org/10.1145/3772318.3791226

1 Introduction

Cyberattacks pose a permanent and growing threat to organizations and society. To address this challenge, organizations require capabilities to detect and mitigate cyberattacks in time. The organizational unit that is typically responsible for this task is a security operations center (SOC) monitoring digital systems for signs of potential attacks [9]. SOCs are typically structured in a tiered system. One of the most daunting challenges for modern SOCs is recruiting and retaining sufficiently qualified entry-level security analysts (typically referred to as 'Tier 1 analysts' [19]). Tier 1 analysts are responsible for the initial triage of security alerts. Their task is to review large volumes of events in a Security Information and Event Management (SIEM) system and determine which may indicate genuine threats [73]. If analysts lack the practical skills required for this role, attacks may go undetected, potentially leading to severe consequences for the organization.

SOCs face persistent challenges to staff these analysts, (1) due to the general shortage of cybersecurity professionals[34] and (2) due the short retention rates in Tier 1 positions [70]. Having to review large volumes of noisy, often false-positive alerts while remaining vigilant for signs of real attacks, the job of a SOC analyst is monotonous yet challenging, which leads to very short retention rates, often reported to less than a year on average [65]. Given these challenges, effective onboarding training is essential for SOCs. To maintain operational readiness, this training must quickly equip new analysts to understand and accurately classify incoming alerts [45, 67]. This requires both knowledge of their role, tools, and workflows, as well as the ability to apply that knowledge

effectively in a live monitoring environment. However, conventional methods such as lectures or static e-learning often fail to provide the hands-on experience needed to detect and mitigate cyberattacks [18].

In recent years, training in cyber ranges have emerged as one way to overcome this lack of structured, hands-on training opportunities for security experts in SOCs and beyond. Cyber ranges are environments that replicate organizational networks, systems, and applications, in which participants can practice responding to realistic attack scenarios in a secure setting [57]. However, many cyber range designs emphasize technological realism while overlooking the importance of sound instructional design, that is, the deliberate use of learning theories and structured guidance to ensure participants acquire knowledge and skills effectively [53, 54]. Without clear guidance and structured learning support, participants, especially those with limited prior experience, face cognitive overload and reduced learning outcomes [12, 42]. Some prior studies have proposed instructional enhancements, typically within the Learning Management System (LMS) of a cyber range, including structured scenarios, embedded resources, and targeted feedback [6, 53, 76], but empirical evaluations remain rare and often focus on isolated design elements rather than integrated approaches. This gap leaves practitioners and researchers without clear guidance on how to create a comprehensive cyber range design that truly meets the needs of security expert trainees such as Tier 1 analysts, fostering an effective and engaging learning experience in a cyber range exercise. To this end, this study raises the following question:

RQ. *How can the integration of comprehensive instructional design principles enhance learning in cyber range exercises?*

Contribution. To address the research question, we collaborated with a commercial SOC which already uses a cyber range to train Tier 1 analysts during onboarding. This cyber range provides an isolated environment in which analysts learn to perform threat analysis with a SIEM system using data from a real attacks. While this represents an advanced technical environment for hands-on training, the way *how* trainees learn in the LMS of the cyber range in terms of instructional material, feedback and guidance was not a central aspect within the design of the exercise. To analyze how a sound instructional design can improve a cyber range exercise, we retained the original technical infrastructure and improve the trainees' learning experience through an augmented LMS. The proposed LMS, *Tier 1 Cyber Range Exercise Instructional Redesign* (T1GER), builds upon theoretical instructional design principles to integrate automated, task-level feedback, competitive elements such as a points-based leaderboard, and contextual scaffolding.

We implemented the T1GER LMS design for one existing attack scenario on the cyber range in which analysts learn to analyze a complex `log4j` attack and evaluated it in a randomized controlled trial against the original LMS. The study was conducted with $N = 144$ participants, recruited from cybersecurity courses at two European universities. The participants were randomly assigned to either the control group (original LMS design, $n = 67$) or the treatment group (T1GER design, $n = 77$). Results showed that participants using T1GER perceived the exercise as significantly more motivating and less cognitively demanding, while maintaining equivalent knowledge outcomes. They also completed the training more frequently within the allotted time and in significantly less time overall. These findings suggest that applying instructional design principles can make cyber range exercises both more engaging and more efficient, without sacrificing effectiveness.

2 Background

2.1 Security Operation Centers and Tier 1 Analysts

A SOC is a provider of security services related to network and infrastructure monitoring, attack detection and oftentimes incident response to organization(s). To monitor networks and detect cybersecurity threats, SOCs deploy technologies such as network intrusion detection systems (NIDS) and endpoint detection to generate security events. These generated security events are aggregated and organized by SIEM systems into security alerts and logs [19]. The human analysts interface with the SIEM system [9, 73] to investigate incoming alerts and discern between those related to benign events and those signaling actual threats [41]. Alert volumes vary widely depending on the size of the monitored infrastructure and sensor tuning; however, invariably, most alerts are related to benign events not indicative of a security threat [4, 45]. It is however crucial for SOCs to detect security incidents early, to minimize response time and prevent avoidable impacts on the affected organization(s) [40]. To aid a timely triaging of incoming alerts, SOCs typically employ a tiered analysis approach, where lower tier analysts (so-called Tier 1 analysts) triage alerts to clear those that are not linked to an actual attack from those that might be. Higher tier analysts (Tier 2 and 3) focus on alerts that Tier 1 analysts mark as potential incidents and perform in-depth investigations [19, 62]. Tier 1 analysts are oftentimes more junior and inexperienced than higher tiers. Furthermore, Tier 1 analysts tend to remain in the role for relatively short periods of time (due to alert burnout and the rapid accumulation of experience [65]), leading to high turnover rates in SOCs [66, 70].

2.2 Tier 1 Analyst Training in SOCs

For a tiered SOC to work effectively, Tier 1 analysts must have the ability to consistently and swiftly classify between security events which are certainly benign and those which may be more severe. Therefore, effective training for Tier 1 analyst to conduct their work is essential in SOCs. However, currently, many SOC analysts view existing trainings as ineffective [45, 66]. As different SOCs employ different tools and specific operational processes (e.g., different SIEMs, alert sets, escalation procedure etc.), the detailed training material and learning objectives cannot be duplicated from one SOC to another. Although a one-to-one duplication of training material is not effective for SOCs, there are many overarching skill sets for Tier 1 analysts. For example, virtually all SOCs (and therefore analysts) use a SIEM [9, 73] to interpret relevant logs [19, 41, 71] and analysts often use OSINT tools and the Internet to retrieve specific information on IP addresses or domains [39, 60, 68]. However, as opposed to collaborating across SOCs to develop unified training frameworks, SOCs design their own trainings [45, 79] or effectively pick and combine multiple external trainings from different vendors in the status quo.

The implementation of the training itself also differs across SOCs. Although externally organized trainings exist, those trainings are specific in nature such as certification programs or tool-specific training packages purchased from the tool developer [45, 65] which are less relevant to junior Tier 1 analysts who need to be accustomed to the fundamentals of the SOC's threat analysis process. Therefore, trainings for Tier 1 analysts tend to be internally organized, oftentimes employing a combination of passive and hands-on training strategies. Passive strategies may include reading internal documentation such as internal wikis or organizational procedures [66], or classroom setting lectures [39]. Irregardless of the effectiveness of such passive strategies, internal documents need to be maintained and lectures need to be given, both requiring expert time. Furthermore, the high turnover of Tier 1 analysts [67, 70] requires frequent training sessions, which are often scheduled ad-hoc during the onboarding of new analysts rather than at fixed intervals [66]. Hands-on trainings such as scenario-based trainings [15, 31] or capture the flag challenges [5] do exist, but are mainly targeted at training senior analysts on coordinated response rather than junior analysts on basic alert analysis skills and procedures. There is a gap for scalable and engaging basic Tier 1 analyst trainings that can be easily modified and applied across SOCs.

2.3 Cyber Range Exercises

Cyber ranges are representations of real-world digital infrastructures, such as networks, applications or entire systems, that provide a safe and legal environment for advanced cybersecurity training and testing [56]. The concept originated in the military sector in the late 2000s, following the idea of shooting ranges that provide a safe environment to practice handling of firearms without posing harm in the real world [22]. Following this concept, cyber ranges allow trainees to gain cybersecurity skills in a controlled environment without endangering real-world systems. Since their introduction, cyber ranges have spread beyond the military, finding broad applications in academia [13, 29, 32], industry [1, 3, 33], and public institutions [11, 49, 50]. A cyber range exercise refers to a specific training or testing scenario conducted on a cyber range [27]. Cyber range exercises usually simulate attack–defense situations in which trainees take on the role of attackers, defenders, or both. This enables participants to experience realistic cyberattacks and practice technical as well as decision-making skills in a structured way. The technological setup of cyber ranges can vary. Cyber ranges can be implemented as fully virtual environments, relying on virtualization to recreate systems and networks (as the cyber range in this paper), or as hybrid solutions that also integrate physical devices where higher fidelity is required [35, 37]. Due to their advanced nature, cyber range exercises are often employed (e.g., in NATO's Locked Shields exercise) to strengthen coordination between detection and response teams and to simulate sophisticated scenarios in which a red team actively attempts to evade detection.

To provide training capabilities for junior analysts, cyber ranges should maintain the real(-istic) component of their training, while incorporating a LMS to guide trainees through an exercise [78]. A LMS structures the exercise by presenting tasks, objectives, and supporting material, ensuring that participants can follow a coherent training path. Depending on the cyber range exercise design, it can provide automated scoring and feedback [10], enabling trainees to understand the consequences of their actions and learn from mistakes [75]. Beyond learning support, LMSs can be used to enhance engagement through gamification elements typical to cybersecurity exercises such as capture-the-flag challenges such as points, badges, or leaderboards, which foster motivation and competitive spirit [8, 74].

Glas et al. [28] introduce a framework to make cyber range exercises more attainable, especially for professionals with little previous experience. The study synthesized design principles from instructional models that foster authentic and complex learning, such as problem-based learning [46], cognitive apprenticeship [14] and cognitive flexibility theory [64]. The resulting framework proposes a set of instructional design principles for cyber range design: *Active participation*, *realistic environment*, *scenario operations*, *supportive information*, *procedural information*, *feedback*, *competition* and *collaboration*. These principles emphasize that training designs should not only replicate realistic technical environments, but also systematically integrate instructional strategies that support learning in the LMS of a cyber range.

2.4 Related Work

Cyber range exercises, among other types of cybersecurity exercises, are widely recognized as powerful instruments to improve cybersecurity learning, yet their design has traditionally prioritized technical infrastructure over instructional rigor. Aspects such as instructional material, feedback, or guidance are mostly only mentioned at a surface level, without explaining why they were designed in a particular way [28]. In other words, cyber range papers seldom discuss how the platform should function from an instructional perspective, and they largely omit any theoretical foundations that would justify specific learning design decisions. This tendency has led to cyber range designs that are technically sophisticated but whose LMS components, while functional, fall short of their instructional potential, often resulting in less effective learning outcomes [12]. In this regard, prior works have investigated how to improve certain aspects of cyber range designs, particularly their LMS, such as how to provide better feedback [75, 76] and how to find the right balance between guidance and independence of especially inexperienced trainees [7, 77]. However, while providing valuable insights on certain design aspects, these approaches remain insufficient on their own to create immersive learning experiences.

Moving beyond individual elements, a second strand of research explores more holistic frameworks for cyber range design. Maennel et al. [53] propose a multidimensional approach that considers social, emotional, and cognitive factors such as psychological safety and relatedness to team members. However, their framework mainly relies on anecdotal feedback and lacks concrete implementation. Glas et al. [28] propose an interdisciplinary framework of six instructional design principles that draw on established theories of authentic and complex learning. Exemplarily implemented in a small-scope cyber range exercises, their study provides first evidence that integrating instructional design principles in cyber range design can foster engagement and improve learning outcomes. We build on this framework in the present paper, applying its principles

to a complex cyber range which is used in a commercial SOC and comparing it to an existing baseline.

Looking at cyber range exercises that specifically target SOC analysts, literature remains relatively scarce. Karagiannis et al. [36] introduce a framework that emphasizes how cyber range scenarios can be structured around educational frameworks such as the NIST NICE framework [58] to avoid ambiguous learning outcomes. While this perspective highlights important instructional aspects of *what* to teach in a scenario, again, it pays relatively little attention to *how* trainees achieve these learning outcomes. Vielberth et al. [72] introduce a cyber range for Tier 1 analysts to learn to create SIEM rules for SIEM event correlation. Although their work was empirically evaluated with participants, it was neither developed nor tested in a real SOC environment, which limits its applicability to authentic Tier 1 analyst workflows

In summary, while previous research has made important contributions to the instructional design of cyber ranges, the field still remains fragmented. Most works either address isolated components or remain at a conceptual level without validation in real-world contexts. This paper addresses this gap by introducing T1GER, a comprehensive LMS design that aims to help cyber range designers to systematically improve the learning experiences in SOCs by operationalizing the interdisciplinary design principles of Glas et al. [28]. The LMS design was integrated into an existing cyber range of a commercial SOC, allowing us to investigate its effect in an operational training environment and validate the approach in a controlled empirical study.

3 Instructional Re-design of a Cyber Range Learning Management System (LMS)

In this section we first introduce the collaborating SOC, detail the existing state-of-the-art training exercise and the current LMS it employs, and the improved instructional design LMS we propose.

3.1 The Collaborating SOC

The collaborating SOC provides detection and monitoring services to numerous entities, including educational institutions and SMEs active in the manufacturing and software development industries. The SOC employs a heavily modified Security Onion [63] Linux base to deploy sensors and collect data from multiple sources. Alerts and logs are generated by a combination of Suricata signatures [24] triggered by incoming and outgoing network traffic and Sigma rules [23] from Windows/Linux hosts systems and network devices such as firewalls. The SOC's workforce varies, and generally consists of 10 to 15 employees in total, of which seven are permanently employed. From the permanent staff, four employees conduct alert investigations regularly as part of their position (two as Tier 1 analysts and two as Tier 2/3 analysts). The remainder of the employees are interns recruited from MSc-level cybersecurity programs in the region who work as junior Tier 1 analysts. As interns oftentimes have a defined internship length of one educational semester, the SOC has a high turnover rate of Tier 1 analysts and thus the SOC is accustomed to providing regular entry level trainings for Tier 1 analysts. The SOC uses (for both training as well as for operations) a defined threat analysis process that analysts employ to identify relevant evidence to investigate an alert. All trainings provided by the collaborating SOC train junior analysts on that process as well as the SIEM technology employed at the SOC.

3.2 Existing Training at the Collaborating SOC

The collaborating SOC employs a scenario-based cyber range exercise as part of their 2-week-long onboarding program for incoming Tier 1 analysts. The exercise was developed internally to grant new analysts a hands-on experience investigating alerts and the threat analysis process (TAP) used at the SOC. During the exercise, analysts interact with the same SIEM interface that is used in the SOC to perform the training tasks reproducing a real alert investigation with a given alert scenario, and answer questions related to the task throughout the training. The main objective of the exercise is not only to go through the alert analysis workflow, but to help trainees learn and internalize the process. To this end, the exercise is designed to provide trainees with guiding steps throughout the analysis, representing a deliberate balance between guidance and authenticity. The SOC has successfully employed this exercise for about 18 months prior to the experiment, and trained approximately 30 junior analysts in that period.

The SOC has identified four categories of analyst skills as key learning outcomes for the current exercise: *TAP knowledge*, *SIEM knowledge*, *Scenario-specific knowledge* and *General alert investigation knowledge*. *TAP knowledge* refers to the theoretical understanding that a trainee has about the TAP, such as what type of information should be collected in what order, or what information has to be collected in an alert investigation. *SIEM knowledge* relates to the practical ability of the trainee to navigate through and operate the SIEM interface used by the SOC, such as knowing how to find logs corresponding to a specific alert. *Scenario-specific knowledge* reflects knowledge specific to the investigated alert, such as how a specific alert is triggered, whether an alert signals a successful attack or is a false positive. Finally, *General alert investigation knowledge* applies to skills transferable across different alert investigations, similar to skills referred to in Section 2.2. Examples of such skills include the ability to interpret a variety of protocol-specific logs and the ability to use an OSINT tool effectively to investigate the maliciousness of a domain.

Before conducting the exercise, all trainees receive theoretical classroom-style trainings about the TAP, their SIEM system and the baseline knowledge to complete the exercise. These theoretical trainings are given by a senior analyst and are on average 1.5 hours long. Moreover, trainees receive and are expected to read documentation regarding commonly used open source intelligence (OSINT) tools, and a decision support system integrated in the SOC's SIEM. After the trainee has received the baseline trainings and read the required documents, the trainees receive access to the SIEM of the cyber range exercise to perform a step-by-step alert investigation based on a real scenario with real alert data.

Figure 1 shows the SIEM interface of the cyber range, identical to the SIEM used for day-to-day operations at the SOC. However, to protect the privacy of monitored customers and to keep the cyber range static in terms of the alert and log data it contains, the SIEM interface is not directly connected to the SOC's operational systems. Rather, the interface reports real network traffic and alert data collected from the network in which the SOC operates. The

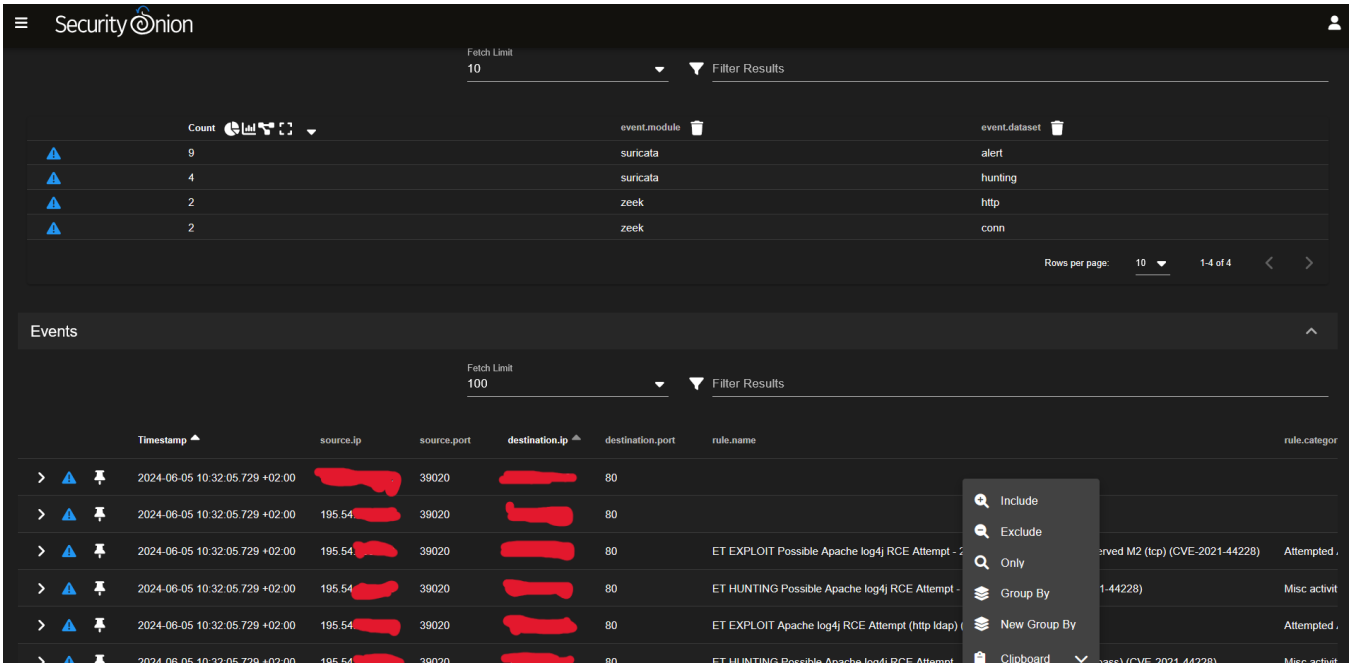


Figure 1: The SIEM interface (Security Onion Console UI [63]) used by the collaborating SOC. The upper part of the figure shows the number of logs or alerts fetched from an unknown query (not in the figure). The lower part of the figure shows the alerts and logs themselves. Sensitive information is anonymized.

network traffic data is collected in a period of 2 days and contains around 300k security events (including alerts) and 150M network logs.

3.3 Existing LMS at the Collaborating SOC

The cyber range consists of two independently operating components. The first is the SIEM interface (Figure 1), where analysts perform their tasks as described above. The second is the existing LMS, implemented as a task management interface, where analysts receive tasks to investigate in the SIEM and answer related questions. The task management interface is built on a conventional survey tool that contains a set of tasks (the number of which varies by investigated scenario). When analysts first access the LMS, they are introduced to the task of conducting an alert investigation following the TAP and are provided with contextual information, such as the IP range of the monitored customer. At this stage, the trainee also receives their login credentials and a link to the SIEM interface (directly pointing to the alert associated with the chosen scenario). The remainder of the LMS guides the trainee through the SOC's threat analysis process, explaining what information should be collected at different stages, how to collect it, and why it is relevant to alert investigations. After reviewing the explanatory text, the trainee must answer a set of questions about the alert investigation (See Figure 5 in the Appendix for examples). To do so, for each question, the trainee switches back and forth between the LMS and the SIEM interface to locate relevant information and submit responses. We note that the LMS does not provide step-by-step instructions to execute mechanically to find the answer to any of the questions. Rather, the LMS delineates what type of information the analyst should consider in order to be able to answer this question. It is then up to the analyst to seek this information within the SIEM (e.g., by identifying related or contextual alerts to the one under investigation as shown Figure 5a in the Appendix). If a trainee requires additional support during the exercise, they can consult a trainer, typically a Tier 2 analyst, who is present during the training. The trainer then guides the trainee how to proceed with the analysis (e.g., by checking and correcting a used SIEM search query) or by interpreting the SIEM events a trainee is investigating (e.g., what a certain correlation of events means in the context of the alert the trainee is investigating).

In summary, participants in the cyber range engage hands-on with realistic security alerts in a SIEM interface and work through multistep tasks (rf. Section 3.2) that mirror an authentic Tier 1 threat analysis process of a SOC. Using the framework by Glas et al. [28] introduced in Sec. 2.3 for categorization, the existing cyber range covers three principles: *active participation*, *realistic environment*, and *scenario operations,* which we summarize as *authentic environment* in the following. This reflects the advanced technical aspects of the existing training, but its relative lack of learning components offering guidance and feedback to the trainee (a training shortcoming documented across SOCs [45, 65, 66]).

3.4 T1GER: An Instructional LMS Re-Design

The T1GER LMS design fosters instructional design improvements for the principles defined in [28] of providing *procedural information*, timely *feedback* and raising trainee engagement through

Table 1: Implementation of instructional design principles proposed by Glas et al. [28] in the original LMS and T1GER, including the identified gaps that motivated the redesign.

Principle	Original		T1GER	
Authentic environment	●	Simulated SIEM system with real-world alert data and tasks to guide the threat analysis process.	●	No changes to the original design.
Procedural information	◐	Help from trainer (senior analyst) on request.	●	Structured, task-specific hints embedded in the tasks, enabling scaffolding.
Feedback	◐	Feedback from trainer (senior analyst) on request; final right/wrong summary after the exercise.	●	Immediate task-level feedback with explanations directly integrated in the exercise.
Competition	○	No motivational competitive elements.	●	Scoring system and (anonymized) leaderboard.
Collaboration	-	Excluded to preserve task authenticity.	-	No changes to the original design.

competition. Collaboration was deliberately not introduced in this iteration, as Tier 1 alert triaging is typically an individual activity in SOCs. To preserve authenticity, we retained the technical environment and the exact same task sequence and process of the original LMS described in Sec. 3.2. Details on the design improvements introduced by T1GER and the gap they fill in the original LMS are provided below. An overview of changes is given in Table 1.

3.4.1 *Procedural information.*

Gap analysis. In the original cyber range design, procedural information, i.e., how to perform the actual threat analysis process, relies strongly on the presence of a trainer, typically a Tier 2 analyst. Having a senior analyst present at a training who can provide trainees with directed and individualized guidance can surely be beneficial. However, this approach comes with several limitations. First, the quality and depth of support may vary on the individual trainer-trainee interaction, which creates inconsistencies in the learning experience across trainees and exercise sessions, e.g., if training sessions are supervised by different trainers. Second, trainees must explicitly ask for support, which not everyone might be comfortable doing, e.g., due to language-barriers. For some trainees, this additional barrier discourages them from seeking clarification, even when they would benefit from it. Senior analysts in the SOC, reflecting on their experiences with the original cyber range design prior to this study, noted that some trainees often refrained from consulting the trainer, even when support would have been necessary. Third, when multiple trainees request help at the same time, waiting times arise as the trainer addresses one participant after another. These delays disrupt the exercise flow and reduce the effectiveness of practice, especially in larger groups.

New design. To counteract these shortfalls, T1GER integrates procedural information directly into the environment. Each task includes contextual hints that provide scaffolding for solving the task. For example, the first task of the scenario we used in the empirical study evolves around the analysis of the following alert rule:

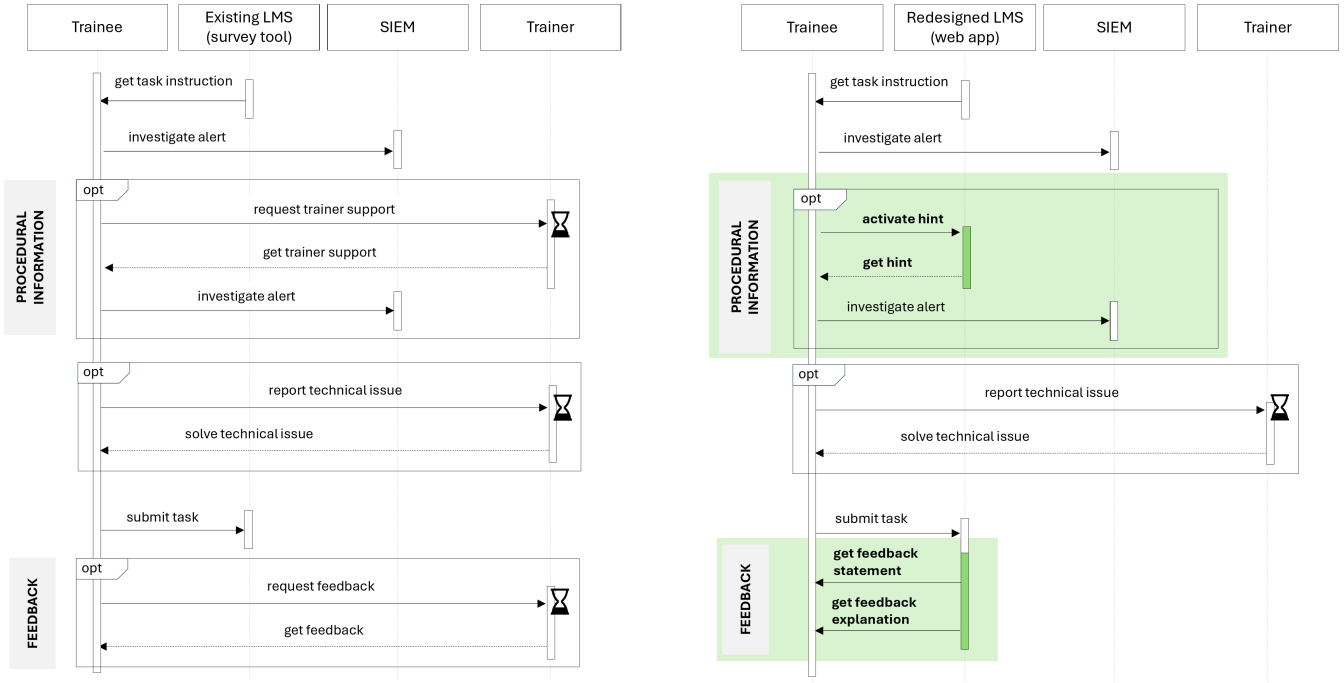
```
alert tcp any any -> [$HOME_NET,$HTTP_SERVERS] any
(msg:"ET EXPLOIT Apache log4j RCE Attempt (tcp ldap)
(CVE-2021-44228)"; flow:established,to_server;
content:"|24 7b|jndi|3a|ldap|3a 2f 2f|"; nocase;
fast_pattern;
reference:url,lunasec.io/docs/blog/log4j-zero-day/;
reference:cve,2021-44228; classtype:attempted-admin;
sid:2034649; rev:1; metadata:attack_target Server,
created_at 2021_12_10, cve CVE_2021_44228, deployment
Perimeter, deployment Internal, former_category EXPLOIT,
signature_severity Major, tag Exploit, updated_at
2021_12_10, mitre_technique_id T1055;)
```

In the first subtask around the analysis of this rule, trainees need to determine the type of traffic that triggers the alert. Here, they can activate the following hint: "The arrow (->) indicates the direction of the traffic. `HOME_NET` refers to the internal network." When using a hint, one point is deducted from the trainee's score. This deduction rule reinforces the principle of working as independently as possible, while still allowing structured support when needed. In the same way, the T1GER LMS design provides similar hints for other elements of this subtask, as well as all other components of any other task. This ensures that the trainee can move forward with their training and choose when to receive information independently, at their own pace, and for the specific elements they need aid for. Critically, this saves Tier 2 analyst time by limiting or removing entirely interventions during training.

3.4.2 *Feedback.*

Gap analysis. In the original cyber range design, feedback is limited to interactions with a trainer on request during the exercise and to a final right/wrong summary. Making feedback trainer-dependent leads to the same drawbacks as for procedural information: the feedback depends on the individual trainer, some trainees do not request it at all, and delays occur when trainers are assisting others. In contrast, the redesign delivers immediate, task-level feedback after each task.

New design. T1GER delivers immediate feedback after each task. Immediate feedback helps prevent trainees from pursuing incorrect lines of reasoning for too long and supports the development of an



(a) Existing instructional design

(b) Instructional redesign *T1GER*

Figure 2: Sequence diagrams illustrating the solution of a task in an exercise, comparing the original instructional design with the T1GER redesign. By embedding support and feedback directly into the exercise, rather than relying on on-request trainer assistance, trainees gain easier access to guidance and avoid waiting times.

accurate mental model of the TAP [17]. To leverage this effect, we enhanced the analysis process in the exercise with feedback on the individual tasks that the process is divided into. Rather than providing binary "correct/incorrect" responses, the feedback offered short explanations that made the underlying reasoning steps transparent and easier to internalize. Since the tasks are implemented in a multiple-response format, the correct solutions and explanations are deterministic rather than tailored to the individual trainee. This aligns with the nature of Tier 1 threat analysis, where the analytical steps to be followed are largely fixed and reproducible. Accordingly, after each task trainees receive not only an indication of whether their answer is correct, but also an explanation of why it is correct or incorrect, with direct reference to the relevant evidence. For example, in the subtask *"Is the alert still relevant?"*, referring to the alert rule shown above, participants get the following feedback after submitting their solution (yes/no): "*Yes mainly because the* threat *is still relevant. Even though the log4j library was updated such that the vulnerability cannot be exploited anymore, this does not mean this update was necessarily patched on all systems you are overlooking. As such, the threat is still relevant.*"

3.4.3 *Competition.*

New design. Whereas competition was not implemented in the original LMS, T1GER incorporates a scoring system and a leaderboard. We introduced this principle to enhance trainees' motivation and engagement. Prior research shows that mild, low-stakes competition can encourage learners to invest more effort, persist longer, and approach tasks more actively, which in turn strengthens the learning effect [14, 61]. The competitive elements are therefore not intended to mirror real SOC practice but to stimulate learners to try their best during the exercise and remain focused throughout, ultimately supporting deeper processing of the instructional content. In detail, participants gain points for each correctly solved task. Activating hints deducts points from their score. To preserve anonymity among peers, the leaderboard only shows a pseudonym for each trainee, which they are automatically assigned to upon registration on the LMS. The leaderboard displays the top five trainees as well as each trainee's own rank, but can be minimized if individuals preferred not to see it. In line with prior research, the goal of this competitive element is to increase motivation and engagement without creating excessive performance pressure.

3.5 Overview of Improvements and Implementation

Figure 2 shows the interaction of trainee, trainer, LMS, and SIEM in the original LMS design compared to T1GER. The redesign reduces trainer dependence by embedding support hints and feedback directly into the exercise, providing immediate information to the trainee and without requiring trainer time. This aims at improving

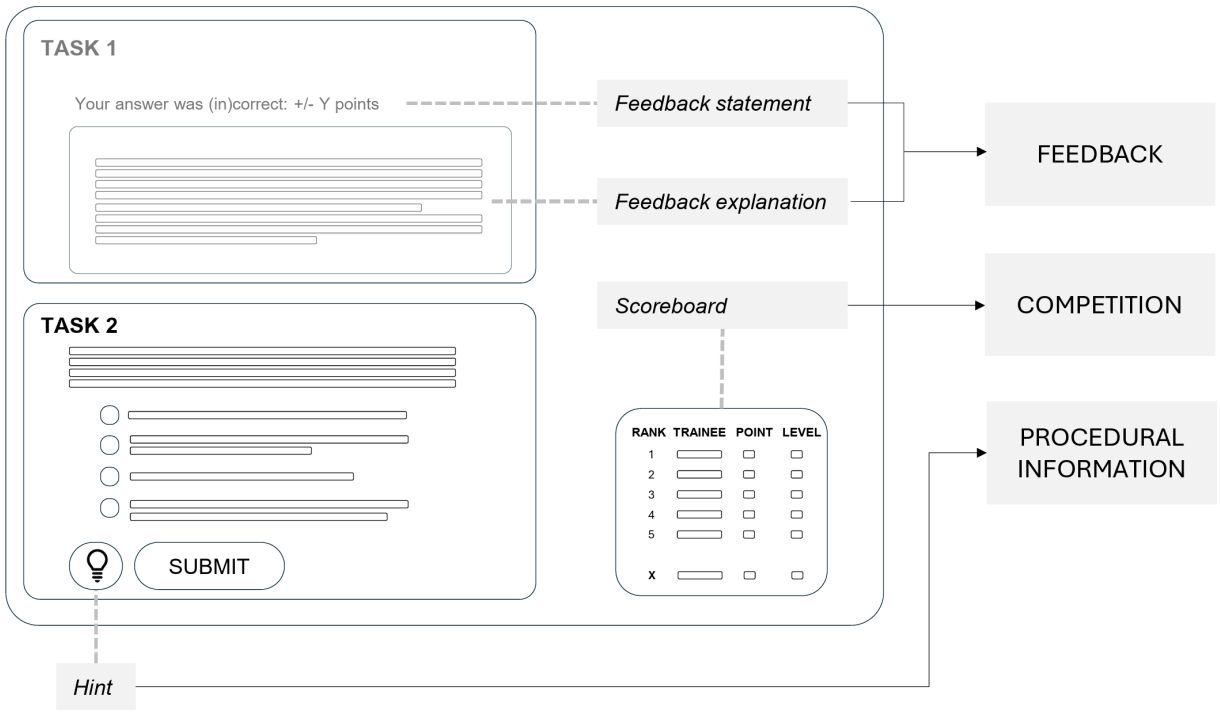


Figure 3: User interface implementing the T1GER redesign, incorporating built-in procedural information, feedback and competition, illustrated here with one completed task (Task 1) as an example.

the quality of the cyber range exercise through enhanced individual learning experiences, greater consistency, and better scalability.

T1GER was implemented as a web application, replacing the original LMS (rf. Sec. 3.3). The web application was developed with `VueJS`, while user management, scoreboard facilities, and user monitoring were implemented with `Google Firebase`. The web application dynamically generates tasks from JSON files, which define the questions, possible answers, contextual hints, and feedback explanations. This design makes it easy to add or modify tasks without changing the application itself and allows the environment to be quickly adapted for different scenarios (e.g. other alerts). As in the original design, the LMS in the form of the web application itself is independent of the SIEM system; it only provides a link that open the SIEM system in another browser tab, as in the original design. The design concept of the user interface and the applied design principles are depicted in Figure 3. Screenshots of the application are included in Figure 6 in the Appendix. The source code of the application is made available open source over a GitHub repository.[1]

4 Experiment Method

The effectiveness of the approach described in the previous section was evaluated in a randomized controlled trial, in which the T1GER LMS design serves as the treatment group (*redesign*) and the original LMS design as the control group (*control*). Method and results of this evaluation are described in the following.

4.1 Experiment Design

Our experiment involves the investigation of a security alert in the collaborating SOC's SIEM interface. The overall study design is depicted in Figure 4.

A week prior to the experiment, participants received a 1.5 hrs lecture on alert analysis delivered by a senior analyst at the collaborating SOC. The lecture covered the threat analysis process employed at the SOC and focused on the technologies attendees will interface with during the experiment. Only students who attended this preparatory lecture were eligible to participate in the experiment on day 2 of the study.

On study day 2, participants were randomly assigned to one of two experimental groups by drawing a lot from a bowl upon arrival. Depending on their assignment, participants were directed to one of two dedicated classrooms to keep the groups fully separate during the experiment. Participants assigned to the *control* group used the original LMS described in Sec. 3.3, those assigned to the *redesign* group used the T1GER LMS described in Sec. 3.4. Both groups share the same technical platform, i.e., SIEM system and data as outlined in Sec. 3.2. For the *control* group, a researcher and a Tier 2 analyst from the SOC were present in the room to address participants' content-related questions as they arose. Another researcher was present in the room with the treatment *redesign* group. However, as the T1GER LMS design is deliberately designed to include all necessary instructional materials within the LMS, the researcher was solely available for the participants to address technical or infrastructure-related issues. This also reflects the overall setup

[1] https://github.com/potiri/T1GER/

delineated in Figure 2 whereby with the new design expert time is not needed to assist trainees.

The training session was limited to 90 minutes. At the end of the investigation, participants filled in a posttest questionnaire to measure perceived learning experience and learning outcomes. Details of this test are reported in Sec. 4.3. Participants who were unable to complete the training within this time frame were instructed to discontinue the exercise after 90 minutes and continue with the posttest.

During our experiments subjects are asked to investigate an alert related to the `log4j` vulnerability, a severe vulnerability in an Apache security logging library that allows unauthenticated users to execute arbitrary code on the system. This alert is part of the original training offered at the collaborating SOC, and it was selected as it develops through all phases of the SOC's analysis process and requires the consideration of contextual alerts and logs, alert history related to the target, and the identification of evidence that the attack was (un)successful. Participants perform this analysis in a real environment and with real operational data such that additional alerts and logs related to involved systems, as well as other systems, fully represent what an analyst would have to navigate through during a real investigation.[2] The same scenario with the same set of tasks defined in the original LMS (in the case of the `log4j` scenario, 16 tasks) was used for both groups.

4.2 Subjects and Recruitment

Participants were recruited from a Bachelor-level course at a German university (February 2025) and a Master-level course at a Dutch university (December 2024). All students enrolled in the course were invited to voluntarily participate in the exercise. Students were encouraged to participate both through the opportunity to gain hands-on experience with a real-world incident in a SIEM system and through bonus points awarded for participation in both courses' final examination. These bonus points were not tied to students' performance in the training and served as the only form of compensation. Otherwise, no form of monetary or material incentives were provided.

In total, 157 students participated in the training. One participant in the *redesign* group did not complete the posttest and was excluded from analysis. Twelve additional participants (four in the *redesign* group and eight in the *control* group) were excluded for failing an attention check in the posttest questionnaire. Thus, the resulting final sample comprised 144 participants, with 77 students assigned to the *redesign* group and 67 to the *control* group.

An a priori power analysis was conducted to determine the required sample size to detect a medium-sized effect (d = 0.4) with 80% power using a two-sided independent samples t-test at α = .05. The analysis indicated that a total of 198 participants (99 per group) would be needed. As the final sample size with 77 and 67 participants was below that threshold, we conducted a *post-hoc* power analysis based on the observed group differences in the two learning experience measures, where we expected to see differences between the two groups. For *learning motivation*, the resulting effect size was Cohen's $d = 0.53$, yielding an estimated power of 88.7%. For *cognitive load*, the resulting effect size was $d = 0.56$, with a power of 91.1%. These results indicate that the final sample was sufficiently powered to detect medium-sized effects in the two groups.

[2]Because the original SOC training spans multiple alerts, we worked with the collaborating SOC to select a subset that kept the experiment realistic yet manageable. We chose alerts for which all steps of the SOC's investigation procedure were relevant, selecting `log4j` in particular because it requires analysts to examine multiple data sources across all investigation phases. This also aligns with the SOC's regular training practice, in which analysts focus on only a limited number of alerts per day.

4.3 Measures and Data Collection Procedure

To assess the effectiveness of the instructional design, we employed both validated psychometric instruments and performance-based domain knowledge tests. The full questionnaire is provided in Appendix G.

Learning experience. We measured participants' learning experience using two self-report scales. *Learning motivation* was assessed via the twelve-item Reduced Instructional Materials Motivation Survey (RIMMS) [52], e.g. "The content and activities of this training held my attention". This instrument is grounded in Keller's ARCS model of motivation, covering four conditions for a motivating learning experience: Attention, Relevance, Confidence, and Satisfaction [38]. The second, *cognitive load*, was assessed using the three-item extraneous cognitive load scale by Klepsch et al. [43]. The scale was inverted indicating that higher values indicate less cognitive load, e.g., "During this training, it was easy (in the sense of non-exhausting) to find the important information." That way, both variables (*learning motivation* and *cognitive load*) can be read so higher values indicate a better learning experience. Both variables were self-assessed by the participants via a five-point Likert scale, ranging from 1 = "Totally disagree" to 5 = "Totally agree". Cronbach's alpha values indicated adequate reliability for both *learning motivation*, $\alpha = .91$, $r = .45$, and *cognitive load*, $\alpha = .81$, $r = .59$. These values suggest that both scales can be interpreted as internally consistent composite measures.

Learning outcomes. Domain-specific learning was assessed using twelve multiple-response knowledge items grouped into four categories, aligned with the defined learning outcomes of existing training (rf Sec. 3.2). *Threat analysis process knowledge* assessed understanding of procedural steps of the cyber threat analysis process. *SIEM knowledge* measured technical knowledge related to working with the SIEM tool. *Scenario-specific knowledge* comprised questions about the `log4j` alert the participants investigated during the training. *General alert investigation knowledge* tested participants' ability to apply what they learned to other alerts. Each category comprised three questions with four response options, of which one was correct (rf. Appendix G). Scores were averaged to obtain a category score ranging from 0 to 1. *Total completion time* was assessed as the duration, in seconds, that participants spent from starting the exercise until its completion, based on system-recorded timestamps. To access the posttest, participants were required to reach the final question of the training. In cases where they were unable to complete the training within the allotted time, they were instructed to skip the remaining tasks in order to proceed and to indicate in the posttest that they had not completed the training within the given time limit of 90 minutes. This variable, *training completion*, was measured with a single posttest item (*yes*/*no*). Importantly, to ensure the validity of this measure, *total completion*

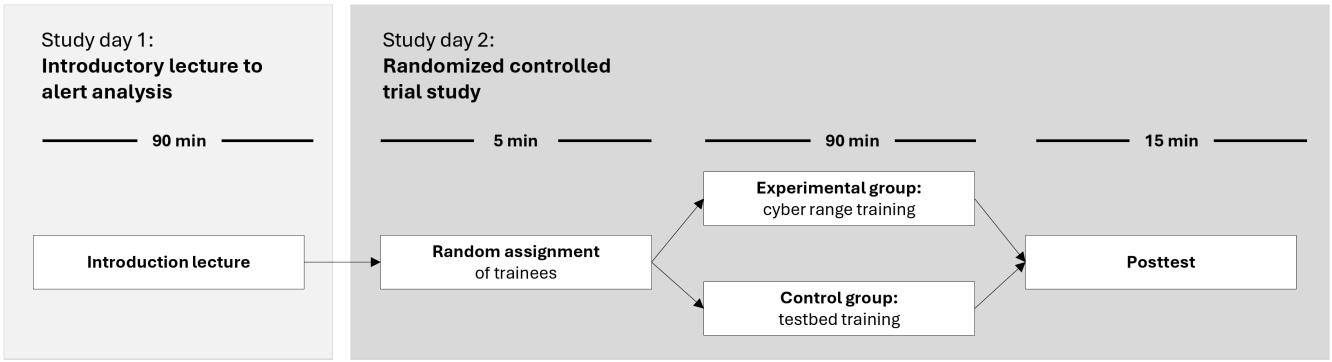


Figure 4: Study procedure

time was only analyzed for participants who self-reported having fully completed the training. It was made clear to the participants that compensation was not dependent on completing the exercise. If participants did not answer the attention check question in the posttest questionnaire correctly, their data was excluded from the analysis, but they still received compensation.

Hints. To enable further analyses within the *redesign* group, we recorded the number of hints (principle of *procedural information*) participants used during the exercise.

4.4 Data Analysis

For the dependent variables regarding participants' learning outcome (*TAP knowledge, SIEM knowledge, scenario-specific knowledge,* and *general alert investigation knowledge*, *training completion* and *total completion time*) and participants' perceived learning experience (*learning motivation* and *cognitive load*) a descriptive analysis (i.e. means and standard deviations) was carried out. Given the ordinal scale format and the non-normal distribution of several variables, group differences between the *redesign* and *control* groups were assessed using Mann–Whitney U tests. Effect sizes r were calculated for each comparison, and Holm corrections were applied to adjust for multiple testing. To provide a more tangible interpretation of participants' *learning experience*, we conducted Chi-square tests of independence to compare the proportion of participants reporting *positive learning experiences* between groups. Specifically, we binarized responses from *learning motivation* and *cognitive load* into *positive* (values > 3, i.e. "neutral") and *negative* (values ≤ 3) ratings. We then calculated the proportions within each group (*redesign* vs. *control*) and tested for differences. Phi coefficients were computed as a measure of effect size. To initially examine associations between the dependent variables and background variables (*gender*, *English proficiency*, *SOC experience* and *educational level*) pairwise Pearson correlations were computed, including significance levels. Finally, multiple linear regression models were fitted for each dependent variable to assess the predictive effect of group assignment while controlling for background variables that showed an effect in the correlation analysis. For *training completion*, a logistic regression model was employed. To better explain the results within the redesign group, we conducted an additional exploratory analysis of *hint* usage. Specifically, we computed a separate correlation matrix for this group only, followed by regression models assessing whether *hints* predicted the dependent variables while controlling for background variables; for *training completion*, consequently, a logistic regression model was used. All analyses were conducted using R (version 4.5.1) [59]. For reproducibility, the full anonymized data set and the R syntax is available in the GitHub repository (rf. Sec. 3.5).

4.5 Ethics

Informed consent for participation in the study was obtained from all students. Participants were explicitly informed that their data would be anonymized and that they could withdraw their consent at any time. The study received ethical approval from the institutional review boards of both participating universities. Participants were informed that they were taking part in a study comparing two instructional designs. After completing the training and the posttest, participants were given the opportunity to access the alternative training format, if they wished to do so.

5 Results

Regarding participants' *gender*, 96 participants self-identified as *man*, 46 as *woman*, one as *non-binary* and one participant selected "prefer not to say". Participants' *education level* was reported as either enrolled in a *bachelor*'s or *master*'s degree program: 54 were *bachelor* students and 90 *master* students. Since the training was in English and the majority of participants were not native English speakers, the participants' level of English proficiency may have influenced their understanding of the training content. To this end, *English proficiency* was assessed as an additional background variable. On the European CEFR scale, a total of 66 participants reported "Advanced English (C1)", 52 reported "Proficient (C2)", 23 selected "Upper-intermediate English (B2)", and 3 selected "Intermediate English (B1)". For the correlation and regression analyses, *English proficiency* was coded as a binary variable as either very high (C2) or intermediate (B1, B2, C1). Lastly, we assessed whether participants had prior experience working as SOC analysts or with a SIEM system (*SOC experience*). Overall, 8 participants selected "Experience with a SIEM system from educational/private settings", 3 selected "Experience in a SOC (less than one year)", and 2 selected

Table 2: Descriptive analyses of the two groups (*redesign*: $n = 77$, *control*: $n = 67$).

(a) Sample description by group (total numbers).

	Redesign	Control
Gender		
Man	51	45
Woman	25	21
Non-binary	1	0
Prefer not to say	0	1
Education Level		
Bachelor	28	26
Master	49	41
English Proficiency		
Intermediate (B1)	2	1
Upper-intermediate (B2)	13	10
Advanced (C1)	28	38
Proficient (C2)	34	18
SOC Experience		
No experience	70	61
Edu./priv. experience	4	4
Practical experience (< 1 year)	1	2
Practical experience (> 1 year)	2	0

(b) Mean and standard deviations (in parentheses) for dependent variables.

	Redesign	Control
Learning experience		
Learning motivation	3.7 (.71)	3.33 (.70)
Cognitive load	3.49 (.82)	3.01 (.90)
Learning outcomes		
TAP knowledge	.55 (.30)	.57 (.32)
SIEM knowledge	.68 (.26)	.69 (.27)
Scenario-specific knowledge	.57 (.31)	.58 (.29)
General alert investigation knowledge	.44 (.29)	.54 (.31)
Training completion	.86 (.35)	.69 (.47)
Total completion time (min)[a]	64.92 (10.31)	73.37 (18.48)

[a] Total completion time was only analyzed for participants who completed the training within the allotted time ($n = 105$). Due to recording errors for five participants in the *control* group, the final sample comprised $n = 66$ for the *redesign* group and $n = 41$ for the *control* group.

"Experience in a SOC (more than one year)". For the correlation and regression analyses, *SOC experience* was again coded as a binary variable, distinguishing between any form of SOC experience (educational, less than one year, or more than one year) and no SOC experience. The distribution of background variables in the two groups is provided in Table 2 (a).

5.1 Group Differences

To examine group differences in learning experience and learning outcomes, we first conducted a descriptive comparison and then conducted inferential analyses.

Learning experience. Participants in the *redesign* group reported higher scores in both *learning motivation* ($M = 3.71$, $SD = 0.71$) and *cognitive load* ($M = 3.49$, $SD = 0.82$) than those in the *control* group (*learning motivation*: $M = 3.33$, $SD = 0.70$; *cognitive load*: $M = 3.01$, $SD = 0.90$). Mann–Whitney U tests confirmed these differences as significant: *learning motivation*, $U = 3360$, $p = .001$, $r = .26$; *cognitive load*, $U = 3382.5$, $p = .001$, $r = .27$. When categorizing *learning experience* into *positive* and *negative*, Chi-square tests revealed significant group differences in the proportion of participants reporting positive experiences. Categorizing in positive and negative learning experiences, a significantly higher proportion of participants in the *redesign* group reported a positive *learning motivation* compared to the *control* group. Specifically, participants in the *redesign* group were about 1.6 times more likely to report positive *learning motivation* than those in the *control* group, $\chi^2(1, N = 144) = 4.99$, $p = .025$, $\phi = -.20$. Similarly, they were roughly 1.7 times more likely to report a positive *cognitive load*, $\chi^2(1, N = 144) = 5.86$, $p = .015$, $\phi = -.22$.

Learning outcomes. For knowledge-related variables (*TAP knowledge*, *SIEM knowledge*, *scenario-specific knowledge*, and *general alert investigation knowledge*), descriptive analyses suggested a slightly better mean performance in the *control* group, but Mann–Whitney U tests did not reveal significant differences, indicating that learning outcomes were comparable between groups (rf. Table 2 (b)). Regarding completion, out of the 77 participants in the *redesign* group, 66 ($M = .86$, $SD = .35$) reported completing the training within the allotted time, compared to 46 out of 67 participants ($M = .69$, $SD = .47$) in the *control* group. A Chi-square test confirmed this difference as significant, $\chi^2(1, N = 144) = 5.08$, $p = .024$, indicating that participants in the *redesign* group were more likely to complete the training in time. For those who did complete the training in time, participants in the *redesign* group spent on average less time ($M = 64.92$, $SD = 10.31$ minutes) than their peers in the *control* group ($M = 73.37$, $SD = 18.48$ minutes). A Mann–Whitney U test confirmed this difference, $U = 745$, $p < .001$, $r = .33$, based on $n = 66$ in the *redesign* group and $n = 41$ in the *control* group (five cases in the latter excluded due to recording errors). Since the same participants were tested across multiple dependent variables, we applied a Holm–Bonferroni correction across the eight outcome tests. After correction, the group differences remained significant for *total completion time* ($p = .0008$), *learning motivation* ($p = .0106$), and *cognitive load* ($p = .0085$). The effect on *training completion* did not remain significant after adjustment ($p = .0725$). This confirms that the primary effects on learning experience and efficiency are robust, while differences in knowledge outcomes and completion rates may reflect smaller or more variable effects that warrant further investigation.

5.2 Group Comparisons Accounting for Background Variables

To examine whether observed group differences remained after adjusting for background variables, linear models were estimated for

Table 3: Regression results for dependent variables related to *learning experience* and *learning outcome* controlling for *education level, English proficiency, gender,* and *SOC experience.*

	Learning experience		Learning outcomes					
Predictor	*Motivation*	*Cogn*	*TAP*	*SIEM*[a]	*Scenario*	*General*	*TT (min)*[b]	*Comp*[c]
group (*redesign*)	.35**	.45**	-.04	-.02	-.03	-.10*	-8.35*	1.14**
SE	.11	.14	.05	.05	.05	.05	3.48	.44
Educational level (Master)	.41**	.54***	.08	.09.	.12*	.05	7.59*	-0.02
SE	.13	.15	.06	.05	.05	.06	3.16	.47
English proficiency (high)	.07	.07	.11.	.09.	.08	.04	-1.02	-0.45
SE	.13	.16	.06	.05	.06	.06	2.51	.50
SOC (yes)	.36.	.42.	.07	.15*	.12	.09	0.39	1.42
SE	.20	.24	.07	.06	.08	.09	3.92	1.09
gender (f)	-.06	-.15	.08	-.03	-.07	.03	1.48	-0.80.
SE	.12	.15	.05	.05	.05	.06	2.24	.46
R^2_{adj}	.17	.20	.03	.10	.09	.02	.10	–
F (5,138)	7.04***	7.98***	1.99.	4.16**	3.93**	1.46	4.15**[b]	–

Note. Coefficients reflect the effect of being in the *redesign* group relative to the *control* group. * $p < .05$, ** $p < .01$, *** $p < .001$. Motivation: *learning motivation*, Cogn: *cognitive load*, TAP: *TAP knowledge*, SIEM: *SIEM knowledge*, Scenario: *scenario-specific knowledge*, General: *general alert investigation knowledge*, TT: *total completion time* in minutes, Comp: *training completion.* English proficiency (high): *English proficiency* dummy variable coded 1 = very high (C2), 0 = intermediate (B1, B2, C1). Educational level (Master): *Educational level* dummy variable coded 1 = Master's degree, 0 = Bachelor's degree. Gender (f): *Gender* dummy variable coded 1 = female, 0 = all other categories. SOC (yes): *SOC experience* dummy variable coded 1 = SOC experience, 0 = no SOC experience.

[a] HAC-robust standard errors used for *SIEM* due to autocorrelation in residuals.

[b] HAC-robust standard errors used for *TT*; $F(5, 102)$ due to missing data.

[c] Logistic regression; coefficients are log-odds. Odds ratio for group = 3.14. No F-test or R^2_{adj} reported.

each outcome variable listed in Table 2 (b). Before conducting the regression analysis, we examined bivariate correlations between all dependent variables and background variables (rf. Table 5 in the Appendix). Pearson correlations were computed for the full sample. *Gender (female)* correlated significantly with *scenario-specific knowledge*, showing a small effect size ($r = -.18$). Both *education level* and *English proficiency* were significantly associated with multiple dependent variables and were retained as covariates in the main analyses.

Prior to interpreting the regression models, we examined the underlying assumptions of multiple linear regression. Residual plots were inspected to assess linearity, homoscedasticity, and the presence of outliers. The normality of residuals was evaluated using Q-Q plots and the Shapiro–Wilk test. Multicollinearity was examined before as part of the correlation analysis. The Durbin–Watson test was applied to assess the independence of residuals. For *SIEM knowledge* and *total completion time*, the Durbin–Watson test indicated significant autocorrelation; therefore, heteroskedasticity- and autocorrelation-consistent (HAC) standard errors were applied. In the following, we report the findings of the regression models. The full results of the analyses are provided in Table 3.

Learning experience. The model for *learning motivation* was statistically significant, $F(4, 139) = 7.04$, $p < .001$, $R^2_{\text{adj}} = .17$, with significant effects of *group* ($\beta = .35$, $p = .003$) and *education level* ($\beta = .45$, $p = .001$). *English proficiency*, *SOC experience* and *gender* were not significant predictors. Similarly, the model for *cognitive load* reached significance, $F(4, 139) = 7.98$, $p < .001$, $R^2_{\text{adj}} = .20$, with effects for *group* ($\beta = .45$, $p = .001$) and *education level* ($\beta = .54$, $p < .001$), but not for the remaining covariates. These findings confirm the non-parametric group comparisons, showing that participants in the *redesign* group consistently reported higher *learning motivation* and lower *cognitive load* than those in the *control* group, independently of background variables.

Learning outcomes. Although the group effect reached significance in the model for *general alert investigation knowledge*, the overall model was not statistically significant, indicating that the included predictors explained little variance in this outcome. Thus, no significant effect of *group* could be observed overall. Regarding background variables, the model for *SIEM knowledge* was significant, $F(4, 139) = 4.13$, $p = .003$, $R^2_{\text{adj}} = .08$, and showed significant effects of *education level* ($\beta = .10$, $p = .033$) and *SOC experience* ($\beta = .15$, $p = .010$). Similarly, the model for *scenario-specific knowledge* was significant, $F(4, 139) = 4.35$, $p = .002$, $R^2_{\text{adj}} = .09$, again showing a significant effect of *education level* ($\beta = .13$, $p = .021$). No other background variables reached significance in these models.

The logistic regression model for *training completion* indicated that participants in the *redesign* group were over three times more likely to complete the training compared to those in the *control* group, $B = 1.14$, $SE = 0.44$, $z = 2.58$, $p = .010$, $OR = 3.14$. The model for *total completion time* also showed a statistically significant effect of group, while accounting for background variables, $F(4, 102) = 4.15$, $p = .004$, $R^2_{\text{adj}} = .11$.; participants in the *redesign* group completed the training significantly faster than those in

the control group, $\beta = -8.35$, $p = .018$. However, unexpectedly, completion time increased with higher *education level*, $\beta = 7.59$, $p = .018$, suggesting that participants with more advanced educational backgrounds spent more time on the exercise, possibly engaging in more detailed analyses of the alert. Combined with insights from the scenario model, it emerges that higher scenario knowledge comes at the cost of a higher time spent on the exercise, and that specialized cybersecurity knowledge plays a significant role on both outcomes. This suggests that nuances related to the investigated attack are only apparent to more specialized analysts. In this context, the T1GER approach appears to significantly improve training *efficiency*, reducing required time while still supporting more specialized analysts in conducting thorough investigations.

5.3 Effect of Hints within Redesign Group

To better understand how trainees engaged with the T1GER redesign and whether specific interaction patterns could have driven the observed learning outcomes, we conducted an exploratory analysis within the cyber range group focusing on the improvement of procedural information, i.e., in-system hint usage, as an independent variable. Thus, we investigated if the usage of *hints* had an effect on *learning experience* or *learning outcomes*.

On average, participants used 2.16 ($SD = 1.93$) out of 16 available hints, indicating that trainees did not rely on hints by default but requested them only when necessary, as intended by the scoring system. Regression assumptions were checked as in the full-cohort models, and no violations were observed. Correlations showed significant associations only with *scenario-specific knowledge* and *general alert investigation knowledge*. This pattern was confirmed in the regression analyses accounting for background variables, which showed significant effects only for *scenario-specific knowledge*, $\beta = -0.04$, $p = .026$, and *general alert investigation knowledge*, $\beta = -0.04$, $p = .038$. Meanwhile, *hint* usage had no effect on learning experience (*learning motivation* and *cognitive load*), nor on *training completion* or *training completion time*. The full results of the correlation and regression analyses can be found in the Appendix (Tables 6 and 7).

These results suggest that the scaffolding mechanism to provide procedural information functioned as intended: hints were used sparingly and primarily by participants who encountered greater difficulty, which is reflected in the small negative effects on the two knowledge variables. However, relying on hints did not provide a substantial performance advantage or enhance the learning experience. This indicates that the effectiveness of the T1GER redesign is not attributable to the procedural-information feature alone but reflects the broader set of instructional principles embedded in the design.

Summary of findings. Our findings demonstrate the advantages of the T1GER LMS design. Directly comparing means in the two groups with non-parametric tests, participants in the *redesign* group reported significantly more favorable learning experiences, meaning they found the experience more motivating and less cognitively demanding than their peers in the *control* group. The regression analyses confirmed these results, accounting for *education level*, *English proficiency*, and *gender*. Similarly, for completion and efficiency, Chi-square tests showed that a higher proportion of participants in the *redesign* group completed the training within the allotted time, and Mann–Whitney U tests confirmed that they did so in significantly less time. These findings were corroborated by regression analyses, which demonstrated that participants in the *redesign* group finished the exercise in on average 8 minutes, i.e., 12%, faster, even after controlling for background variables. Notably, while higher *education levels* predicted longer *completion times*, the T1GER reduced time demands across the board, indicating that the intervention enhanced training efficiency without disadvantaging more advanced participants. With respect to learning outcomes, no reliable group differences were found. Both the non-parametric tests and regression models indicated comparable performance between groups. In summary, these results underline that the T1GER LMS design can improve subjective learning experience and learning efficiency without compromising objective learning gains. An exploratory analysis of *hint* usage within the *redesign* group further showed that the procedural information (scaffolding) operated as intended, used mainly when participants struggled, and did not itself account for better learning experience or outcomes of the *redesign* group. This indicates that the benefits of the T1GER LMS arise from the combined instructional principles rather than only from providing trainees with more procedural information.

6 Discussion, Limitations, and Future Work

Our findings show a significant improvement in learning motivation and cognitive load for subjects who trained with T1GER. This suggests that alert investigation exercises become more engaging while less cognitively demanding by applying instructional design principles to cyber ranges. As analysts oftentimes find their trainings to be insufficient [45] and as alert investigation is a cognitively demanding task by nature [30], the improved learning motivation and cognitive load may significantly improve learning efficiency and engagement by new analysts.

Interestingly, our results show that our approach does not affect the achieved learning outcomes. Therefore, no extra training would be required to compensate for our proposed LMS redesign, as our results suggest that participants learn equally as much as the less engaging training requiring more cognitive load. Moreover, our findings indicate that the completion rate (within 90 minutes) and the time to complete both improve significantly by employing the proposed redesign. Therefore, T1GER training appears to be more efficient and to contribute to decreasing the training effort for trainee and trainers alike.

An interesting nuance is the role of background education. Our findings suggest that analysts with a more specialized cybersecurity background develop a more thorough understanding of the investigated scenarios, at the cost of a higher investigation time. On the other hand, the improved efficiency of the T1GER approach reduces time requirements, thus promoting swift yet effective trainings without penalizing thorough investigations.

6.1 Implications for practice

Typically, training in SOCs is either insufficient in material [66], not engaging [31], or requires large setup in terms of IT infrastructure

and training staff [5, 44]. As knowledge conveyed in alert investigation trainings can be exceptionally specific [31, 45], most SOCs are not able to employ a dedicated trainer. Yet, scalable training solutions do not appear to be widely available, or adopted. Our proposed T1GER LMS design tackles this issue directly by allowing SOCs to employ trainings with as much content while reducing the need of domain-specific trainers. Although SOCs are required to initially adapt the training to their needs (e.g., devise a fitting scenario or modify the questions), SOCs are required to undertake such actions already to achieve hands-on trainings considered to be best practice by prior research [16, 26]. Moreover, as SOCs oftentimes have ad-hoc hiring and training schedules, executing the training requires a high workload.

In addition to SOCs already focused on designing and executing trainings, the T1GER approach benefits SOCs without a well-defined or any training program as well. As new analysts in such SOCs oftentimes shadow senior analysts for a period of time [66], the shadowed analyst may be distracted from a shadowing trainee. Since alert investigations is a task already associated with high cognitive load and fatigue, further distractions for senior analysts may lead to slower and inaccurate alert investigations. By contrast, the integration of the T1GER LMS design significantly reduces the requirement for analyst time, resulting in higher efficiency of the training activity. Moreover, as our solution does not require domain-specific trainers or different senior analysts, the training becomes more reproducible and consistent by design. This is in line with the fact that standardization and compliance are becoming increasingly relevant to the security industry [69], making reproducibility even more crucial for SOCs.

Beyond SOCs as organizational units, the increased learning motivation of our proposed solution benefits prospective analysts as well. Additional engagement during skill development prolongs the duration in which the analyst is engaged by applying their newly acquired skills (i.e., their work as a SOC analyst), which may contribute to mitigating the diverse causes of analyst burnout [20]. Similarly, lower cognitive load during skill development may lead to a lower incidence of fatigue and other stress-related problems.

Finally, our findings point out the importance of specialized knowledge on the efficiency and thoroughness of the analyst training. This suggests that SOCs looking for junior analysts may benefit from recruiting cybersecurity-trained junior professionals, to improve the effectiveness and efficiency of non-specialized cybersecurity trainings and confirming findings in related work [45]. This also indicates that specialized detection engineering training programs, currently only marginally included in computer science curricula [2], could help form a proficient workforce in the security monitoring and response domains.

6.2 Implications for Research and Future Work

Our study highlights that applying the instructional design principles into alert investigation trainings significantly reduces the cognitive load of analysts. Whereas T1GER improves cognitive load during training, other critical SOC processes such as threat hunting and incident response remain to be addressed. Previous studies [36, 72] exist in which cyber ranges or specific scenarios have been proposed for trainings relevant to SOCs. In line with this, future work could implement and evaluate the effect of instructional design principles into SOC trainings beyond alert investigation with learning outcomes more inline with such tasks. This is especially relevant as trainings of different tasks are conducted separately in SOCs [45, 66], and thus effective scalability of trainings only can occur if other trainings are scaled as well. Similarly, different SOCs may prioritize different scenarios for training, for example including different attack patterns or data sources to the investigation. Therefore, future work could research effective generation of tailored training scenarios, perhaps (semi-)automatically.

Considering learning outcomes in alert investigation exercises, our work does not assess the potential long-term effects of T1GER, specifically with respect to retaining the learning outcomes. Although longitudinal studies are difficult to conduct with job positions suffering from high-turnover rates such as Tier 1 analysts, a longitudinal study would be critical to better understand how each learning outcome is affected differently through applying the instructional design principles. Further considering learning outcomes, our work is inconclusive in how to improve (as opposed to maintain) learning outcomes compared to currently employed trainings. Future work could consider how to ensure prospect analysts understand the key material better while maintaining scalability. Especially as automation and human-AI teaming becomes more relevant by the day in SOCs [70], new learning outcomes to alert investigation trainings may need to be considered such as the ability to critically evaluate explainable AI justifications [21, 51] for alert labeling as opposed to directly evaluating the (lack of) evidence of network logs. Moreover, through the use of AI, graph-based visualizations become more feasible by accounting for the context of the alert more effectively [55, 70]. Therefore, skills relating to using SIEMs, such as using queries effectively to find relevant information, become less relevant compared to interpreting interrelations between triggered alerts.

Moreover, research about trainings in other domains highlight promising benefits of employing LLMs and/or agentic AI as sparring partners to the trainee [25, 47, 48]. Further research could develop new lines to evaluate such technologies in supporting and reasoning along the trainee during the investigation, as an effective sparring partner further alleviates the need of an external or a senior employee acting as a trainer. This could extend prior approaches in the domain of decision support systems for security analysts [40] where tailored trainings can be made for such systems, or develop new directions where the integrated hints and feedback proposed in T1GER are tailored to the specific decisions of the trainee analyst. Particularly, these evaluations should be task specific (e.g. threat hunting as opposed to incident reporting) and subject-profile specific (e.g. senior rather than junior analysts). Importantly, it remains an open question whether model specialization (e.g. cybersecurity-specific models such as CISCO's Foundation-sec-8B model, SecureBERT, and others) and fine-tuning for specific tasks (e.g. CISCO's Foundation-sec-8B-reasoning for cybersecurity reasoning tasks) impacts the quality and effectiveness of analyst task support. Our findings also suggest that learning goals related to the process and the technology (i.e., TAP, SIEM, and general knowledge) can be adequately achieved also by relatively non-expert trainees with a

general information systems education rather than a specialized cybersecurity background. This testifies to the suitability of this type of training approach to a broad range of recipients, possibly providing the basis for a portfolio of specializations other than detection, such as communication, incident coordination, or response.

The results of our study demonstrate that the redesign, grounded in a set of literature-based principles, improved the exercise compared to the original version. Our evaluation focused on the effectiveness of the integrated design as a whole, not on how individual principles contributed to this improvement. Although the exploratory analysis of hints offered initial insight into the role of scaffolding procedural information, the remaining principles were not monitored separately. Accordingly, a promising direction for future research is to investigate the standalone and interacting effects of individual principles in more detail.

Another direction for future research concerns the deliberate balance between authenticity and guidance in the redesigned exercise. Because the exercise targets novice participants, the design intentionally incorporated more guidance (e.g., immediate feedback and hints) than analysts would encounter in a real-world analysis process. This trade-off was made to support learning, even if it meant deviating from full operational authenticity. Future work could investigate how this balance should shift for more experienced participants, for whom reduced guidance or more realistic feedback conditions may be beneficial. Such research could help determine how to adapt cyber range designs to different skill levels while maintaining both authenticity and instructional effectiveness.

6.3 Threats to Validity

Construct validity. The threat landscape is dynamic even within one SOC, as zero-day vulnerabilities are discovered, used and then slowly patched as time elapses. In other words, the chosen scenario relating to the `log4j` vulnerability may not realistically reflect the day-to-day operations of a Tier 1 analyst. Yet, the overall process in SOCs, is more static. Concepts of IDS generating alerts and collecting relevant information about and surrounding the alert is at the foundation of how SOC analysis works in practice. There is little indication to believe that this process and data is changing in the near future.

Internal validity. As our experiment considers a diverse sample from different universities and academic experiences, we accounted for several background factors. However, in reality, participants from one group may have different relevant skill sets affecting the performance of their training. These skills may stem from a plethora of other factors, such as relevant job experience, affinity with intrusion detection or media literacy on recent zero-day vulnerabilities. However, many factors possibly relate to educational level, where relevant education is often required to acquire the relevant job experience, or where cybersecurity specific education programs increase the ability (and possibly the affinity) to understand recent vulnerability blog posts or reports. As it is unfeasible to consider all potential factors, we captured a limited set of background variables about our subjects.

External validity. We identify two external threats to validity in our work. Namely, the generalizability of our student subjects to SOC recruits and the training material of the collaborating SOC and its context to other SOCs. Most of our subjects are students and may not be aspiring to be SOC analysts nor have the same skill set that a SOC analyst might have at the time of recruitment before the initial training. This is especially the case for 43 subjects following a general information systems Bachelor. However, Tier 1 analysts are oftentimes considered entry-level positions, and many SOCs recruit analysts immediately after completing an IT-related Bachelors program [60]. Therefore, our subjects, especially those studying at a cybersecurity specific MSc program, have sufficient capacity as potential entry-level recruits to participate in our training. Moreover, to mitigate the potential gap between our subjects and recruits, we solely focused on exercises related to alert investigations over other tool-specific exercises to reduce the required domain-specific knowledge.

Regarding the generalizability of our training to other SOCs, it is likely that other SOCs utilize different technologies, SIEM systems, handle different types of alert data and logs and employ different alert investigation processes. Yet, the fundamental process of alert investigation from an information gathering perspective is similar across SOCs that employ rule-based monitoring. Namely, analysts must investigate a large volume of alerts, which often results in false positives. To discern benign events from attack-related alerts, analysts then inspect the alert and if needed collect information of a plethora of logs and other system to find further evidence. All these elements are included in our training, and thus our results apply beyond our collaborating SOC. However, other SOCs may have different scenarios of interest, which would require different questions to be asked in the cyber range. As aforementioned in Section 6.2, the ability to devise multiple scenarios and allowing SOCs to pick and choose from such scenarios would mitigate this threat.

7 Conclusion

Integrating instructional design principles into cyber range exercises, as we propose with the T1GER LMS design, fosters better training experiences for trainees. Integrating T1GER into an existing cyber range, we showed that trainees that use our augmented LMS design can learn complex threat analysis procedures in a way that is more motivating, less cognitively demanding, and less time-consuming. Reducing reliance on individual trainers, the T1GER approach also improves reproducibility and scalability, making cyber range exercises more practical to use. These findings demonstrate the potential of interdisciplinary research to transform cybersecurity education and pave the way to a stronger, better-prepared cybersecurity workforce.

Acknowledgments

Part of this study is funded by NWO through the INTERSECT project, Grant No. NWA.1162.18.301, the CATRIN project, Grant No. NWA.1215.18.003, and the SeReNity project grant number CS.010.

References

[1] Accenture. 2025. Accenture Security ICS Cyber Range. https://www.accenture.com/us-en/services/security/cyber-resilience. Accessed: August 22, 2025.

[2] ACM Joint Task Force on Cybersecurity Education. 2017. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs*

in Cybersecurity. Technical Report. Association for Computing Machinery (ACM). https://www.acm.org/binaries/cOontent/assets/education/curricula-recommendations/csec2017.pdf

[3] Airbus. 2025. Airbus CyberRange: An advanced simulation solution. https://www.cyber.airbus.com/cyberrange/. Accessed: August 22, 2025.

[4] Bushra A. Alahmadi, Louise Axon, and Ivan Martinovic. 2022. 99% False Positives: A Qualitative Study of SOC Analysts' Perspectives on Security Alarms. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 2783–2800. https://www.usenix.org/conference/usenixsecurity22/presentation/alahmadi

[5] Basil Alothman, Aldanah Alhajraf, Reem Alajmi, Rawan Farraj, Nourah Alshareef, and Murad Khan. 2022. Developing a Cyber Incident Exercises Model to Educate Security Teams. *Electronics* 11 (05 2022), 1575. doi:10.3390/electronics11101575

[6] Mauro Andreolini, Vincenzo Giuseppe Colacino, Michele Colajanni, and Mirco Marchetti. 2020. A Framework for the Evaluation of Trainee Performance in Cyber Range Exercises. *Mobile Networks and Applications* 25, 1 (2020), 236–247. https://doi.org/10.1007/s11036-019-01442-0

[7] Nathan Backman. 2016. Facilitating a Battle Between Hackers: Computer Security Outside of the Classroom. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education* (Memphis, Tennessee, USA) *(SIGCSE '16)*. Association for Computing Machinery, New York, NY, USA, 603–608. doi:10.1145/2839509.2844648

[8] Razvan Beuran, Dat Tang, Cuong Pham, Ken-ichi Chinen, Yasuo Tan, and Yoichi Shinoda. 2018. Integrated framework for hands-on cybersecurity training: CyTrONE. *Computers & Security* 78 (2018), 43–59. doi:10.1016/j.cose.2018.06.001

[9] Sandeep Bhatt, Pratyusa K. Manadhata, and Loai Zomlot. 2014. The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy* 12, 5 (2014), 35–41. doi:10.1109/MSP.2014.103

[10] Chiara Braghin, Stelvio Cimato, Ernesto Damiani, Fulvio Frati, Elvinia Riccobene, and Sadegh Astaneh. 2020. Towards the Monitoring and Evaluation of Trainees' Activities in Cyber Ranges. In *Model-driven Simulation and Training Environments for Cybersecurity*, George Hatzivasilis and Sotiris Ioannidis (Eds.). Springer International Publishing, Cham, 79–91.

[11] Agnė Brilingaitė, Linas Bukauskas, and Eduardas Kutka. 2017. Development of an Educational Platform for Cyber Defence Training. In *Proceedings of the 2017 European Conference on Cyber Warfare and Security*. Academic Conferences International Limited, Academic Conferences Ltd, Dublin, Ireland, 73–81.

[12] Agnė Brilingaitė, Linas Bukauskas, and Aušrius Juozapavičius. 2020. A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security* 88 (2020), 101607. doi:10.1016/j.cose.2019.101607

[13] Pavel Čeleda, Jakub Čegan, Jan Vykopal, and Daniel Tovarňák. 2015. Kypo–a platform for cyber defence exercises.

[14] Allan Collins, John Seely Brown, and Susan E Newman. 1991. *Educational Values and Cognitive Instruction: Implications for Reform*. Routledge, New York, Chapter Cognitive apprenticeship: Teaching the crafts of reading, writing, and mathematics, 453–494.

[15] Michael Collins, Alefiya Hussain, and Stephen Schwab. 2022. Towards an Operations-Aware Experimentation Methodology. In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 384–393. doi:10.1109/EuroSPW55150.2022.00046

[16] Michael Collins, Alefiya Hussain, and Stephen Schwab. 2022. Towards an Operations-Aware Experimentation Methodology. In *Proceedings of the 2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. 384–393. doi:10.1109/EuroSPW55150.2022.00046

[17] Daniel Corral, Shana K Carpenter, and Sam Clingan-Siverly. 2020. The effects of immediate versus delayed feedback on complex concept learning. *Quarterly Journal of Experimental Psychology* 74, 4 (Dec. 2020), 786–799. doi:10.1177/1747021820977739

[18] William Crumpler and James A Lewis. 2019. The cybersecurity workforce gap. Center for Strategic and International Studies (CSIS) Washington, DC, USA.

[19] A. D'Amico and K. Whitley. 2008. *The Real Work of Computer Network Defense Analysts*. Springer Berlin Heidelberg, Berlin, Heidelberg, 19–37. doi:10.1007/978-3-540-78243-8_2

[20] Evangelia Demerouti, Friedhelm Nachreiner, and Wilmar Schaufeli. 2001. The Job Demands–Resources Model of Burnout. *Journal of Applied Psychology* 86 (06 2001), 499–512. doi:10.1037/0021-9010.86.3.499

[21] Håkon Svee Eriksson and Gudmund Grov. 2022. Towards XAI in the SOC – a user centric study of explainable alerts with SHAP and LIME. In *2022 IEEE International Conference on Big Data (Big Data)*. 2595–2600. doi:10.1109/BigData55660.2022.10020248

[22] Bernard Ferguson, Anne Tall, and Denise Olsen. 2014. National Cyber Range Overview. In *Proceedings of the 2014 IEEE Military Communications Conference*. IEEE, Baltimore, 123–128. doi:10.1109/MILCOM.2014.27

[23] Sigma Detection Format. [n. d.]. Sigma Rules. https://sigmahq.io/docs/basics/rules.html. [Online; last accessed Sep, 2025].

[24] Open Information Security Foundation. [n. d.]. Suricata Rules. https://docs.suricata.io/en/latest/rules/index.html. [Online; last accessed Sep, 2025].

[25] Aidan Gilson, Conrad W Safranek, Thomas Huang, Vimig Socrates, Ling Chi, Richard Andrew Taylor, and David Chartash. 2023. How Does ChatGPT Perform on the United States Medical Licensing Examination? The Implications of Large Language Models for Medical Education and Knowledge Assessment. *JMIR Med Educ* 9 (8 Feb 2023). doi:10.2196/45312

[26] Magdalena Glas, Fabian Böhm, Falko Schönteich, and Günther Pernul. 2023. Cyber Range Exercises: Potentials and Open Challenges for Organizations. In *Human Aspects of Information Security and Assurance*, Steven Furnell and Nathan Clarke (Eds.). Springer Nature Switzerland, Cham, 24–35.

[27] Magdalena Glas, Clara Hilmer, and Gunther Pernul. 2025. Cyber Ranges: Five Use Cases for Improving Cybersecurity Skills Development in Organizations. *IEEE Security & Privacy* 23 (2025). Issue 5. doi:10.1109/MSEC.2025.3596735 preprint.

[28] Magdalena Glas, Gerhard Messmann, and Günther Pernul. 2024. Complex yet attainable? An interdisciplinary approach to designing better cyber range exercises. *Computers & Security* 144 (2024), 103965. doi:10.1016/j.cose.2024.103965

[29] Magdalena Glas, Manfred Vielberth, and Guenther Pernul. 2023. Train as You Fight: Evaluating Authentic Cybersecurity Training in Cyber Ranges. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems* (Hamburg, Germany) *(CHI '23)*. Association for Computing Machinery, New York, NY, USA, Article 622, 19 pages. doi:10.1145/3544548.3581046

[30] Eric T. Greenlee, Gregory J. Funke, Joel S. Warm, Ben D. Sawyer, Victor S. Finomore, Vince F. Mancuso, Matthew E. Funke, and Gerald Matthews. 2016. Stress and Workload Profiles of Network Analysis: Not All Tasks Are Created Equal. In *Advances in Human Factors in Cybersecurity*, Denise Nicholson (Ed.). Springer International Publishing, Cham, 153–166.

[31] Francis Hahn, Spencer Cherry, Kumar Shashwat, Laura Buldrini, Daniel Lende, and Xinming Ou. 2025. Tools Make Me Snore: A Next-Gen Framework for Training SOC Analysts Non-Perishable Skills. doi:10.14722/wosoc.2025.23015

[32] George Hatzivasilis, Sotiris Ioannidis, Michail Smyrlis, George Spanoudakis, Fulvio Frati, Chiara Braghin, Ernesto Damiani, Hristo Koshutanski, George Tsakirakis, Torsten Hildebrandt, Ludger Goeke, Sebastian Pape, Oleg Blinder, Michael Vinov, George Leftheriotis, Martin Kunc, Fotis Oikonomou, Giovanni Magilo, Vito Petrarolo, Antonio Chieti, and Robert Bordianu. 2021. The THREAT-ARREST Cyber Range Platform. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. IEEE, Virtual, 422–427. doi:10.1109/CSR51186.2021.9527963

[33] IBM. 2025. IBM Security X-Force Cyber Range. https://www.ibm.com/services/security-operations-center. Accessed: August 22, 2025.

[34] (ISC)². 2024. *(ISC)² Cybersecurity Workforce Study 2024 - Global Cybersecurity Workforce Prepares for an AI-Driven World*. Technical Report. International Information System Security Certification Consortium. 1–49 pages.

[35] Vyron Kampourakis, Vasileios Gkioulos, and Sokratis Katsikas. 2025. A step-by-step definition of a reference architecture for cyber ranges. *Journal of Information Security and Applications* 88 (2025), 103917. doi:10.1016/j.jisa.2024.103917

[36] Stylianos Karagiannis, Emmanouil Magkos, Eleftherios Karavaras, Antonios Karnavas, Maria Nefeli Nikiforos, and Christoforos Ntantogian. 2024. Towards NICE-by-Design Cybersecurity Learning Environments: A Cyber Range for SOC Teams. *Journal of Network and Systems Management* 32, 2 (April 2024), 1–29. doi:10.1007/s10922-024-09816-w

[37] Georgios Kavallieratos, Sokratis K. Katsikas, and Vasileios Gkioulos. 2019. Towards a Cyber-Physical Range. In *Proceedings of the 5th on Cyber-Physical System Security Workshop* (Auckland, New Zealand) *(CPSS '19)*. Association for Computing Machinery, New York, NY, USA, 25–34. doi:10.1145/3327961.3329532

[38] John M Keller. 1987. Development and use of the ARCS model of instructional design. *Journal of instructional development* 10, 3 (1987), 2–10.

[39] Leon Kersten, Kim Beelen, Emmanuele Zambon, Chris Snijders, and Luca Allodi. 2025. A Field Study to Uncover and a Tool to Support the Alert Investigation Process of Tier-1 Analysts. In *Symposium on Usable Security and Privacy (USEC) 2025*. doi:10.14722/usec.2025.23034

[40] Leon Kersten, Santiago Darré, Tom Mulders, Emmanuele Zambon, Marco Caselli, Chris Snijders, and Luca Allodi. 2024. A Security Alert Investigation Tool Supporting Tier 1 Analysts in Contextualizing and Understanding Network Security Events. In *2024 Annual Computer Security Applications Conference (ACSAC)*. 890–905. doi:10.1109/ACSAC63791.2024.00076

[41] Leon Kersten, Tom Mulders, Emmanuele Zambon, Chris Snijders, and Luca Allodi. 2023. Give Me Structure: Synthesis and Evaluation of a (Network) Threat Analysis Process Supporting Tier 1 Investigations in a Security Operation Center. In *Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023)*. USENIX Association, Anaheim, CA, 97–111.

[42] Jason Kick. 2014. *Cyber Exercise Playbook*. Technical Report. MITRE Corporation. https://apps.dtic.mil/sti/citations/ADA624910

[43] Melina Klepsch, Florian Schmitz, and Tina Seufert. 2017. Development and Validation of Two Instruments Measuring Intrinsic, Extraneous, and Germane Cognitive Load. *Frontiers in Psychology* 8 (Nov. 2017), 1–18. doi:10.3389/fpsyg.2017.01997

[44] Benjamin J. Knox, Ricardo G. Lugo, and Stefan Sütterlin. 2019. Cognisance as a Human Factor in Military Cyber Defence Education. *IFAC-PapersOnLine* 52, 19 (2019), 163–168. doi:10.1016/j.ifacol.2019.12.168 14th IFAC Symposium on Analysis, Design, and Evaluation of Human Machine Systems HMS 2019.

[45] Faris Bugra Kokulu, Ananta Soneji, Tiffany Bao, Yan Shoshitaishvili, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. 2019. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 1955–1970. doi:10.1145/3319535.3354239

[46] Janet L. Kolodner, Paul J. Camp, David Crismond, Barbara Fasse, Jackie Gray, Jennifer Holbrook, Sadhana Puntambekar, and Mike Ryan. 2003. Problem-Based Learning Meets Case-Based Reasoning in the Middle-School Science Classroom: Putting Learning by Design Into Practice. *Journal of the Learning Sciences* 12, 4 (2003), 495–547. doi:10.1207/s15327809jls1204_2

[47] Rune Johan Krumsvik. 2024. Artificial intelligence in nurse education – a new sparring partner? *Nordic Journal of Digital Literacy* 19, 3 (2024), 172–186. doi:10.18261/njdl.19.3.5

[48] Rune Johan Krumsvik. 2025. Chatbots and academic writing for doctoral students. *Education and Information Technologies* 30, 7 (2025), 9427 – 9461. doi:10.1007/s10639-024-13177-x

[49] Maria Leitner, Florian Skopik, and Timea Pahi. 2024. Operational cyber incident coordination revisited: providing cyber situational awareness across organizations and countries. *Information Security Journal: A Global Perspective* 33, 5 (2024), 486–507. arXiv:https://doi.org/10.1080/19393555.2024.2334787 doi:10.1080/19393555.2024.2334787

[50] Sandra Lielbārde, Agnė Brilingaitė, Linas Bukauskas, Evita Roponena, Elizabete Citskovska, and Rūta Pirta. 2025. *Maritime Cyber Resilience: Bridging Cybersecurity and Regulatory Frameworks*. Springer Nature Switzerland, Cham, 217–228. doi:10.1007/978-3-031-94855-8_14

[51] Derek Lin. 2022. MATE: Summarizing Alerts to Interpretable Outcomes with MITRE ATT&CK. In *2022 IEEE International Conference on Big Data (Big Data)*. 4295–4302. doi:10.1109/BigData55660.2022.10020587

[52] Nicole Loorbach, Oscar Peters, Joyce Karreman, and Michaël Steehouder. 2014. Validation of the Instructional Materials Motivation Survey (IMMS) in a self-directed instructional setting aimed at working with technology. *British Journal of Educational Technology* 46, 1 (Feb. 2014), 204–218. doi:10.1111/bjet.12138

[53] Kaie Maennel, Agnė Brilingaitė, Linas Bukauskas, Aušrius Juozapavičius, Benjamin James Knox, Ricardo Gregorio Lugo, Olaf Maennel, Ginta Majore, and Stefan Sütterlin. 2023. A Multidimensional Cyber Defense Exercise: Emphasis on Emotional, Social, and Cognitive Aspects. *SAGE Open* 13, 1 (2023), 215824402311563. doi:10.1177/21582440231156367

[54] Jelena Mirkovic and Peter A. H. Peterson. 2014. Class Capture-the-Flag Exercises. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*. USENIX Association, San Diego, CA. https://www.usenix.org/conference/3gse14/summit-program/presentation/mirkovic

[55] Azqa Nadeem, Sicco Verwer, and Shanchieh Jay Yang. 2021. SAGE: Intrusion Alert-driven Attack Graph Extractor . In *2021 IEEE Symposium on Visualization for Cyber Security (VizSec)*. IEEE Computer Society, Los Alamitos, CA, USA, 36–41. doi:10.1109/VizSec53666.2021.00009

[56] National Initiative for Cybersecurity Education (NICE). 2020. *The Cyber Range: A Guide*. Technical Report. National Initiative for Cybersecurity Education (NICE).

[57] National Initiative for Cybersecurity Education (NICE). 2024. *The Cyber Range: A Guide - Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification, and Training*. Technical Report. National Institute for Standardization and Technology (NIST). Cyber Range Project Team, Cyber Range Project Team and the NICE Community Coordinating Council, Cybersecurity Skills Competitions Community of Interest.

[58] Rodney Petersen, Danielle Santos, Matthew C. Smith, Karen A. Wetzel, and Greg Witte. 2020. *Workforce Framework for Cybersecurity (NICE Framework)*. Technical Report. National Institute of Standards and Technology. doi:10.6028/nist.sp.800-181r1

[59] R Core Team. 2025. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, Vienna, Austria. https://www.R-project.org/

[60] Adriana Radu, Leon Kersten, Rik Wosyka, Tom Mulders, Emmanuele Zambon, and Luca Allodi. 2025. A Test Tool to Evaluate the Skill Sets of Tier-1 Security Analysts in a SOC Environment: A Case Study from Recruitment to Operations. doi:10.14722/wosoc.2025.23001

[61] Richard M. Ryan and Edward L. Deci. 2000. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist* 55, 1 (2000), 68–78. doi:10.1037/0003-066x.55.1.68

[62] Reza Sadoddin and Ali Ghorbani. 2006. Alert Correlation Survey: Framework and Techniques *(PST '06)*. Association for Computing Machinery, New York, NY, USA, Article 37, 10 pages. doi:10.1145/1501434.1501479

[63] Security Onion Solutions. [n. d.]. Security Onion 2. https://securityonionsolutions.com/software. [Online; last accessed Sep, 2025].

[64] Rand Spiro, Richard Coulson, Paul Feltovich, and Daniel Anderson. 1994. Cognitive Flexibility Theory: Advanced Knowledge Acquisition in Ill-Structured Domains. In *Theoretical Models and Processes of Reading* (fourth ed.), Harry Singer and Robert B. Ruddell (Eds.). International Reading Association, Newark, NJ, 544–557. doi:10.1598/0710.22

[65] Sathya Chandran Sundaramurthy, Alexandru G. Bardas, Jacob Case, Xinming Ou, Michael Wesch, John McHugh, and S. Raj Rajagopalan. 2015. A Human Capital Model for Mitigating Security Analyst Burnout. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)*. USENIX Association, Ottawa, 347–359. https://www.usenix.org/conference/soups2015/proceedings/presentation/sundaramurthy

[66] Sathya Chandran Sundaramurthy, Jacob Case, Tony Truong, Loai Zomlot, and Marcel Hoffmann. 2014. A Tale of Three Security Operation Centers. In *Proceedings of the ACM Conference on Computer and Communications Security*. doi:10.1145/2663887.2663904

[67] Sathya Chandran Sundaramurthy, John McHugh, Xinming Ou, Michael Wesch, Alexandru G. Bardas, and S. Raj Rajagopalan. 2016. Turning Contradictions into Innovations or: How We Learned to Stop Whining and Improve Security Operations. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association, Denver, CO, 237–251.

[68] Anikó Szarvák and Valéria Póser. 2021. Review of using Open Source Software for SOC for education purposes – a case study. In *2021 IEEE 25th International Conference on Intelligent Engineering Systems (INES)*. 000209–000214. doi:10.1109/INES52918.2021.9512928

[69] Terence C. C. Tan, Anthonie B. Ruighaver, and Atif Ahmad. 2010. Information Security Governance: When Compliance Becomes More Important than Security. In *Security and Privacy – Silver Linings in the Cloud*, Kai Rannenberg, Vijay Varadharajan, and Christian Weber (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 55–67.

[70] Shahroz Tariq, Mohan Baruwal Chhetri, Surya Nepal, and Cecile Paris. 2025. Alert Fatigue in Security Operations Centres: Research Challenges and Opportunities. *ACM Comput. Surv.* 57, 9, Article 224 (April 2025), 38 pages. doi:10.1145/3723158

[71] Manfred Vielberth, Fabian Böhm, Ines Fichtinger, and Günther Pernul. 2020. Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access* 8 (2020), 227756–227779. doi:10.1109/ACCESS.2020.3045514

[72] Manfred Vielberth, Magdalena Glas, Marietheres Dietz, Stylianos Karagiannis, Emmanouil Magkos, and Günther Pernul. 2021. A Digital Twin-Based Cyber Range for SOC Analysts. In *Data and Applications Security and Privacy XXXV*, Ken Barker and Kambiz Ghazinour (Eds.). Springer International Publishing, Cham, 293–311.

[73] Manfred Vielberth and Günther Pernul. 2018. A Security Information and Event Management Pattern. In *Proceedings of the 12th Latin American Conference on PatternLanguages of Programs (SugarLoafPLoP 2018),*. doi:10.5283/EPUB.41139

[74] Valdemar Švábenský, Jan Vykopal, Milan Cermak, and Martin Laštovička. 2018. Enhancing Cybersecurity Skills by Creating Serious Games. In *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education* (Larnaca, Cyprus) *(ITiCSE 2018)*. Association for Computing Machinery, New York, NY, USA, 194–199. doi:10.1145/3197091.3197123

[75] Valdemar Švábenský, Richard Weiss, Jack Cook, Jan Vykopal, Pavel Čeleda, Jens Mache, Radoslav Chudovský, and Ankur Chattopadhyay. 2022. Evaluating Two Approaches to Assessing Student Progress in Cybersecurity Exercises. In *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 1*. Association for Computing Machinery, New York, NY, USA, 787–793. doi:10.1145/3478431.3499414

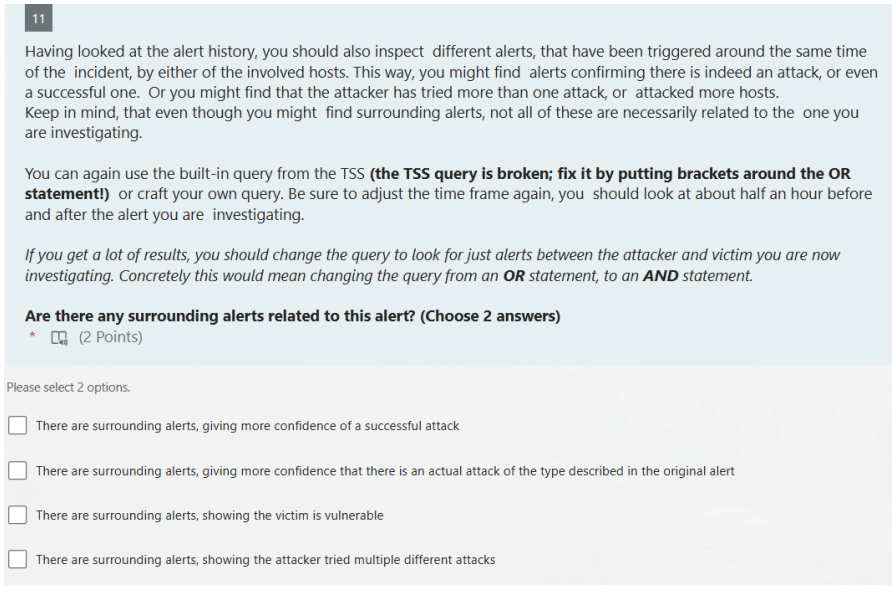
[76] Jan Vykopal, Radek Ošlejšek, Karolína Burská, and Kristína Zákopčanová. 2018. Timely Feedback in Unstructured Cybersecurity Exercises. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*. Association for Computing Machinery, New York, NY, USA, 173–178. doi:10.1145/3159450.3159561

[77] Richard Weiss, Frankly Turbak, Jens Mache, Erik Nilsen, and Michael E. Locasto. 2016. Finding the Balance Between Guidance and Independence in Cybersecurity Exercises. In *Proceedings of the 2016 USENIX Workshop on Advances in Security Education (ASE 16)*. USENIX Association, Austin, TX, 1–8. https://www.usenix.org/conference/ase16/workshop-program/presentation/weiss

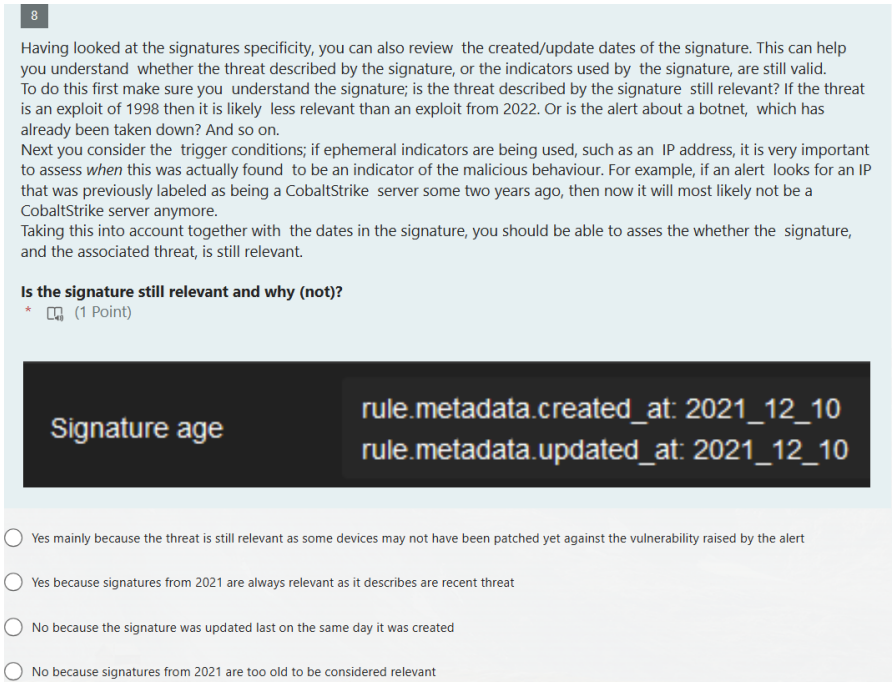
[78] Muhammad Mudassar Yamin and Basel Katt. 2022. Modeling and executing cyber security exercise scenarios in cyber ranges. *Computers & Security* 116 (2022), 102635. doi:10.1016/j.cose.2022.102635

[79] Chen Zhong, John Yen, Peng Liu, Rob F. Erbacher, Christopher Garneau, and Bo Chen. 2017. *Studying Analysts' Data Triage Operations in Cyber Defense Situational Analysis*. Springer International Publishing, Cham, 128–169. doi:10.1007/978-3-319-61152-5_6

A Examples of Tasks in the Existing LMS



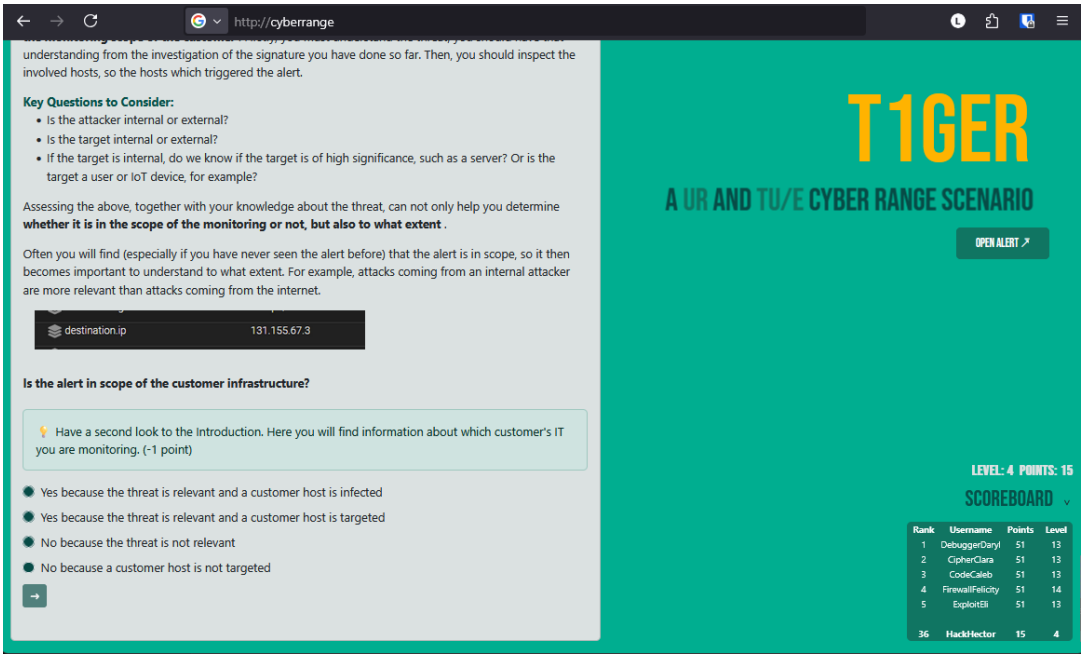
(a) A question regarding other alerts surrounding the investigated alert. The trainee is guided in how to find the surrounding alerts, and then is asked to select two correct statements.



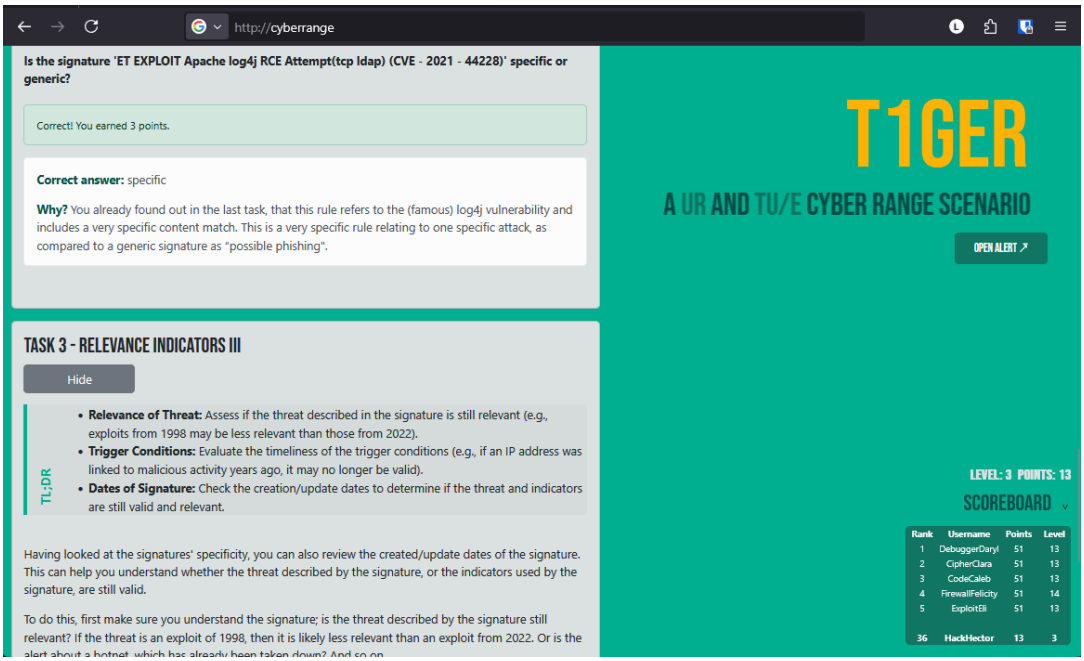
(b) A question regarding the relevancy of a triggered alert. The LMS explains how to interpret information regarding the creation and update dates of alert rules via examples and asks the trainee to apply the knowledge.

Figure 5: Examples of two questions asked in the existing LMS.

B User Interface of T1GER Implementation



(a) Procedural information support through hint. When activated, the hint appears in a highlighted box above the four response choices.



(b) Feedback statement and explanation. After response submission, the correct answer is displayed with an explanation and context what this means for the overall analysis.

Figure 6: User interface of the web application implementing T1GER.

C Man–Whitney U Test

Table 4: Mann–Whitney U Test results by group with Holm-adjusted p-values

	Motivation	*Cogn*	*TAP*	*SIEM*	*Scenario*	*General*	*TT*
U	3360.0*	3382.5**	2511.5	2576.5	2548.0	2145.0	745.0***
r	.26	.27	.02	<.01	.01	.15	.33

Note. * $p < .05$, ** $p < .01$, *** $p < .001$. Motivation: *learning motivation*, Cogn: *cognitive load*, TAP: *TAP knowledge*, SIEM: *SIEM knowledge*, Scenario: *scenario-specific knowledge*, General: *general alert investigation knowledge*, TT: *total completion time.*

D Correlation Analysis (full cohort)

Table 5: Correlation matrix (upper triangle only).

	Dependent var.							Background var.			
	COGN	*TAP*	*SIEM*	*Scenario*	*General*	*Compl.*	*TT*	*Edu(M)*	*Gen(f)*	*Eng(high)*	*SOC(yes)*
Motivation	.78 ***	.09	.23 **	.15	.00	.18 *	-.06	.34 ***	-.12	.24 **	0.21*
COGN	-	.13	.28 ***	.13	-.01	.19 *	.01	.36 ***	-.15	.24 **	0.20*
TAP	-	-	.17 *	.23 **	.23 **	.01	.11	.18 *	.05	.19 *	0.11
SIEM	-	-	-	.14	.16	.02	.18	.27 ***	-.14	.26 **	0.22**
Scenario	-	-	-	-	.25 **	.02	.00	.28 ***	-.18 *	.24 **	0.18*
General	-	-	-	-	-	-.08	.19	.11	.02	.07	0.11
Comp	-	-	-	-	-	-	-	.03	-.14	.02	0.11
TT	-	-	-	-	-	-	-	.23 *	.01	.02	0.07
Edu (M)	-	-	-	-	-	-	-	-	-.21 *	.40 ***	-0.03
Gen(f)	-	-	-	-	-	-	-	-	-	-.24 **	-0.06
Eng(high)	-	-	-	-	-	-	-	-	-	-	0.17*

Note. * $p < .05$, ** $p < .01$, *** $p < .001$. Motivation: *learning motivation*, Cogn: *cognitive load*, TAP: *TAP knowledge*, SIEM: *SIEM knowledge*, Scenario: *scenario-specific knowledge*, General: *general alert investigation knowledge*, TT: *total completion time*, Comp: *training completion*, Eng (high): English proficiency dummy variable coded 1 = very high (C2), 0 = intermediate (B1, B2, C1). Edu (M): Educational level dummy variable coded 1 = Master's degree, 0 = Bachelor's degree. Gen (f): Gender dummy variable coded 1 = female, 0 = all other categories. SOC (yes): SOC experience variable coded 1 = SOC experience, 0 = no SOC experience.

E Correlation Analysis (redesign group)

Table 6: Correlation matrix (upper triangle only).

	Dependent var.								Background var.			
	Motiv.	*COGN*	*TAP*	*SIEM*	*Scenario*	*General*	*Compl.*	*TT*	*Edu(M)*	*Gen(f)*	*Eng(high)*	*SOC(yes)*
Hints	-.19	-.07	-.12	-.11	-.36 **	-.28 *	-.12	-.03	-.32 **	.11	-.28 *	-.10
Motivation	-	.76 ***	.15	.25 *	.19	.15	.08	.04	.29 **	.03	.14	.19
COGN	-	-	.16	.27 *	.08	.06	.05	.15	.27 *	-.15	.11	.16
TAP	-	-	-	.27 *	.28 *	.23 *	.01	.18	.36 **	.05	.23 *	.02
SIEM	-	-	-	-	.19	.21	.08	.23	.30 **	-.14	.18	.21
Scenario	-	-	-	-	-	.21	.03	-.11	.29 *	-.18 *	.23 *	.15
General	-	-	-	-	-	-	-.06	.07	.25 *	.09	.12	.09
Comp	-	-	-	-	-	-	-	-	-.08	.05	-.09	.00
TT	-	-	-	-	-	-	-	-	.32 **	-.14	.13	-.08
Edu (M)	-	-	-	-	-	-	-	-	-	-.15	.56 ***	.15
Gen(f)	-	-	-	-	-	-	-	-	-	-	-.17	-.03
Eng(high)	-	-	-	-	-	-	-	-	-	-	-	.08

Note. * $p < .05$, ** $p < .01$, *** $p < .001$. Motivation: *learning motivation*, Cogn: *cognitive load*, TAP: *TAP knowledge*, SIEM: *SIEM knowledge*, Scenario: *scenario-specific knowledge*, General: *general alert investigation knowledge*, TT: *total completion time*, Comp: *training completion.* Eng (high): English proficiency dummy coded 1 = very high (C2), 0 = B1–C1. Edu (M): educational level dummy coded 1 = Master's degree, 0 = Bachelor's degree. Gen (f): gender dummy coded 1 = female, 0 = all others. SOC (yes): prior SOC/SIEM experience coded 1 = yes. Hints: number of in-system hints used.

F Regression Analysis (redesign group)

Table 7: Regression results for dependent variables related to *learning experience* and *learning outcomes* within the cyber range group, controlling for *education level*, *English proficiency*, *gender*, and *SOC experience*.

	Learning experience		Learning outcomes					
Predictor	*Motivation*	*Cogn*	*TAP*	*SIEM*	*Scenario*	*General*	*TT (min)*[a]	*Comp*[b]
Hints	-.04	.02	-.00	.00	-.04*	-.04*	.55	-.21
SE	.04	.05	.02	.02	.02	.02	.75	.17
Educational level (Master)	.40.	.49*	.22*	.14.	.09	.12	9.00**	-.58
SE	.20	.24	.09	.07	.08	.08	3.32	.96
English proficiency (high)	-.09	-.12	.03	-.00	.03	-.03	-1.77	-.55
SE	.19	.23	.08	.07	.08	.08	3.19	.84
SOC experience (yes)	.36	.35	-.03	.15	.11	.04	-4.47	.03
SE	.28	.32	.12	.10	.11	.11	4.33	1.17
Gender (f)	-.04	-.21	.07	-.07	-.07	.08	.36	-.63
SE	.17	.20	.07	.06	.07	.07	2.72	.70
R^2_{adj}	.06	.04	.08	.07	.13	.07	.06	–
F (5,71)	1.95	1.63	2.37*	2.16.	3.24**	2.14.	1.83	–

Note. * $p < .05$, ** $p < .01$, *** $p < .001$. Cogn = *cognitive load*. TAP = *threat analysis process knowledge*. Scenario = *scenario-specific knowledge*. General = *general alert investigation knowledge*. TT = *total completion time* in minutes. Comp = *training completion*. English proficiency (high): 1 = C2, 0 = intermediate (B1–C1). Educational level (Master): 1 = Master's, 0 = Bachelor's. Gender (f): 1 = woman, 0 = all other categories. SOC experience (yes): 1 = experience, 0 = no experience.
[a] $F(5, 60)$ due to missing data.
[b] Logistic regression; coefficients are log-odds. Odds ratio for group = 0.81. No F-test or R^2_{adj} reported.

G Posttest Questionnaire

(1) **Demographics and Background**
- Gender: *Man, Woman, Non-binary, Prefer not to say*
- Which university do you attend? *TU/e, UR*
- Current level of study: *BSc, MSc*
- English proficiency level: *Intermediate (B1), Upper-intermediate (B2), Advanced (C1), Proficient (C2)*
- Do you have previous experience with navigating SIEM interfaces or investigating alerts?
  - *Yes, more than one year in a SOC*
  - *Yes, less than one year in a SOC (e.g., internship)*
  - *Yes, in educational/private settings*
  - *No*
- Did you manage to finish the training? *Yes, No*
- Would you escalate the alert you analyzed in your training to a Tier 2 analyst? *Yes, No*

(2) **TAP knowledge**
- Remember the threat analysis process (TAP). List the stages in the order you should consider them when investigating an alert.
  - *Relevance Indicators*
  - *Contextual Information*
  - *Additional Alerts*
  - *Attack Evidence*
- Which observation is part of attack evidence?
  - *40 connection logs are associated to the external IP*
  - *10 packets exchanged*
  - *Multiple high-profile alerts*
  - *IP found malicious established a connection*
- Which observation is not related to relevance indicators?
  - *Triggered alert involves IP 131.155.0.146*
  - *Rule last updated on 2022-08-30*
  - *Signature is very specific*
  - *Rule created on 2020-04-12*
  - *40 connection logs associated to IP*

(3) **SIEM knowledge**
- Which button do you press to fetch logs corresponding to an alert? (screenshot included)
  - *Correlate*
  - *Include*
  - *CyberChef*

  - *Hunt*
- What does the highlighted field correspond to? (screenshot included)
  - *Description of the alert*
  - *Raw network traffic*
  - *The signature that triggered the alert*
  - *The victim's IP address*
- What do you do to view all logs for a specific IP address?
  - *Click on alert name → actions → hunt*
  - *Click on IP → actions → hunt*
  - *Click on alert name → exclude*
  - *Click on IP → exclude*

(4) **Scenario-specific knowledge**
- A log4j remote code execution (RCE) attack is successful when...
  - *A malicious attacker establishes a connection*
  - *SIEM raises an alert*
  - *Related logs contain lots of traffic*
  - *A victim connects to a host with the malicious payload*
- Alert: ET EXPLOIT Apache log4j RCE Attempt (http ldap) (CVE-2021-44228) — identify the most likely true statement. (screenshot included)
  - *Attacker attempted two log4j attacks to different victims*
  - *Attacker attempted two attacks to the same victim*
  - *Two alerts triggered correctly*
  - *Only one alert triggered correctly*
- Investigate with OSINT tools: which domain is associated with IP 51.254.164.52, and is it malicious?
  - *abuse@ovh.net, not malicious*
  - *ip52.ip-51-254-164.eu, malicious*
  - *ip52.ip-51-254-164.eu, not malicious*
  - *abuse@ovh.net, malicious*
- Is this signature generic or specific, and why? (screenshot included)
  - *Generic – applies to all traffic via TFTP (port 69)*
  - *Generic – rule length very short*
  - *Specific – searches for a string in packets*
  - *Specific – specifies a port*

(5) **General alert investigation knowledge**
- Select the correct statement regarding connection logs (conn logs).
  - *Sometimes you can observe the payload*
  - *Relate to transport layer*
  - *Protocol-specific*
  - *Always relevant to an investigation*
- When should you escalate an alert (classify as interesting)?
  - *When not a false positive*
  - *When a successful attack has impact*
  - *When severity is at least high*
  - *When an attack could impact the monitored customer*

(6) **Cognitive Load** ***(5-point Likert scale, 1: totally disagree - 5: totally agree)***
- During this training, it was easy (non-exhausting) to find the important information.
- The design of the training was convenient for learning.
- During the training, it was easy to recognize and link the crucial information.

(7) **Learning motivation** ***(5-point Likert scale, 1: totally disagree - 5: totally agree)***
- The way the training was delivered helped me maintain attention.
- The presentation of the information helped me stay focused.
- The variety of reading passages, exercises, and illustrations helped me concentrate.
- It is clear how the training content relates to what I already know.
- The content and writing style convey the value of learning secure coding.
- The task content will be useful to me.
- As I worked through the instructions, I felt confident in analyzing alerts.
- After some time, I was confident I could complete the tasks.
- The good organization of the content helped me feel confident in learning to analyze alerts.
- Attention check: Tick the second option from the right ("Agree").
- I enjoyed solving these tasks so much that I was motivated to keep working.
- I really enjoyed solving these tasks.
- I liked how the tasks were presented and designed.