A Digital Twin-Based Cyber Range for SOC Analysts

Manfred Vielberth, Magdalena Glas, Marietheres Dietz, Stylianos Karagiannis, Emmanouil Magkos, Günther Pernul

A Digital Twin-based Cyber Range for SOC Analysts

Manfred Vielberth[1][0000−0002−1119−4715], Magdalena Glas[1][0000−0003−0239−7526], Marietheres Dietz[1][0000−0002−6885−4622], Stylianos Karagiannis[2][0000−0001−9571−4417], Emmanouil Magkos[2][0000−0002−5922−4274], and Günther Pernul[1][0000−0003−1338−9003]

[1] Chair of Information Systems, University of Regensburg, Regensburg, Germany
{first.author}@ur.de
[2] Department of Informatics, Ionian University, Corfu, Greece
{skaragiannis,emagos}@ionio.gr

Abstract. Security Operations Centers (SOCs) provide a holistic view of a company's security operations. While aiming to harness this potential, companies are lacking sufficiently skilled cybersecurity analysts. One approach to meet this demand is to create a cyber range to equip potential analysts with the skills required. The digital twin paradigm offers great benefit by providing a realistic virtual environment to create a cyber range. However, to the best of our knowledge, tapping this potential to train SOC analysts has not been attempted yet. To address this research gap, a concept of a digital twin-based cyber range for SOC analysts is proposed and implemented. As part of the virtual training environment, several attacks against an industrial system are simulated. Being provided with a SIEM system that displays the real-time log data, the trainees solve increasingly complex tasks in which they have to detect the attacks performed against the system. Thereby, they learn how to interact with a SIEM system and create rules that correlate events aiming to detect security incidents. To evaluate the implemented cyber range, a comprehensive user study demonstrates a significant increase of knowledge within SIEM-related topics among the participants. Additionally, it indicates that the cyber range was subjectively perceived as a positive learning experience by the participants.

Keywords: Cyber Range · Security Operations Center · Digital Twin

1 Introduction

As cyber-attacks become increasingly sophisticated and use more and more points of attack, it is essential to establish a holistic view of organizations' security. As a recently published report [2] indicates, organizations are becoming better at detecting and mitigating direct attacks. However, more advanced attacks are on the rise, targeting the victim indirectly through weak spots in the business ecosystem or the supply chain. Over the recent years, Security Operations Centers (SOCs) have emerged to address this problem by providing

a holistic view of organizations' cybersecurity. However, this has increased the demand for security personnel, making it difficult to find enough well-trained analysts for SOCs. This is worsened by the so-called "alert burnout", since an analyst's daily work can be quite tedious and tiring. According to a SANS survey [23], the key to low attrition rates is to invest more in analysts' training. Therefore, it is crucial to create a means to train analysts as quickly and effectively as possible, considering that the requirements can vary from company to company. To create a suitable training environment, cyber ranges can be used to train analysts by simulating realistic scenarios without disrupting business operations. To be as close as possible to the specifics of the company, the integration of a digital twin is a promising option. Thereby, the relevant section of the company infrastructure for which the experts are to be trained can be mirrored, creating a training environment that barely differs from the company's real environment.

The contribution of this paper is twofold. First, we examine which components of a digital twin can be used for cyber ranges. Based on this, a cyber range for SOC analysts is designed and prototypically implemented. To show that the proposed concept offers advantages for the training of security analysts, it is evaluated through an extensive empirical user study.

The remainder of this paper is structured as follows. Section 2 provides the foundation of the conducted research. In Section 3, the digital twin's potential for cyber ranges is outlined along with the current research gap. Based on that, Section 4 proposes a concept for a digital twin-based cyber range, including a scenario and learning concept and concludes with a description of the prototypical implementation of the concept. Section 5 covers the evaluation of the concept in the form of a comprehensive user study by presenting the methodology and the results of the evaluation. Finally, the work is concluded in Section 6.

2 Background and Related Work

2.1 Cyber Range

As conventional training methods that only focus on transferring theoretical knowledge do not meet the demand for practical knowledge and skills within the cybersecurity domain, cyber ranges have gained attention over the past years [32]. Generally, cyber ranges are virtual environments, which are used for cybersecurity training [28]. As the name indicates, the expression is derived from shooting range, as both provide an environment in which people can be trained without harming or interfering with the environment for which they are educated. Application areas range from public settings such as military defense and intelligence, academic and educational, to commercial purposes driven by the industry [29].

The idea of using cyber ranges to train specialists in attack detection and in cybersecurity in general is not entirely new. For example, the Austrian Institute of Technology recently introduced a cyber range of industrial control systems [20], not only targeting education, but also serving as a platform for

conducting research and development by testing new approaches and methods. This is only one example in this context. For a deeper insight into related approaches, we would like to refer to two extensive literature reviews which provide a good overview of preliminary work [32, 29]. Although some works in this area exist, to the best of our knowledge, no approach combines the digital twin's potential with the concept of cyber ranges for educating SOC analysts to date. Additionally, the effect of the approaches on the obtained knowledge has not gained sufficient attention in previous works.

According to Yamin et al. [32], a cyber range can be described by following a taxonomy with six domains. However, the description of a cyber range does not necessarily have to consider all domains, but instead, can focus on selected ones. As this paper applies the taxonomy for describing the developed cyber range, the six domains are elaborated briefly in the following:

Scenario: A scenario defines the storyline and context of a training exercise performed in a cyber range. It supports the purpose of the training, such as education, experimenting, or testing. Thereby, it is allocated to a domain (e.g., networking, critical infrastructure, or IoT). Additionally, a scenario can either be static or dynamic. A dynamic scenario means that changes are made during the exercise, for example, by simulating infrastructure components.

Environment: The environment presents the topology in which the scenario is executed. This includes the underlying technology used to build a system model (simulation, emulation, hardware, or hybrid).

Teaming: Teaming describes which teams are part of the scenario. The most important teams are a red team with the goal to exploit vulnerabilities of the system, and a blue team with the task to defend the system against attacks. Teams can also be autonomous if specific technologies automate them.

Learning: The learning domain covers explanatory elements of a scenario such as texts, images, or video clips used for initial knowledge transfer.

Monitoring: Participants' actions can be monitored in real-time during an exercise by using appropriate tools.

Management: This domain covers how management tasks, such as role and resource allocation, are performed. It also comprises interfaces for controlling the scenario or the environment during the exercise.

Furthermore, it is worth mentioning in this context that the term can be narrowed down further. Kavallieratos et al. [17] define a cyber-physical range as a testbed that enables the testing of the security posture of cyber-physical systems. The cyber range presented in this paper can be assigned to this class.

2.2 Security Operations Center (SOC)

The term Security Operations Center has been around in research for more than a decade. However, attention has significantly increased in the last three to five years as SOCs have emerged as a central pivotal point for security operations in practice [30]. The SOC represents an organizational aspect of an enterprise's

security strategy. It combines processes, technologies, and people [21, 27] to manage and enhance an organization's overall security posture. This goal can usually not be accomplished by a single entity or system, but rather by a complex structure. It creates situational awareness, mitigates the exposed risks, and helps to fulfill regulatory requirements [19]. Additionally, a SOC provides governance and compliance as a framework in which people operate and to which processes and technologies are tailored. A central role within a SOC is taken by security analysts. Using appropriate tools, they can attempt to detect security incidents, then analyze them and react appropriately. Therefore, the success of a SOC depends to a large extent on the skills and training of the analysts. Within a SOC, a SIEM system is usually used as the central tool [31]. A SIEM aims to collect security-relevant data (usually log data) in a central location and analyze it in a correlated manner to detect security incidents. For this purpose, SIEM systems use detection rules that are usually created by analysts, in most cases in JSON or XML format. These fulfill the purpose of triggering an alert if defined conditions within the log data apply.

2.3 Digital Twin

The digital twin refers to a concept that differs in meaning depending on its application area [22]. In general, a digital twin can be defined as a virtual representation of any real-world asset (e.g., system or process). The digital twin accompanies its real-world asset's lifecycle, which may range from phases like idea/planning over operation to decommissioning [6]. The digital twin gathers data about its real-world twin during these phases and enriches the data with semantics [3]. This way, the twin is able to represent its counterpart in-depth and provides a solid basis for simulations and further analytical measures.

Especially in cybersecurity, the digital twin holds several benefits [26]. It can support lifecycle security [11], including the security-by-design paradigm by offering simulations and system testing, in which the security level of the asset can be assessed. Moreover, digital forensics may profit from the vast data and documentary capabilities of a digital twin [7].

3 Investigating the Potential of the Digital Twin for building Cyber Ranges

In order to extract what digital twins offer for cyber ranges, we must first regard the foundation of digital twin deployment in cybersecurity. According to [11], the digital twin is required to provide sufficient fidelity for security measures that rely on its data. A digital twin offering this characteristic can then be successfully implemented for cybersecurity. This definition presents the prerequisite for combining digital twins and cyber ranges. Currently, one work conceptually proposes to utilize a digital twin as a cyber range [4]. However, an implementation has not been realized to date. In their approach, the digital twin is merely

applied as cyber range with the purpose of security training, while other purposes are not considered. However, the digital twin originally serves completely different purposes, such as monitoring and controlling its counterparts' operation[6]. Thus, in this paper, we propose to use the digital twin as a valuable input to create a cyber range rather than turning it into one. In this matter, we investigate which digital twin characteristics can provide valuable input for cyber ranges in the following. The core parts included in a digital twin represent (a) *data, enhanced with semantic technologies*, (b) *analysis, simulation and other intelligent services* as well as (c) *access control and interfaces* [6].

Data of the digital twin's real-world counterpart is produced along its lifecycle, stored in the digital twin and given context by adding *semantics* [3]. This data supports high-fidelity modeling of the counterpart to virtually represent the real-world system. Added semantics offer better comprehension and modeling of the connection and the context of the system's components. This can prove to be an essential input for creating cyber ranges as well. To maximize the training potential of cyber ranges, the virtually represented system and related security incidents should resemble reality as close as possible. This way, security analysts can be trained in a highly realistic environment. However, not all data held in a digital twin may be relevant for building cyber ranges. The virtual system, used to build a cyber range might represent only a part of a complex real-world system, e.g., by focusing on the network level. In this case, the physics-related data of the system might not be of interest. Moreover, the resulting data of digital twin analyses (like predictive maintenance) typically are not relevant. In general, only a subset of digital twin data is required for creating the cyber range – depending on the complexity level, granularity, and the part of the system being represented.

Analysis, simulation, and other intelligent services represent operation modes of a digital twin. According to [7], three modes can be used for security purposes as well: analysis, simulation, and replication. Table 1 summarizes these modes and their potential benefits for building cyber ranges. Each operation mode re-

Table 1. Digital twin security operation modes and their potential for cyber ranges.

Operation mode	Required data	Related work	Benefit	Effort
Analysis	historical/state data	[24]	low	moderate
Simulation	specification data (for emulation)	[10, 8]	high	moderate
Replication	specification data (for emulation), historical/state data (stimuli)	[9, 13]	moderate	high

lies on digital twin data and has already been tackled in terms of security in some works (see Table 1). **Analysis** usually takes historical/state data of the physical counterpart into account to apply analytical measures such as anomaly

detection, pattern recognition, etc. For cyber ranges, this data has to be virtually reproduced (moderate effort). However, there is no virtual system that can be explored by security analysts (low benefit). **Simulation**, in contrast, requires only specification data to build the emulation. On top of the emulation, different (security) scenarios can be applied to a virtual system to create a simulation, where the security analyst in training can not only see produced data of the virtual system but also interact with the system (high benefit). Moreover, the simulations can be taken from digital twins and directly used in or tailored to the cyber range (moderate effort). **Replication**, on the other hand, requires high effort to be used for cyber ranges as it relies on integrating not only specification data to build the emulation, but also on current state data of the physical counterpart to defer the stimuli changing the systems state. However, it only provides moderate benefit as the system is always in synchronization with its real-world counterpart and alternative scenarios (e.g., security incidents and countermeasures) cannot be tested.

Other important parts of digital twins are *access control and interfaces* (e.g., implemented in [25]). Although control mechanisms in digital twins for accessing their data and analytic capabilities represent no relevant input for cyber ranges, interfaces might be used to transmit data from the digital twin.

To conclude, some parts of the digital twin offer benefits for building cyber ranges. Especially the operation mode simulation can be used to create a virtual environment close to reality. Such a system simulation model can be directly transferred from the digital twin into the cyber range and – if necessary – customized to meet the cyber range's needs. The interfaces part of the digital twin might help to transfer the model, while additional data might help to create simulation scenarios or to get an overview of the system that is virtually represented. Overall, the simulation capability of the digital twin presents a valuable input for cyber ranges and will be concentrated on in the following.

4 A Cyber Range for SOC Analysts

To create the cyber range, it is first necessary to define the *learning objectives*, the *target group*, and the *requirements*. In the case of our cyber range, the analyst in training - hereafter referred to as the trainee - should be introduced to the tasks of a SOC analyst and learn how to work with a SIEM system. In the process, he or she should acquire the following skills and know-how:

S1: Knowledge of how selected incidents or attacks on the industrial system work.
S2: Manual detection of anomalies or incidents by analyzing log data with a SIEM system.
S3: Create both syntactically correct and semantically appropriate rules to detect the incidents.

The target group are individuals who want to achieve skills in security analytics within a SOC – for example, because they want to work as analysts in a SOC in

the future. They are assumed to have basic cybersecurity skills but have never worked with a SIEM system or in a SOC. Even though incident response often lies within an analyst's responsibilities, this will not be considered in this cyber range as, in our opinion, it is too complex to start with and would create too steep a learning curve. However, this could be addressed in future work.

One requirement for the cyber range is to run it entirely virtual in order for the trainees to take part in the cyber range remotely without physical presence. This allows the trainees to take part without too much effort. Additionally, it facilitates the evaluation with an international user study. Furthermore, since the user study is to take place in times when – due to COVID-19 restrictions – face-to-face contact should be kept to a minimum, conducting it in a classroom setting is not an option.

In the following, first the general concept of the cyber range is presented. Based on this, the scenario is described with the help of which the user should acquire the skills outlined above. Subsequently, the prototypical implementation of the cyber range is elaborated upon, with a brief description of the technologies used.

4.1 Cyber Range Concept

Our cyber range consists of five main building blocks (compare Fig. 1): A *virtual environment*, a *SOC*, a *management and monitoring* unit, a *learning management system*, and the *digital twin*, which lies outside of the cyber range. Thus, it represents a security analytics service [12] combined with cyber range specific components. In the following, these building blocks are explained in more detail.

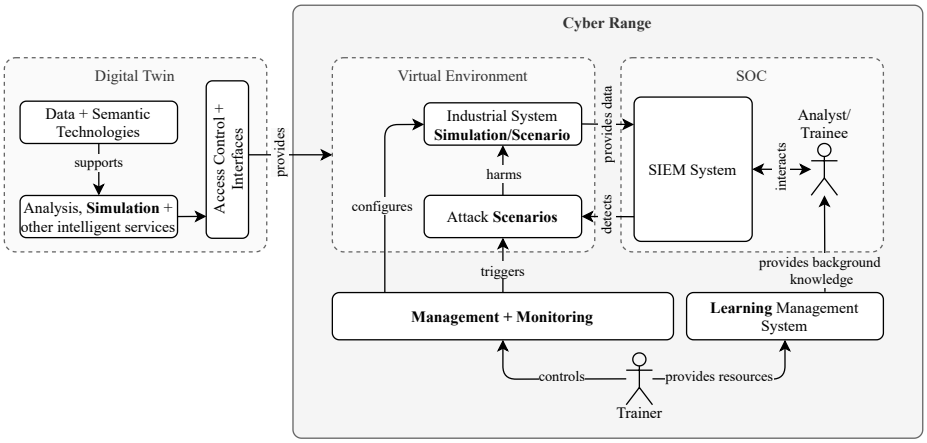


Fig. 1. Basic concept of the digital twin-based cyber range for SOC analysts.

As investigated in Section 3, the **digital twin** provides a system *simulation* model used to create the *virtual environment*. The simulation model is supported

by specification data, enabling a realistic simulation of the physical counterpart with which the trainee can dynamically interact, like with the real system within the organization. The data for the simulation is provided through respective *interfaces* and protected by *access control* capabilities.

The **virtual environment** implements and reflects the scenario of the cyber range through the simulation. For this purpose, an *industrial system* is simulated on the one hand and simulated *attacks* harming the industrial system are carried out on the other. Thereby, the planned training *scenario* is reproduced, guiding the trainee through several training units similar to a playbook, elaborated in more detail in Section 4.2. In the process, the simulated industrial system produces log data documenting its operation and providing traces pointing to the attack scenarios.

Within the **SOC** building block, a *SIEM system* is provided, which provides the actual point of interaction with the trainee. The SIEM represents the system for which an analyst is trained, and ideally is also a system in practical use in the trainee's organization. This ensures that the trainee learns to work with a system that is as close to the real SIEM as possible or even identical to it. The log data of the industrial system is fed into the SIEM. In the first step, the trainee interacts with the SIEM to analyze and manually detect the simulated attacks based on the available data. In the next step, the trainee can use this to create correlation rules in the SIEM, which detect attacks automatically.

The **learning management system (LMS)** provides additional learning material for the trainee and introduces the scenario. This information can be presented in various forms, such as videos or simple textual descriptions. In our case, an introduction to the functioning of SIEM systems and the structure of SIEM rules is provided. In addition, hints on the attacks are given to make it easier to get started using the SIEM. These materials are prepared by the trainer and are included in the LMS so that they can be accessed during the procedure. A more detailed description of the prepared media is given in Section 4.2.

With the help of the **management and monitoring** building block, the trainer can oversee the trainees' progress during training. Additionally, it configures the simulation of the industrial system and automatically triggers attack simulations depending on the progress of the training.

4.2 Scenario and Learning Concept

The scenario represented by the cyber range is an Industrial Control System (ICS)-based setting of a filling plant. Thereto, the simulation from the digital twin is used, which enables a realistic representation of the industrial filling plant. Figure 2 illustrates the setting in a simplified way for better understanding. The filling plant consists of a tank containing liquid that is to be filled into bottles. The tank is equipped with a sensor measuring the liquid level at regular intervals. To control how much liquid is bottled, the system includes a motoric valve that can be opened and closed. The flow-level sensor is being used to check how much liquid flows through the pipe towards the bottle at any given time. The level of the bottle itself is monitored with another sensor. Each sensor and the actuator is

controlled by one of the three Programmable Logic Controllers (PLCs) connected through a switch via Ethernet, which store the sensor data and communicate via Ethernet/IP. The interface between the employees and the industrial plant is realized with the help of a Human-Machine Interface (HMI). This allows an employee to read the measured and logged sensor values and intervene in the plant's operation. Within the scenario, it is assumed that an attacker has gained direct access to the network of the industrial plant. This allows him or her to carry out various attacks, which can then be detected in the SIEM.

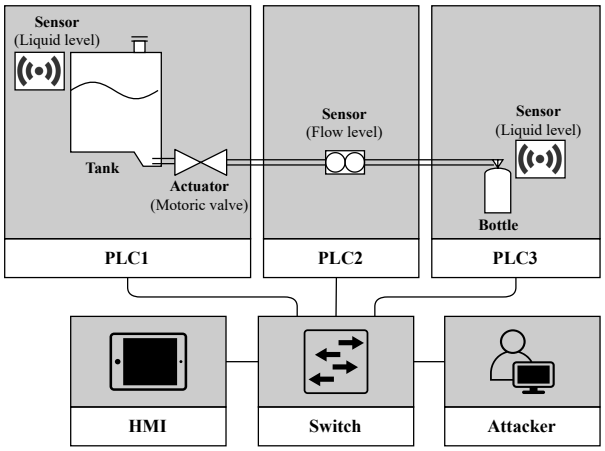


Fig. 2. ICS Scenario of the cyber range.

As shown in Fig. 3 the trainee is guided through the scenario by several learning materials provided by the LMS. Each step within the scenario is accompanied by a task that the trainee must complete.

The scenario is designed to slowly introduce to rule creation by requiring the trainee to solve increasingly elaborate tasks. It starts with a general introduction, where only simple questions about the events captured by the SIEM have to be answered. Once the first step is complete, increasingly complex attacks are simulated one after another, which the trainee must first detect manually (S2). Then he or she is required to create rules (S3) that automatically detect these attacks. The rules to be created also increase in complexity. In order not to overtax the trainee, large parts of the rule are initially given, and the trainee only has to add certain parts. Then, starting with the scenario step "log file manipulation", the trainee has to create the whole rules themselves. The complexity of the rules to be learned can be divided into three difficulty levels: Starting with very simple rules for which only one condition must be met, to multi-stage rules that build on each other and for which several conditions must be met, to rules that also query an IP address range.

The LMS provides various media to support the trainee's learning between each scenario step. These are either explanatory texts or videos that convey knowledge for the subsequent step in the scenario. In each case, the simulated attack is briefly presented from the attacker's point of view (S1) to provide guidance on what the trainee must look for in the SIEM. It also explains how to use the SIEM and how rules are structured. Gamification elements are used to motivate the trainee during the training session. The trainee receives points for each task he or she solves and can use them to move up levels. If a task is answered incorrectly, the trainee can correct the answer, but points are lost to prevent solutions from simply being guessed. If the trainee is stuck, hints can be bought with earned points, which guide towards the solution.

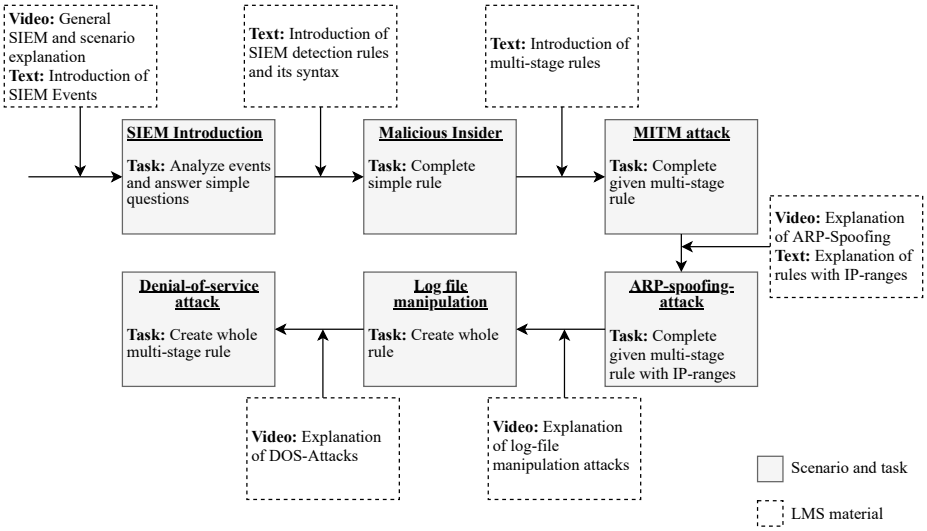


Fig. 3. Learning concept for the cyber range.

4.3 Prototypical Implementation

The overall architecture of the cyber range is shown in Fig. 4. To simulate the industrial system, the digital twin's simulation component is transferred to the cyber range to create a realistic virtual environment. The simulation is realized with MiniCPS[3], an academic framework for simulating cyber-physical systems which builds upon Mininet[4]. To monitor the network traffic, a firewall captures the TCP-traffic within the network and detects certain abnormalities such as ambiguous responses to ARP-requests. The firewall functionalities are

[3] https://github.com/scy-phy/minicps
[4] http://mininet.org/

implemented with scapy[5]. The PLCs and the HMI produce system logs on the main functions of the filling process and the firewall monitoring, which are stored as log files in a common logs directory.

As described in Section 4.2, the attacker performs various attacks against the network components. To implement the attacks, the network tools Ettercap[6] (for the ARP-Spoofing/Man-In-The-Middle-Attack) and hping3[7] (for the Denial-Of-Service-Attack) are used. The Log-File-Manipulation-Attack is performed by simply deleting the log file in which the system logs of PLC1 are stored. For the filling plant simulation to produce consistent system logs over the cyber range's lifetime, the attacks are automated and repeated periodically. The

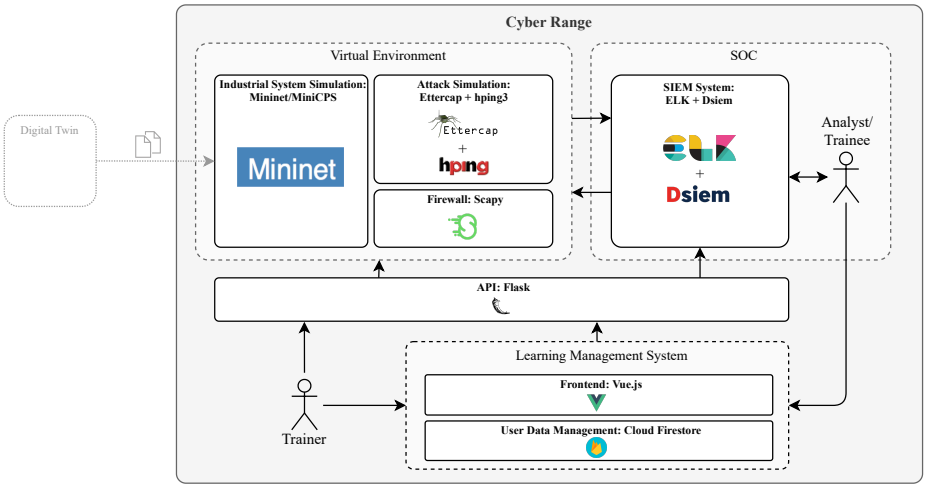


Fig. 4. Architecture of the prototypical implementation.

open-source tool Dsiem[8] is the implemented SIEM system of the cyber range. It builds upon Elasticsearch, Logstash, Filebeat, and Kibana. With Logstash and Filebeat, the aforementioned log data is parsed and normalized as so-called SIEM events, which are then forwarded to Dsiem. Dsiem correlates SIEM events with predefined rules to generate SIEM alarms. Finally, these SIEM events and alarms are transferred to Elasticsearch and visualized in Kibana. The virtual environment and the SIEM system are realized as a microservice-infrastructure separated from the LMS and with each component being deployed in a docker container. This modular architecture facilitates reusing the infrastructure for future work and enables its extension as well as the replacement of one or more of the components.

[5] https://scapy.net/
[6] https://www.ettercap-project.org/
[7] http://www.hping.org/
[8] https://www.dsiem.org/

The LMS is realized with the JavaScript framework Vue.js[9]. A screenshot of the user interface of the cyber range is presented in the Appendix (Fig. 6). One section of the LMS displays a Kibana-based SIEM dashboard for Dsiem. It visualizes the SIEM events produced by the digital twin-based simulation and the SIEM alarms triggered by the Dsiem rules and enables the trainees to interact with the SIEM system in real-time. The other section of the LMS consists of the provided learning material and the tasks the trainees need to complete. The trainee's current score, and the scores of the other trainees taking part in the training at the same time, are displayed on a scoreboard. This functionality is implemented by storing each trainee's current score in a Realtime Firestore[10]. Additionally, a timestamp is saved whenever a trainee completes a task. This enables the trainer to monitor the trainees' progress while the cyber range is being conducted.

The SIEM and the LMS are connected via a REST-API implemented with Flask[11]. Every time a trainee creates a detection rule by completing one of the tasks, an API request is set off to activate the respective rule in Dsiem. Dsiem then starts triggering alarms based on the new rule which are visualized on the SIEM dashboard inside the LMS. The LMS, therefore, enables the trainees to interact directly with the SIEM system and see the impact of detection rules without having to gain a deeper understanding of the project structure of the SIEM system beforehand. Furthermore, the Flask API provides functions for the trainer to interact with the microservice architecture of the digital twin-based simulation and the SIEM system. These functions can be used to start and stop the infrastructure and reset single components in case any technical issues occur while the cyber range training is being conducted. The source code of the project, together with further documentation, is available on GitHub[12].

5 User Study Evaluation

5.1 Method

To measure the effectiveness of the cyber range, it is necessary to evaluate whether it leads to an improvement of the participants' knowledge or skill level. Since a cyber range in our case is similar to a serious game according to the definition of Girard et al. [15], methods from this context can be applied to measure the effectiveness. Besides qualitative methods [16], it is possible to quantitatively evaluate this by measuring the participants' skills and knowledge before and after the training [15]. In the present case, to the best of our knowledge, a comparable system targeting the training of analysts within a SOC does not exist. Therefore it is not possible to evaluate the increase of performance of participants of the cyber range training against participants of a control group in order to compare

[9] https://vuejs.org/
[10] https://firebase.google.com/docs/firestore
[11] https://flask.palletsprojects.com/en/1.1.x/
[12] https://github.com/DigitalTwinSocCyberrange

it to a similar training concept. Instead, it is more suitable to use a one group pre-test/post-test design proposed by Hauge et al. [16] to show whether or not an increase in knowledge has been achieved. Therefore, two assessment questionnaires are constructed consisting of 13 multiple-choice questions (Q1 - Q13) for evaluating the learning outcomes of the cyber range. These aim at testing the knowledge of the participants, whereby four answer options are given for each question. These questionnaires are disseminated before and after the training to measure the improvement of the participant's knowledge.

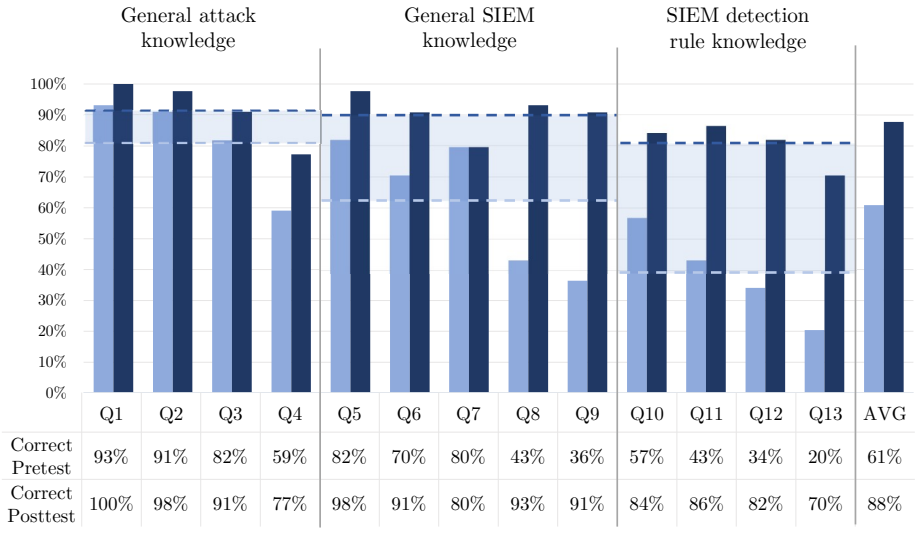
As the cyber range concept should not only lead to an increase of knowledge but also provide a positive learning experience, the training aims to attract the participant's attention and provide a high level of engagement. Metrics for measuring the engagement levels of the participants are provided by Keller's ARCS model of motivational design [18] which has been used in the past to evaluate security and privacy educational approaches before [14]. It focuses on the intrinsic attributes enhancing motivation, and includes metrics that relate to Attention, Relevance, Confidence, and Satisfaction. The ARCS model can be extended by an extra metric for perceived learning, which measures the subjective impression of whether learning has occurred [5, 1]. This part of the evaluation was implemented by constructing a feedback questionnaire based on the ARCS model, extended by the perceived learning condition. Thereto, the participants can indicate the degree of agreement to 16 statements, with a Likert scale ranging from 1 to 5 ("completely disagree" to "fully agree") after the training.

Participants. Participants were recruited in cybersecurity-related courses at both the University of Regensburg (Germany) and Ionian University (Greece). This ensures that all participants have at least a basic knowledge of cybersecurity, reflecting the target group of the cyber range. In total $n = 44$ test persons participated in the study: 22 German students and 22 Greek students, whereby 12 were female and 32 male. 24 students were undergraduate and 20 were postgraduate students.

Procedure. The study was conducted entirely online over several video conferencing sessions. For each session, 10 virtual machines with one cyber range each were available, limiting the simultaneous number of participants to 10. The user study was divided into three phases. After a short welcome and introduction to the cyber range at the start of the session, the participants were asked to complete the first questionnaire to record their previous knowledge. In the second phase, they were asked to open the cyber range and complete the training contained within. Participation was not time-limited, but most of the participants completed all tasks after a maximum of 2 hours. After having completed the second phase, the test persons were asked to fill in the two remaining questionnaires in the third phase, which tested their knowledge afterwards and assessed their motivation during the training. During the execution of the cyber range, we ensured that the trainer intervened as little as possible in the test persons' performance of the tasks in order to avoid influencing them and their results.

5.2 Results

To show that the participants of the study achieved a learning effect, the results from the assessment of the pre-, and post-knowledge are analyzed in the following. The study's questions can be divided into three classes: General knowledge about cybersecurity attacks, general knowledge about SIEM, and specific knowledge about the structure and functionality of SIEM detection rules. Figure 5 shows the results of the pre-, and post-test. Thereto, the mean percentage of correctly answered questions in both test runs is visualized. The dashed lines indicate the mean in the respective knowledge classes.



	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11	Q12	Q13	AVG
Correct Pretest	93%	91%	82%	59%	82%	70%	80%	43%	36%	57%	43%	34%	20%	61%
Correct Posttest	100%	98%	91%	77%	98%	91%	80%	93%	91%	84%	86%	82%	70%	88%

Fig. 5. Comparison of test persons' knowledge (measured by percentage of correct answers for questions Q1 to Q13) before and after participation in the cyber range. Grouped by knowledge classes, with the dashed lines visualizing the mean of each class.

A paired t-test was conducted to examine the increase in knowledge overall and across the individual knowledge classes[13]. It shows that the mean of correctly answered questions significantly increased by 26.92% ($t = -12.472, SD = 0.143191, p < 0.001$). In the first class, "general attack knowledge" the mean increase is smaller (10.23%) and less significant ($t = -3.448, SD = 0.196763, p = 0.0013$). This is, however, expected because the test persons possess a certain level of pre-knowledge in cybersecurity and therefore about simple attacks. Thus, the increase from an already high level is smaller. Within the class "general SIEM knowledge", an increase of 28.18% is observed ($t = -7.398, SD = 0.252681, p < 0.001$). Based on the pre-test, it could be determined that some pre-knowledge

[13] The SPSS output of the t-test can be found in Fig. 7 in the appendix

was already present within this class. However, a significant increase could still be achieved. Within the "SIEM detection rule knowledge" class, a significant increase of 42.05% is indicated ($t = -8.417, SD = 0.331368, p < 0.001$).

Since an increase in knowledge does not necessarily show that the cyber range was a positive experience for the participants, it is necessary to evaluate the results from the feedback survey. The aggregated results can be found in Table 2. The results indicate that the cyber range was, in general, received quite well by the test persons. Both the mean and the median are at least 4 for all conditions on a scale of 1 to 5 (where a higher value indicates the participants' agreement).

Table 2. Results of the feedback questionnaire.

Condition	Mean	Median	Standard deviation
Attention	4.395	5	0.753
Relevance	4.352	4	0.724
Confidence	4.090	4	0.778
Satisfaction	4.284	4	0.738
Perceived learning	4.460	5	0.602

To ensure a high standard of reproducibility and reusability, the anonymized data of all the results and the used questionnaires are available as a public data set[14].

5.3 Discussion

Overall, the results of the user study reveal that an increase in knowledge could be achieved among the participants. Although the increase in general knowledge about attacks (S1) was quite small, a significant increase in knowledge about attack detection using a SIEM system (S2 and S3) is shown – leading to the conclusion that the previously defined goals are achieved. Taking into consideration the results of the evaluation, in the following, we discuss some details we found to be particularly noteworthy.

Within the cyber range, the participants were able to score points by solving the tasks provided as described in Section 4.2. The score of a participant thereby indicates to what extent he or she was able to solve the tasks without requiring many attempts to provide the correct solution. While this score was not explicitly used for evaluating the effectiveness of the cyber range, we find it worth examining - especially for participants with particularly high or low increase in knowledge. Five participants showed a notably large increase in knowledge in the assessment questionnaire from 50% or less to more than 90% after participating in the cyber range. The score results of these participants

[14] https://github.com/DigitalTwinSocCyberrange/userStudy

vary from 43 to 100 out of 101 possible points. This shows that though initially failing some tasks of the cyber range, a participant can still gain a large increase of knowledge. In contrast, three participants did not present any improvement in the pre-, and post-assessment. These participants achieved comparably low scores ranging from 28 to 33 points. This indicates difficulties in engaging with the overall approach. However, it is noteworthy that these participants still provided positive feedback on the cyber range.

Considering the results of the feedback survey, a noticeable aspect is a somewhat lower result for Confidence compared to the other values. This is also confirmed by some participants' oral feedback, who told us that they were somewhat overstrained at the beginning. In our estimation, this was mainly due to an information overload, as they were confronted with both the SIEM and the LMS. In the future, the cyber range could be adapted so that trainees are not shown all information from the start, but only selected content that is then gradually expanded. The value for perceived learning also sticks out, indicating whether the participants themselves assess whether they learned something during the procedure. With a value of 4.460, it is slightly higher than the others. This confirms the result from comparing the pre-, and post-test, as the participants themselves also have the impression of having gained knowledge.

6 Conclusions

This work demonstrates how cyber ranges can be utilized for training security analysts in a SOC. It shows that cyber ranges are suitable for the acquisition of general knowledge about SIEM as well as for specific training on how to create SIEM rules. The provided cyber range concept builds upon the simulation component of a digital twin of an industrial filling plant. This ensures that the analysts are trained based on a realistic scenario. To show the increase in knowledge and the perceived learning experience, the concept is implemented and evaluated in an international study among both Greek and German participants. To the best of our knowledge, this is the first cyber range to utilize the potential of a digital twin, specifically targeting the training of SOC analysts.

Like any other research effort, this paper contains limitations. Since, to our knowledge, no approach with the same objective exists, it was not possible to compare the knowledge gains. However, we were able to show that a cyber range is, in general, suitable for imparting knowledge. Nonetheless, we did not concentrate on an evaluation comparing our cyber range to other concepts.

In summary, this work provides a new approach to train SOC analysts. By proposing security training, it addresses the current problem of the increasing demand for security analysts personnel, which will continue to grow. Furthermore, the attack detection training of SOC analysts is only one of many possible applications of the presented cyber range. Among many other possibilities, it could also be used for penetration testing of industrial plants or incident response exercises in future research.

Appendix

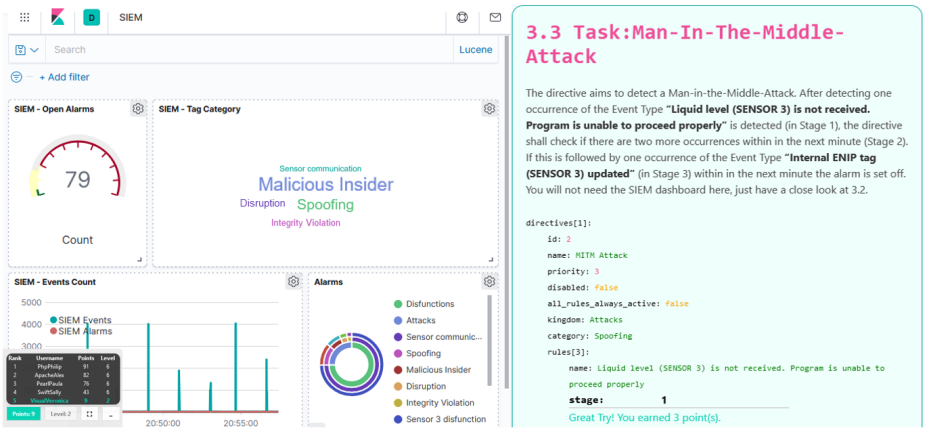


Fig. 6. Screenshot of the cyber range interface: SIEM dashboard and LMS

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Err. Mean
Pair 1	Correct_pre	,60839	44	,139608	,021047
	Correct_post	,87762	44	,148677	,022414
Pair 2	Correct_pre_att	,81250	44	,187742	,028303
	Correct_post_att	,91477	44	,142069	,021418
Pair 3	Correct_pre_SIEM	,62273	44	,280252	,042250
	Correct_post_SIEM	,90455	44	,146199	,022040
Pair 4	Correct_pre_rule	,38636	44	,255489	,038516
	Correct_post_rule	,80682	44	,240298	,036226

Paired Samples Test

		Paired Differences					t	df	Sig. (2-tailed)
					95% Conf. Interval of the Diff.				
		Mean	Std. Deviation	Std. Err. Mean	Lower	Upper			
Pair 1	Correct_pre - Correct_post	-,269231	,143191	,021587	-,312765	-,225697	-12,472	43	,000
Pair 2	Correct_pre_att - Correct_post_att	-,102273	,196763	,029663	-,162094	-,042451	-3,448	43	,001
Pair 3	Correct_pre_SIEM - Correct_post_SIEM	-,281818	,252681	,038093	-,358640	-,204996	-7,398	43	,000
Pair 4	Correct_pre_rule - Correct_post_rule	-,420455	,331368	,049956	-,521199	-,319710	-8,417	43	,000

Fig. 7. SPSS Output of the t-test

References

1. Barzilai, S., Blau, I.: Scaffolding game-based learning: Impact on learning achievements, perceived learning, and game experiences. Computers and Education **70**, 65–79 (2014)
2. Bissel, K., Lasalle, R., Dal Cin, P.: Third annual state of cyber resilience report. Accenture (2020)
3. Boschert, S., Heinrich, C., Rosen, R.: Next Generation Digital Twin. In: Proceedings of the 12th International Symposium on Tools and Methods of Competitive Engineering. pp. 209–217. TMCE 2018 (2018)
4. Bécue, A., Fourastier, Y., Praça, I., Savarit, A., Baron, C., Gradussofs, B., Pouille, E., Thomas, C.: CyberFactory1 — Securing the industry 4.0 with cyber-ranges and digital twins. In: 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS). pp. 1–4 (2018)
5. Caspi, A., Blau, I.: Social presence in online discussion groups: Testing three conceptions and their relations to perceived learning. Social Psychology of Education **11**(3), 323–346 (2008)
6. Dietz, M., Pernul, G.: Digital Twin: Empowering Enterprises Towards a System-of-Systems Approach. Business & Information Systems Engineering **62**(2), 179–184 (2020)
7. Dietz, M., Pernul, G.: Unleashing the Digital Twin's Potential for ICS Security. IEEE Security Privacy **18**(4), 20–27 (2020)
8. Dietz, M., Vielberth, M., Pernul, G.: Integrating Digital Twin Security Simulations in the Security Operations Center. In: Proceedings of the 15th International Conference on Availability, Reliability and Security. ARES '20, ACM, New York, NY, USA (2020)
9. Eckhart, M., Ekelhart, A.: A Specification-Based State Replication Approach for Digital Twins. In: Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy. p. 36–47. CPS-SPC '18, ACM, New York, NY, USA (2018)
10. Eckhart, M., Ekelhart, A.: Towards Security-Aware Virtual Environments for Digital Twins. In: Proceedings of the 4th ACM Workshop on Cyber-Physical System Security (CPSS '18). pp. 61–72 (2018)
11. Eckhart, M., Ekelhart, A.: Digital Twins for Cyber-Physical Systems Security: State of the Art and Outlook, pp. 383–412. Springer International Publishing, Cham (2019)
12. Empl, P., Pernul, G.: A flexible security analytics service for the industrial iot. In: Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems. pp. 23–32. ACM, New York, NY, USA (2021)
13. Gehrmann, C., Gunnarsson, M.: A Digital Twin Based Industrial Automation and Control System Security Architecture. IEEE Transactions on Industrial Informatics **16**, 669–680 (2020)
14. Giannakas, F., Papasalouros, A., Kambourakis, G., Gritzalis, S.: A comprehensive cybersecurity learning platform for elementary education. Information Security Journal **28**(3), 81–106 (2019)
15. Girard, C., Ecalle, J., Magnan, A.: Serious games as new educational tools: how effective are they? A meta-analysis of recent studies. Journal of Computer Assisted Learning **29**(3), 207–219 (2013)
16. Hauge, J.B., Boyle, E., Mayer, I., Nadolski, R., Riedel, J.C.K.H., Moreno-Ger, P., Bellotti, F., Lim, T., Ritchie, J.: Study Design and Data Gathering Guide for Serious Games' Evaluation. In: Tennyson, R., Connolly, T.M., Hainey, T., Boyle,

E., Baxter, G., Moreno-Ger, P. (eds.) Psychology, Pedagogy, and Assessment in Serious Games, pp. 394–419. Advances in Game-Based Learning, IGI Global (2014)
17. Kavallieratos, G., Katsikas, S.K., Gkioulos, V.: Towards a cyber-physical range. In: Proceedings of the 5th on Cyber-Physical System Security Workshop - CPSS '19. pp. 25–34. ACM Press, New York, USA (2019)
18. Keller, J.M.: Development and use of the ARCS model of instructional design. Journal of Instructional Development **10**(3), 2–10 (1987)
19. Kelley, D., Moritz, R.: Best Practices for Building a Security Operations Center. Information Systems Security **14**(6), 27–32 (2006)
20. Leitner, M., Frank, M., Hotwagner, W., Langner, G., Maurhart, O., Pahi, T., Reuter, L., Skopik, F., Smith, P., Warum, M.: AIT Cyber Range: Flexible Cyber Security Environment for Exercises, Training and Research. In: Proceedings of the European Interdisciplinary Cybersecurity Conference, pp. 1–6 (2020)
21. Madani, A., Rezayi, S., Gharaee, H.: Log management comprehensive architecture in Security Operation Center (SOC). In: 2011 International Conference on Computational Aspects of Social Networks (CASoN). pp. 284–289. IEEE (2011)
22. Negri, E., Fumagalli, L., Macchi, M.: A Review of the Roles of Digital Twin in CPS-based Production Systems. Procedia Manufacturing **11**, 939–948 (2017)
23. Pescatore, J., Filkins, B.: Closing the Critical Skills Gap for Modern and Effective Security Operations Centers (SOCs). SANS Institute (2020)
24. Pokhrel, A., Katta, V., Colomo-Palacios, R.: Digital Twin for Cybersecurity Incident Prediction: A Multivocal Literature Review. In: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops. p. 671–678. ICSEW'20, ACM, New York, NY, USA (2020)
25. Putz, B., Dietz, M., Empl, P., Pernul, G.: EtherTwin: Blockchain-based Secure Digital Twin Information Management. Information Processing Management **58**(1), 102425 (2021)
26. Rubio, J.E., Roman, R., Lopez, J.: Analysis of Cybersecurity Threats in Industry 4.0: The Case of Intrusion Detection. In: D'Agostino, G., Scala, A. (eds.) Critical Information Infrastructures Security. pp. 119–130. Springer International Publishing, Cham (2018)
27. Schinagl, S., Schoon, K., Paans, R.: A Framework for Designing a Security Operations Centre (SOC). In: 2015 48th Hawaii International Conference on System Sciences. pp. 2253–2262. IEEE (2015)
28. Tian, Z., Cui, Y., An, L., Su, S., Yin, X., Yin, L., Cui, X.: A Real-Time Correlation of Host-Level Events in Cyber Range Service for Smart Campus. IEEE Access **6**, 35355–35364 (2018)
29. Ukwandu, E., Farah, M.A.B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I., Bellekens, X.: A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. Sensors (Basel, Switzerland) **20**(24) (2020)
30. Vielberth, M., Bohm, F., Fichtinger, I., Pernul, G.: Security Operations Center: A Systematic Study and Open Challenges. IEEE Access **8**, 227756–227779 (2020)
31. Vielberth, M., Pernul, G.: A Security Information and Event Management Pattern. In: 12th Latin American Conference on Pattern Languages of Programs (SugarLoafPLoP 2018), pp. 1–12. The Hillside Group (2018)
32. Yamin, M.M., Katt, B., Gkioulos, V.: Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security **88**, 101636 (2020)