Using Digital Twin Technologies to Train Information Security Professionals

Alina R. Kasimova[a], Lina Kh. Safiullina[b] and Anna A. Alekseeva[c]
Department of Information Security, Kazan National Research Technological University, Karl Marx street, Kazan, Russia
KasimovaAR@corp.knrtu.ru, SafiullinaLKh@corp.knrtu.ru, annank90@mail.ru

Keywords: Cyber range, vulnerabilities, information security, training, network attacks, monitoring.

Abstract: This paper explores the possibility of using digital twins of enterprise information systems, based on the Cyber polygon, to train Information Security students. The term "cyber polygon" is defined as a digital twin of the enterprise IT structure, allowing the implementation of various attack scenarios. A cyber polygon allows students to develop skills in eliminating vulnerabilities without harming real systems. The authors conducted a study with Information Security students to assess how cyber-range-based training affects their learning. Statistical analysis showed that second- and third-year students practiced scenarios as both the monitoring and response teams. Repeated practice significantly reduced the time to close vulnerabilities, but the same scenarios should not be overused to prevent memorization. Moreover, third-year students showed better results than second-years due to greater experience with the cyber range.

1 INTRODUCTION

Ever-increasing digitalization pace in the Russian Federation, implementation of the Digital Economy project, and formation of the Data Economy project ensure the information technology development and, along with this, carry new threats and risks (Chelnintseva, 2023, Mustafaev, 2021). Information security (IS) of public, corporate, financial and other systems becomes the key task of digital transformation. Number and preparation level of cyberattacks increase yearly, and what is more, the share of targeted attacks on production sector grows (Ghiasi, 2023, Duo 2022). At the same time, the market of IS specialists is experiencing an acute shortage of competent personnel, and the need for them will only increase (Defitsit kadrov v IB-otrasli RF dostigayet poryadka 100 tys. chelovek i budet rasti – ekspert, 2024, Zasseev, 2023). It is usually considered that the main reason for this deficiency is the withdrawal of foreign vendors that developed devoted IS solutions from the Russian market; however, the shortage of professionals is also associated with the rapid technology development, with the increasing cyberthreats, and what is more, with the insufficient practical experiences of IS specialists, both being trained and currently working. At the same time, the rapidly evolving digitalization of all industries of the Russian Federation dictates new requirements for IS systems and for professionals that protect them.

According to the IB-BANK.RU industry portal (Rynok truda vo vtorom kvartale 2023 goda, 2023), the demand for IS professionals in 2023 was 37% higher than that in the same period of 2022; and 54% of Russian companies are experiencing the shortage of IS specialists, 0.8 CVs being submitted per vacancy. Along with the number of specialists, the most pressing is the issue of their training quality. The 38% increase in the number of cyberattacks in the second quarter of 2023 compared to the same period of 2022 (325 thousand incidents) stimulated the relevant agency to update the educational standards for training IT professionals majoring in IS (Solominsky, 2023).

Integrated group of training areas, coded 10.00.00, is one of the most demanded ones requiring specialized laboratories, network devices, software products, and data simulation and analysis systems for their implementation. Educational standards

[a] https://orcid.org/0000-0001-8927-9113
[b] https://orcid.org/0000-0002-2765-0973
[c] https://orcid.org/0000-0002-6119-1934

provide for possible replacement of specially equipped spaces with their virtual twins. Digital twin (DT) is an example of virtually representing a physical system that frames or mirrors the characteristics of its physical analog as realistically as possible (Varghese, 2022, Shinkevich, 2023).

Using DT for developing and testing security systems can facilitate the detection of potential IS threats and accelerate the adoption of protection measures. In addition, a DT of an information or IS system can be used for effectively training both employees responsible for IS at enterprises and students majoring in the areas grouped under code 10.00.00.

A universal example of a DT as an analog of the company's digital environment is the cyber range that represents a multifunctional hardware and software system intended for educating, training, and drilling their information security personnel.

Using a cyber range for implementing data collection, analysis, and management within the system is quite promising, as it does not affect the real infrastructure of the enterprise and represents the so-called "sandbox" (a controlled environment that, in addition to everything else, can be used to validate and verify the data).

Aim of this study was to study the impact of the cyber range as a digital twin of the company's network upon the quality of training the novice IS professionals and upon the minimization of cyberattack risks.

To achieve our aim, we chose the following objectives:

- Define the concept of the cyber range as a digital twin of the enterprise IT system (network), as well as its functionality and structure;
- Conduct cyber drills for recent graduates using a cyber range; and
- Study how cyber drills affect the professional training level and the enterprise security system management.

According to different approaches, there are many definitions of digital twins (DTs). For example, based on virtual simulation, DT is defined as a digital dynamic model in the virtual world, that is thoroughly consistent with the physical object in the real world, suitable for imitating its characteristics, behavior, lifecycle, and performance (Zhuang, 2018, Grinyaev, 2021, Kasimova, 2023). Based on a cyber system, DT is a virtual replica of a physical system, which really simulates all its functional capabilities or is a part of the cyber-physical system and provides employees with the data on the manufacturing system (Graessler, 2017, Korovin, 2021, Dietz 2020)

Regulatory documents related to digital twins (State Standard 57700.37, 2021) define a digital twin as a system that consists of a digital model of the product and the two-way data communications with the product (if there is a product) and/or its subcomponents. In the context of this study, we used the following definition of a digital twin: It is a virtual copy of the vulnerable information system of a standard chemical company with network security subsystems and an incident investigation system.

Using a cyber range is based on a technology that allows automatically deploying a consistent IT infrastructure. For a full-fledged simulation of the processes, all systems are configured according to the suite of applications, users, and their behaviors, which allows ensuring the infrastructure operation realism. Attacks on the system in each segment are variable in their complexity; therefore, it is possible to choose a relevant scenario of impossible events for students having different levels of knowledge and experience. The cyber range must ensure the detectability of attacks, investigation of IS incidents, and implementing steps to prevent the attacks.

In using a cyber range to solve the problems of information security control and minimization of attack risks, we can use algorithms of data collection and safe testing of the known vulnerabilities, as well as their impact on the company's technology and business processes. To be used in training, a cyber range as a digital twin of the IT infrastructure must ensure the execution of the following functions:

- Practicing skills related to analyzing the events and investigating the IS incidents;
- Practicing skills related to assessing the safety of systems and removing vulnerabilities, including through cyber drills and contests;
- Testing the software, equipment and tools, and data security facilities for security and absence of vulnerabilities; and
- Enriching the database of threats, vulnerabilities, and attack scenarios.

Today's market of cyber ranges offers both Russian products, such as Ampire manufactured by Perspektivny monitoring (Advanced Monitoring Company), BI.ZONE Cyber Polygon, Jet CyberCamp, The Standoff, Kiberpoligon (Cyber Range), Kibermir (Cyber World), etc., and foreign products, such as Check Point Cyber Range, Cisco Cyber Range, Cyber Ranges, and Project Ares (Pepelyaev, 2023).

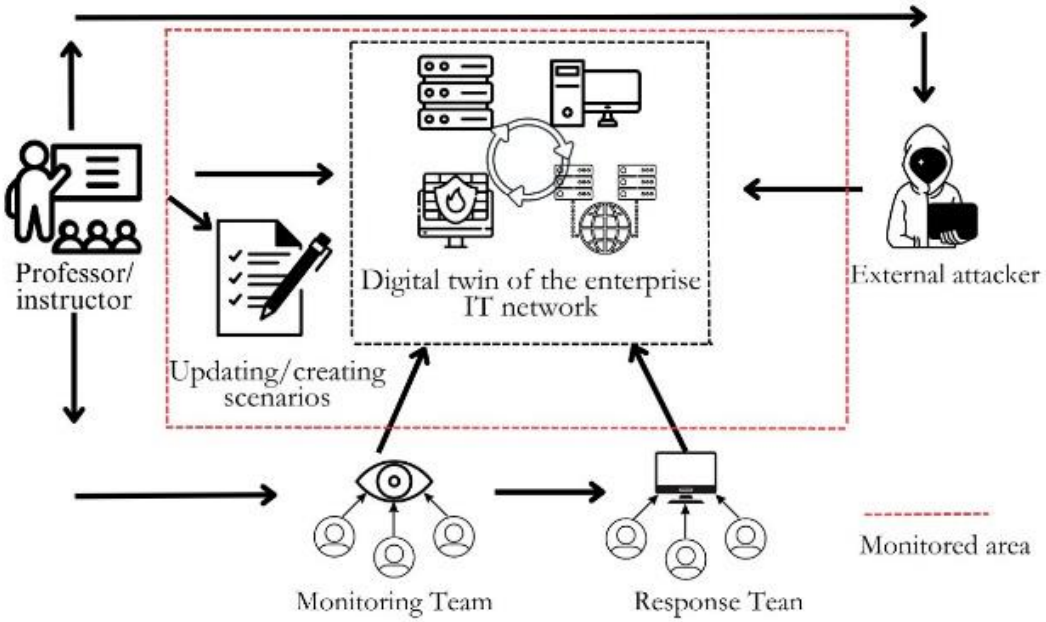

Figure 1: Architecture of the cyber range used.

The above platforms may have different architectures and comprise standard network models of companies, attacking scenarios, and infrastructure elements; however, the common framework of cyber ranges is similar and has some mandatory elements, such as network model, attack simulating models (scenarios), monitoring and response tools, and reporting. Figure 1 shows an exemplary cyber range architecture. In training novice specialists on a cyber range, it is important to have a possibility of simulating a specific network or IT infrastructure of the enterprise, as well as enriching the base of attacking scenarios, allocating roles, segmenting, supporting the reporting system, and working as part of the Red Team. In this case, the aim of the Red Team is to detect vulnerabilities and weak spots in the company's security systems and provide recommendations of how to improve them.

2 METHODS

Cyber drills were conducted for novice specialists using the Ampire software suite intended for training the employees of the relevant departments on the computer attack identification techniques, development of practical skills in investigating the computer IS incidents, algorithms of team interaction, and implementation of protection measures aimed at removing the IS deficiencies detected in general- and special-purpose information networks. Digital twin configurations, functionality, and expected usability and performance are described in (Kasimova, 2022, Baranov, 2022).

We should notice the following key aspects of arranging cyber training:

1. Allocation of roles: Administrator, Teacher, Student. Administrator deploys infrastructure, creates and blocks users, and manages the DTs of information systems. Teacher manages the users during training, starts/stops attacks or certain details, removes the attack consequences, and organizes students into monitoring and response teams. Students can have access to the DT templates of the network, IT system, and information protection system of the enterprise. Depending on whether an individual student is in the response team or monitoring team, they may have access to either creating incident records and conduct follow-ups or directly connect to the system nodes.

2. Choosing a scenario. Each scenario in the Ampire network DT is based on modeling targeted computer attacks on the IT infrastructure of a certain company, focusing on practicing protection skills (Vasiliev, 2021). According to the template, a completely automated training attack is conducted, modeling the actions of an intruder or insider. Scenarios are presented as the standard information system templates of some enterprises, which may include the following segments:

- Databases;
- WWW resources;
- Network infrastructure;
- File servers;
- Guarding server;
- Anti-virus;
- Anti-SPAM;
- Process-control system;
- Scientific and technical information;
- Corporate portal against insiders; and
- Anti-DOS-attacks.

To study the effects provided by cyber drills with the company's network DT on enhancing the expertise of novice specialists, we used the scenario of the attacker's actions on the company's database segment, shown in Figure 2.

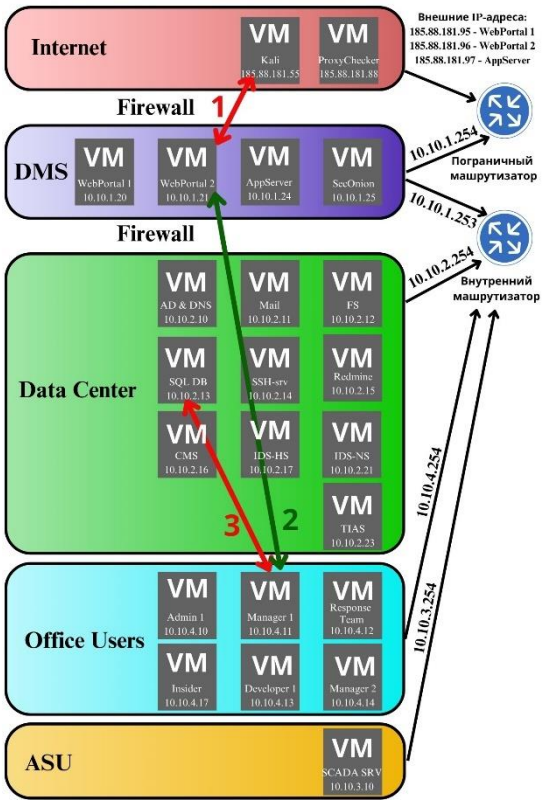

Figure 2: Diagram of the scenario of an intruder's action on the enterprise database system.

According to the scenario, the attacker scans the network and uses the address of 185.88.181.0/24 to find a server with CMS Drupal. Then, using the Drupalgeddon2 vulnerability, the attacker gains control over the host, generates a reverse shell, and waits until the user starts.

The user downloads and runs the malicious file, reporttool.py, with the consequence that the attacker gains control over the user's computer. To connect to the database, an attacker finds the path and scans the 10.10.2.0/27 that allows locating the SSH server and, using the medusa utility guesses the password and gets the access to the SQL server. Having connected successfully, the intruder reads the history file using the .bash_history command and finds the database access password, after which connects and copies the information.

3 RESULTS

Guided by the teacher during their training, the monitoring team defines the list of vulnerabilities, such as Drupalgeddon2, weak SSH password, database password in the clear in the .bash_history file, etc., while the response group defines the techniques for deactivating the attack.

The teacher assesses and registers the number of attempts and analyzes the quantity and quality of incident recording. To analyze the efficiency of using the cyber range in training the novice IS specialists, 238 trainings (cyber drills) were conducted with the group of young professionals over the period from March 23 to November 1, 2023.

We are going to conduct a comparative analysis based on the data of second-year students majoring in Information Security (10.03.01, attempts 1 and 2) and third-year students majoring in IT Security in Law Enforcement (10.05.05) and on the data obtained over the period from September 1 to November 1, 2023, where the data were selected from among the second-year students majoring in 10.03.01 (4 groups) and third-year students in 10.05.05 (2 groups). Figures 3–4 show the results of closing the vulnerabilities. Training quality was analyzed by the completeness and correctness of filling out incident records and by the number of attempts to practice the scenario.

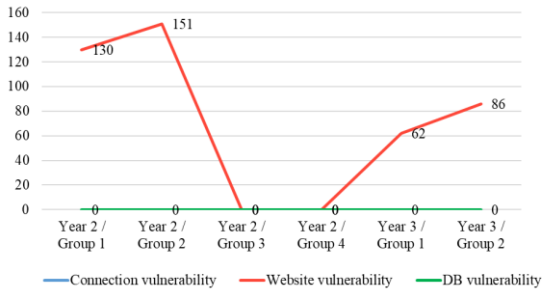

Figure 3: Results of removing vulnerabilities by second-year students majoring in Information Security (10.03.01) and third-year students majoring in IT Security in Law Enforcement (10.05.05). First attempt.

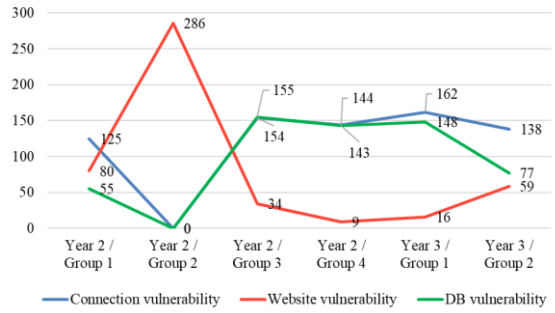

Figure 4: Results of removing vulnerabilities by second-year students majoring in Information Security (10.03.01) and third-year students majoring in IT Security in Law Enforcement (10.05.05). First attempt.

The monitoring team's output shall be incident records filled out correctly and containing as accurate and correct information on the intruder's action detected as possible. The following must be specified briefly: Description of the incident detected, specifying the target object and attacking technique; artifacts identified in the network or on its nodes, which suggest the unauthorized access to the system; IP addresses of the source and the recipient (damaged asset); and the incident recording date and time. The event description shall provide the attack details obtained by the monitoring team when analyzing the events in security devices, searching for information in open sources, jointly discussing the issues, etc. Recommendations provide the list of measures intended for locating the intruder, isolating the nodes damaged, choosing the remedy, etc. Incident records allow assessing the scenario sophistication level and proficiency in closing vulnerabilities and their effects. Table 1 shows the training results.

As the table shows, second- and third-year students fail in closing vulnerabilities at first attempt, while the mean value of correctly filling out incident records is 50%. At the same time, all students succeed in closing vulnerabilities and filling out records at second attempt. The time it takes for closing the vulnerability and recovering information systems is an important factor for the specialist in a company. Multiple practicing various scenarios by the students will improve their response skills and adaptivity to various threats and allow optimizing their actions in security incidents.

4 DISCUSSION

Along with software and new approaches to and conditions of developing professional expertise, students' motivation and personal qualities that may affect the quality of knowledge. Comparing the data presented with the USE scores at admission has shown that the initial knowledge does not influence the quality of activities performed on the cyber range. Second- and third-year students included in the study had average scores 80 and 78.8, respectively; at the same time, the highest total score is 260 for the second-year students and 242 for the third-year students. At the same time, it is obvious that third-year students being new at the cyber range perform better than second-year students..

Table 1: Students' performance in closing vulnerabilities on the cyber range.

Year of study	Number of students	Attempt	Time to close a connection vulnerability (in min.)	Time to close a website vulnerability (in min.)	Time to close a DB vulnerability (in min.)	Number of incident records (in pcs.)	Percentage of correct records (in %)
2	5	1	0	130	0	2	50
2	6	1	0	151	0	2	100
2	6	1	0	0	0	0	0
3	5	1	0	62	0	5	75
3	5	1	0	86	0	4	50
2	5	2	125	55	80	6	100
2	6	2	155	34	154	4	100
2	6	2	144	9	143	3	100
3	4	2	162	16	148	3	100
3	5	2	138	59	77	3	100

5 CONCLUSIONS

Implementing diverse scenarios with specific functionality on the network DT allows developing practical skills to prevent attacks on computer networks, analyzing the situation and interacting with other participating specialists.

Apparently, entry-level specialists acquire practical skills in virtual simulations when participating in cyber drills, which raises their expertise. Testing the scenarios allows verifying and enhancing the response to various scenarios of cyberattacks, which reduces risks for real systems. At the same time, collective participation of specialists fosters the team spirit and collaboration among the information security team members.

Obviously, number of cyber drills conducted using various scenarios will allow training highly qualified professionals capable of confronting threats and promptly responding to attacks on information systems. Conducting drills for enterprise security officers on a cyber range will also contribute to improving the training of specialists, enhancing the security of systems, and more efficiently managing the cyberthreatsWe hope you find the information in this template useful in the preparation of your submission.

REFERENCES

Chelnintseva, E. V., Yarullin ,R. R., 2023. National Project: Digital Economy. Mezhdunarodnyy zhurnal gumanitarnykh i yestestvennykh nauk, no. 5-5 (80), pp. 120–125.

Mustafaev, A.G., Kobzarenko, D.N., Buchaev, A.Ya., 2021. Digital transformation of the economy: Threats to information security. BENEFICIUM, no 2(39), pp. 21–26.

Ghiasi, M. et al., 2023. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electric Power Systems Research, no. 215, pp. 108975.

Duo, W., Zhou, M.C., Abusorrah, A., 2022. A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges. IEEE/CAA Journal of Automatica Sinica, Vol. 9, no. 5, pp. 784-800.

Defitsit kadrov v IB-otrasli RF dostigayet poryadka 100 tys. chelovek i budet rasti – ekspert, 2024. Available at: https://academia.interfax.ru/ru/news/articles/12020 (accessed May 30, 2024) (In Russian).

Zasseev, A.A., Magazieva, Z.A., Aliev, I.M., 2023. Economic aspects of information security. Ekonomika: vchera, segodnya, zavtra, Vol 13, no 8A, pp. 349-355.

Rynok truda vo vtorom kvartale 2023 goda, 2023. Available at: https://ib-bank.ru/bisjournal/post/2112 (accessed May 30, 2024) (In Russian).

Solominsky, A.V., 2023. Current trends in the information security market. Vestnik nauki i obrazovaniya, no 8 (139), pp. 22-27.

Varghese, S.A. et al., 2022. Digital Twin-based Intrusion Detection for Industrial Control Systems. Available at: https://www.researchgate.net/publication/362151115_Digital_Twin-based_Intrusion_Detection_for_Industrial_Control_Systems (accessed May 30, 2024).

Shinkevich, A.I., Kasimova, A.R., Alekseeva, A.A., 2023. Using digital twins to green the chemical industry. Izvestiya Samarskogo nauchnogo tsentra Rossiyskoy akademii nauk, Vol. 25, no 4, pp. 87–94.

Zhuang, Ñ., Liu, J., Xiong, H., 2018. Digital twin-based smart production management and control framework for the complex product assembly shop-floor. International journal of advanced manufacturing technology, Vol. 96, pp. 1149–1163.

Grinyaev, S.N., Remishevskaya, K.V., 2021. Analytical review of the dissertation activity in the field of application of the principles of information security in the design of digital twins. Informatsionnyye voyny, no. 3, pp. 78-81. (In Russian).

Kasimova, A.R. et al., 2023. Using the digital twin in information security management. Prikaspiyskiy zhurnal: upravleniye i vysokiye tekhnologii, no. 1 (61), pp. 48-58.

Graessler, I., Poehler, A., 2017. Integration of a digital twin as human representation in a scheduling procedure of a cyber-physical production system. IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), pp. 289–293.

Korovin, G.B., 2021. The opportunities for using digital twins in industry. Vestnik ZabGU, no 8, pp. 124-133.

Dietz, M., Vielberth, M., Pernul, G., 2020. Integrating digital twin security simulations in the security operations center. Proceedings of the 15th International Conference on Availability, Reliability and Security, pp. 1-9.

State Standard 57700.37–2021 Computer models and simulation. Digital twins of products. General provisions. Moscow, Standartov Publ., 2021, 10 p. (In Russian).

Pepelyaev D.N., Kondrashova E.V., Vishnyakova A.N., 2023. Review of the Russian cyber range market: Choosing the most profitable way to conduct cyber exercises. Tsifrovoy region: opyt, kompetentsii, proyekty: tr. V Yubileynoy Mezhdunarodnoy nauchno-prakticheskoy konferentsii, Bryansk, pp. 699-703. (In Russian).

Kasimova, A.R., Safiullina, L.Kh., 2022. Using digital twins when building an enterprise security system. International Forum KAZAN DIGITAL WEEK – 2022, Vol. 1, pp. 291-298.

Baranov, V.V., Korchagina, A.P., 2022. Developing and implementing a cyber range in training the information security specialists. Vestnik Voyennogo

innovatsionnogo tekhnopolisa “ERA”, Vol. 3, no 4, pp. 401-406.