Journal of Network and Systems Management (2024) 32:42
https://doi.org/10.1007/s10922-024-09816-w

Towards NICE-by-Design Cybersecurity Learning Environments: A Cyber Range for SOC Teams

Stylianos Karagiannis[1,2] · Emmanouil Magkos[1] · Eleftherios Karavaras[1,3] · Antonios Karnavas[1] · Maria Nefeli Nikiforos[1] · Christoforos Ntantogian[1]

Received: 29 September 2023 / Revised: 29 February 2024 / Accepted: 1 March 2024 /
Published online: 9 April 2024

Abstract

Cybersecurity has become an increasingly important field as cyber threats continue to grow in number and complexity. The NICE framework, developed by NIST, provides a structured approach to cybersecurity education. Despite the publication of cybersecurity frameworks, scenario design in cybersecurity is not yet governed by structured design principles, leading to ambiguous learning outcomes. This research uses the NICE framework to provide structure design and development of a cyber range and the relevant scenarios. The proposed methodology and research results can assist the scenario design in cybersecurity and as a methodological procedure for evaluation. Finally, the research provides a better understanding of the NICE framework and demonstrates how it can assist in creating practical cybersecurity scenarios.

Keywords Cyber range · Cybersecurity · Cybersecurity education · NICE framework · Blue team

Stylianos Karagiannis, Emmanouil Magkos and Christoforos Ntantogian contributed equally to this work.

✉ Stylianos Karagiannis
skaragiannis@ionio.gr

✉ Emmanouil Magkos
emagos@ionio.gr

✉ Christoforos Ntantogian
dadoyan@ionio.gr

[1] Department of Informatics, Ionian University, Plateia Tsirigoti 7, 49100 Corfu, Greece

[2] PDM, Fradesso da Silveira n.4 1B, 1300-609 Lisbon, Portugal

[3] Adacom S.A., Kreontos Str. 25, 10442 Athens, Greece

1 Introduction

Cybersecurity is an increasingly important scientific domain since the number and sophistication of cyber threats is growing. According to the International Information Systems Security Certification Consortium (ISC[1]), there is a cybersecurity workforce gap of roughly 4 million in cybersecurity. Despite efforts to address the issue, the skills shortage remains a challenge in cybersecurity [1]. The National Institute of Standards and Technology (NIST[2]), in an attempt to address the skills and workforce gap in cybersecurity, started the National Initiative for Cybersecurity Education (NICE) [2, 3]. The NICE framework proposes a taxonomy with capability indicators, namely Tasks (T), Knowledge (K), Skills (S), or in summary, the TKS taxonomy. NICE has been widely recognized as successful in creating a vast body of information that defines the concepts and practices used by cybersecurity professionals [4, 5]. The first version of NICE was published in April 2013, with later updates released in August 2017 and further important updates during 2019 [5–7].

The NICE framework started as an effort to address the problem, mainly focused on updating the higher education [8] along with various commercial certifications that eventually could not sufficiently address the problem [9, 10]. However, recent research [9] emphasises the importance of creating interdisciplinary competencies for cybersecurity professionals and the role of education transformation. Despite the many educational frameworks for cybersecurity, Furnell et al. (2020) argue that the frameworks alone are insufficient to recognize the range of skills required in the field [11]. Nevertheless, ensuring these skills are effectively integrated and utilized in conjunction is very important.

In addition, researchers have explored other methods to educate professionals in this field. Valdemar et al. [12] analyzed the content of CTF challenges for testing and improving cybersecurity skills and mapped them to formal curricular guidelines. Erdogan et al. [13] developed courses and training materials based on identified work roles. Regarding Security Operations Center (SOC) operations, Vielberth et al. [14] discuss the role of SOC teams in preventing major incidents. Academic research has focused on SOCs, identifying the primary building blocks and challenges within these centres. In their research, the authors [14] suggest that further research should be conducted on establishing a better connection between the human and technological aspects.

Considering the above, providing practical training material that involves hands-on exercises in realistic digital environments is crucial. This issue was addressed in the past using Capture the Flag (CTF) challenges and virtual labs [5, 15–20]. To this end, there are many approaches available for these types of training, including Hack the Box [21], TryHackMe [22], and Vulnhub [23]. In addition, the European Union Agency for Cybersecurity (ENISA) [24] has also published many online training materials and virtual labs on that perspective.

[1] https://www.isc2.org/.

[2] https://www.nist.gov/director/nist-information-quality-standards.

CTF and virtual labs are very important; however, integrating human and technological elements and the interdisciplinary nature of complex cybersecurity topics can be further facilitated through cyber ranges. Cyber ranges employ simulated network environments for cybersecurity training, testing, and experimentation, presenting realistic scenarios. By simulating real-world situations, cyber ranges offer hands-on experience, enhance problem-solving skills, and emphasize collaboration and teamwork, which are crucial in cybersecurity [25, 26]. Cyber ranges received much attention, offering safe, controlled environments to practice technical skills, problem-solving, and teamwork. To this end, Chouliaras et al. [27] conducted a systematic survey of existing cyber ranges to comprehend their characteristics and capabilities and identified best practices for their design. Langner et al. [28] proposed the usage of cyber ranges to create realistic and personalized cybersecurity learning environments. Finally, Yamin et al. [17] conducted a study using cyber ranges to model and execute cybersecurity exercise scenarios and proposed a taxonomy to classify these learning environments.

Despite the benefits of cyber ranges, the design and development can be challenging due to design complexity and maintenance needs [29, 30]. For example, when developing a cyber range, coordination between diverse development teams with additional expertise is often required for developing multidisciplinary scenarios across various sectors or technological domains [27, 31]. Therefore, it is imperative to discover methods to assist and enhance the design and development.

1.1 Contribution

This paper demonstrates the effectiveness of the NICE framework in enhancing scenario design and cyber range development, leading to a more authentic and adaptable training experience. In particular, this research provides the methodology, analysis, and results that can empower educators to develop or upgrade the cyber ranges by constructing relevant scenarios that align with educational frameworks. The key contributions are as follows:

- *An analysis of the NICE framework* to evaluate the effectiveness of the NICE framework in designing and implementing cyber ranges.
- *Propose a methodology for designing and developing cyber ranges using the NICE framework.* Additionally, the NICE framework is leveraged to identify potential areas for improvement or modification in the cyber range design.
- *Development of a NICE-by-design cyber range.* As part of this research, a cyber range is explicitly developed for SOC and blue teams to provide realistic and immersive learning experiences. The proposed NICE-by-design cyber range comprises 16 scenarios covering 5 Specialty Areas.

1.2 Related Work

Despite extensive research efforts to tackle the issue, a comprehensive and structured methodology for leveraging educational frameworks in designing and implementing

cyber ranges has yet to be established. Consequently, there is a gap in our understanding regarding the effective utilization of educational frameworks and their application in developing cyber ranges. While considerable attention has been dedicated to analyzing and comparing existing educational frameworks, further investigation is needed [11, 32]. The most important educational frameworks in cybersecurity have been analyzed by other researchers [11, 33, 34]. Furthermore, Jones et al. [35] used the NICE framework as a guide in developing core competencies for cybersecurity professionals. Nestler et al. [36] used the taxonomy of the NICE framework as a consultation mechanism to build the scenarios. González-Manzano et al. [5] analyzed 35 cybersecurity online courses that fit the NICE framework and proposed a model for designing practical cybersecurity courses.

Research has also been conducted regarding the use of the NICE framework for evaluation, with Dawson et al. [37] applying the framework to match their exercises. Furthermore, Karjalainen et al. [29] used the framework as a baseline to create questionnaires to assess the learners. The advantages of using the NICE framework as a comprehensive list of anticipated learning outcomes were highlighted in [38] and Saharinen et al. [39] proposed a model to design cybersecurity degree programs using the NICE framework.

Regarding evaluation methods for cyber ranges, researchers [40, 41] used the NIST Technical Guide for Information Security and Testing Assessment [42] as a reference point to identify the feature coverage in preparing content for cybersecurity training. The NIST Technical Guide provides a framework for technical information security tests and examination processes. Furthermore, several initiatives have been developed to provide hands-on training, like the NICE Challenge Project (NCP) [43] by NIST and the US National Security Agency (NSA[3]). NCP consists of real-world cybersecurity challenges set within virtualized business environments. Similarly, the San Bernardino California State University has mapped their exercises to the NICE framework [44] and Cyberbit [45] has developed a cybersecurity training and simulation platform for SOC teams. Finally, the University of Virginia [46] has developed a cyber range that aligns its existing courses with the NICE framework to provide a more structured and comprehensive training experience for trainees.

1.3 Structure

The rest of this paper is structured as follows. In Sect. 2, information on the educational frameworks and details of the NICE framework is provided. Section 3 outlines the methodology of this research paper, while Sect. 4 proposes the design and deployment steps for a NICE-by-design cyber range. Finally, Sect. 5 concludes the paper.

[3] https://www.nsa.gov/.

2 Background

2.1 Cybersecurity Educational Frameworks

Adopting a cybersecurity educational framework holds significant importance, influencing the content and structure of the curriculum. When making this decision, it is crucial to evaluate factors like alignment with the curriculum and trainees' learning requirements, the scope of the framework, and the support and resources it offers for implementation. Several cybersecurity education and training approaches exist alongside the NICE framework, such as the Cybersecurity Curriculum 2017 (CSEC2017) by the Joint Task Force on Cybersecurity Education. CSEC2017 emphasizes academic excellence across various cybersecurity domains and is backed by the NSA and Department of Homeland Security (DHS[4]), focusing on technical concepts [20, 47]. However, there are also differences between them; for instance, the NICE framework targets workforce training, while CSEC2017 emphasizes academic excellence. An overview of the most popular frameworks is as follows:

- *CIISec (Chartered Institute of Information Security* [48]) is a cyber and information security institution that offers education and certification programs in cybersecurity. CIISec provided a framework based on a set of competencies. The CIISec framework covers cybersecurity topics such as risk management, cyber law and ethics, and technical concepts, including network security and cryptography.
- *CyBOK* [49] is a framework by the International Association of Computer Science and Information Technology (IACSIT). CyBOK is quite popular as it provides a comprehensive body of knowledge for cybersecurity education and professional training.
- *CAE-cyber defence (CAE-CD)* [50] is a framework by the Canadian Centre for Cyber Security (CCCS) to support the development of cybersecurity education and training programs in Canada.
- *The Cybersecurity Curriculum 2017* by Joint Task Force (JTF) [51] is a framework developed by NIST to support the development of cybersecurity education and training programs in the US.
- *The European Cybersecurity Skills Framework (ECSF)* [52] is a draft framework developed by ENISA to support the development of cybersecurity education and training programs in Europe.

2.2 The NICE Framework

The NICE framework organizes cybersecurity requirements comprehensively through a modular structure with 4 main categories: workforce categories, specialty areas, work roles, and capability indicators [6]. The NICE has undergone several

[4] https://www.dhs.gov/.

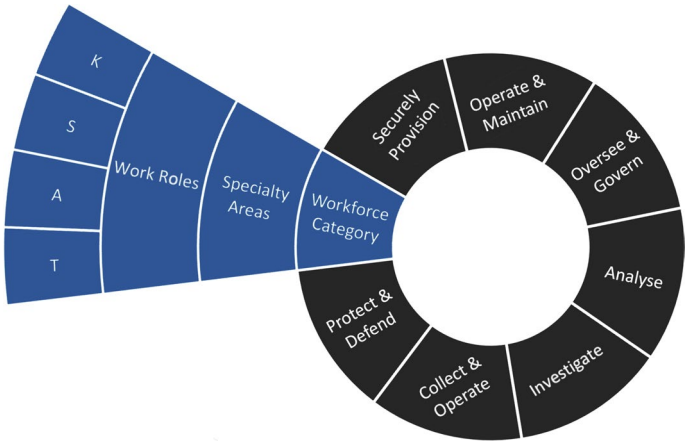

Fig. 1 The main building blocks of the NICE framework. Consider that the Abilities (A) and Skills (S) were merged in the latest framework version

incremental updates, and in this paper, we focus on the version published in 2017 as it remains the most popular and widely used. However, it is important to note that new versions of NICE have been published since 2020. The taxonomy of the framework was initially defined in the first editions of the framework using the KSAT (Knowledge, Skills, Abilities, and Tasks) taxonomy, but in the latest version [7, 53], they were revised to TKS (Tasks, Knowledge, and Skills), merging the Abilities (A) and Skills (S).

Workforce Categories are broad groupings containing 7 workforce categories broken down into 33 Specialty Areas. Specialty Areas focus on specific expertise within each Workforce category. The corresponding Specialty Areas include 52 work roles (see Fig. 1). The TKS indicators specified in the framework are matched to the Work Roles in a modular manner, meaning that multiple TKS may apply to a single work role. The TKS taxonomy is as follows.

1. *Tasks (T)*, are specifically defined pieces of work that fulfil part of a specific work role in a specialty area. For example, a task might include applying secure code documentation (T0014) or developing content for cyber defence tools (T0020). Tasks (T) are specific objectives that must be completed to cover a work role.
2. *Knowledge (K)*, is a body of information necessary to perform a specific function in cybersecurity. For example, Knowledge (K) of computer networking concepts and protocols and network security methodologies (K0001) could be considered necessary to perform vulnerability assessments and network diagnostics, which are important for the work role of "Cyber Defence Analyst—PR-CDA-001." Some TKS indicate high importance for different work roles and specialty areas across the different workforce categories.
3. *Skills (S)*, are observable competencies that are learned through the use of Knowledge (K) and focus on the actions of the learner. For example, a person might develop or acquire the skill of identifying, capturing, containing and reporting

malware (S0003) or developing and deploying signatures (S0020). Skills (S) are more specific and action-oriented than Knowledge (K) and are developed through practice and experience. They represent the ability to perform specific actions and Tasks (T) and are typically more practical. The capability indicator of Abilities (A) has been merged with Skills (S) in the latest version of the NICE framework.[5]

3 Methodology

While the NICE framework is selected in this research for the detailed coverage of cybersecurity topics [33, 54], there's no one-size-fits-all educational approach. The NICE framework was chosen for its comprehensive structure and focus on capability indicators. These indicators aid scenario design, ensuring exposure to relevant cybersecurity challenges. NICE also enables thorough scenario assessment, aligns with real-world job roles, fosters collaboration among developers, and stays updated with evolving trends [11, 33, 34].

The proposed NICE-by-design development process, which is composed of 3 steps, begins with searching the NICE framework for applicable Workforce Categories and relevant Specialty Areas that align with our learning objectives. The next step involves designing the initial technical deployment and architecture of the cyber range, followed by scenario design. The third and final step focuses on evaluating the scenarios using capability indicators from the NICE framework to facilitate potential updates to the developed scenarios.

Step I: Define the learning goals The learning goals are defined by selecting the relevant workforce categories and specialty areas. This process involves setting high-level goals. This process aids in selecting a list of potential work roles to be covered by the cyber range, and the relevant capability indicators will create a roadmap for the scenario design.

Step II: Architecture and scenario design This step focuses on defining the initial architecture and topology of the cyber range along with the creation of the relevant scenarios. Initially, when setting up a cyber range, its architecture is defined based on specific learning objectives, the types of cyber threats to be simulated, the available resources, and the target audience. This initial architecture serves as the foundation for the design and implementation. Scenario design involves creating realistic cyberattack scenarios in the cyber range. As the scenario design progresses, it may become apparent that certain aspects of the cyber range architecture need to be updated or modified to support the scenarios better and ensure the effectiveness of the training.

As a follow-up to Step I, the selected Specialty Area(s) are correlated with smaller scenarios to formulate the learning path. Table 1 serves as a detailed mapping tool during scenario design, aligning learning goals with the capabilities developed through exercises within the cyber range.

[5] https://niccs.cisa.gov/Workforce-development/nice-framework.

Table 1 Reference table to match the scenarios with the NICE framework and the TKS

NICE framework	Description
Workforce category	Workforce category that each scenario could cover
Specialty area	Potential specialty areas covered by each scenario
Work role name/ID	Corresponding work role covered from each scenario
Tasks (T)	Specific pieces of work that fulfil a role in a specialty area. Tasks (T) are defined objectives that must be completed to cover a work role
Knowledge (K)	Body of information necessary to perform a specific function in cybersecurity. Knowledge (K) is acquired through practice and is important across various work roles and specialty areas
Skills (S)	Skills (S) are practical, action-oriented abilities developed through practice and experience, enabling individuals to perform specific tasks effectively
Extra coverage	Additional TKS that can be covered with small updates on each scenario

Step III: Evaluation This step is used to calculate the total coverage of capability indicators and assess if scenarios cover any of the selected Work Roles. Evaluating helps pinpoint gaps, enabling iterative improvements to meet learning goals. Evaluation metrics are calculated using Eq. (1):

$$Coverage = \frac{Total\ TKS\ covered\ within\ the\ Scenarios\ per\ WorkRole}{Total\ TKS\ covered\ by\ NICE\ per\ WorkRole} \times 100\% \quad (1)$$

The above equation calculates numerically the coverage of a specific set of TKS per work role. It divides the number of TKS represented in developed scenarios by the total number of TKS for the work role. The information collected during the evaluation can be used to redesign or update the scenarios in Step II of the methodology. For example, if the scenarios for a specific Work Role (e.g., PR-CDA-001) in the proposed scenarios below have 8 Tasks covered, while the total tasks for the Work Role PR-CDA-001 by NICE is 20, as mentioned in Eq. (1), then the coverage is 8/20 multiplied by 100 = 40%. The evaluation can be used to identify missing elements in the developed scenarios and provide suggestions for updates or extensions to improve their effectiveness in teaching cybersecurity concepts.

4 A Cyber Range for SOC Teams

The cyber range emphasizes Blue Team roles, especially those in Security Operation Centers (SOCs), focusing on protecting, defending, operating, and maintaining information systems. It is structured around two workforce categories: (1) protect and defend (PR) and (2) operate and maintain (OM).

4.1 Learning Goals: Specialty Areas and Work Roles Covered by the Cyber Range

We assume that the cyber range that will be designed will primarily cover the following Specialty Areas. Detailed information on Specialty Areas can be found in the Appendixes 1–5.

- *Specialty area 01—cyber defence analysis (CDA):* CDA involves identifying, analyzing, and reporting security events in simulated networks or systems. Capability indicators include analyzing network traffic, implementing security controls, conducting vulnerability assessments, managing incidents, evaluating security effectiveness, and providing technical guidance. The relevant work role is the cyber defence analyst (PR-CDA-001).
- *Specialty area 02—systems administration (ADM):* ADM involves server and firewall configuration, troubleshooting, and maintenance for smooth operations. It complements other cybersecurity topics and supports system and network administration. The relevant work role is the system administrator (OM-ADM-001).
- *Specialty area 03—network services (NET):* NET focuses on managing networks, firewalls, and configuring network devices for security. Tasks include planning, implementing, and deploying hardware and virtual environments and configuring devices to reduce cyberattack risks and protect organization data and assets. The relevant work role is the network operations specialist (OM-NET-001).
- *Specialty area 04—cyber defence infrastructure support (INF):* INF aligns with analyzing data from cyber defence tools to mitigate threats. It includes understanding tool usage, analyzing events, and evaluating cyber defence security. The relevant work role is the cyber defence infrastructure support specialist (PR-INF-001).
- *Specialty area 05—vulnerability assessment and management (VAM):* VAM identifies vulnerabilities, performs assessments and implements measures to mitigate risks. It is suitable for beginners and focuses on vulnerability and asset management principles. The relevant work role is the vulnerability assessment analyst (PR-VAM-001).

From the above, the work role to be covered is the cyber defence analyst (PR-CDA-001). However, the cyber range could cover other Work roles from the above specialty areas. This is to be evaluated in Sect. 4.3. The NICE-by-design cyber range includes 16 cybersecurity scenarios described in the previous section. The overall learning coverage of the scenarios considering the NICE framework is presented in Table 2.

As shown in Table 2, the Specialty areas covered include the cybersecurity defence analysis (CDA) is covered mostly, followed by defence infrastructure support (INF) and system administration (ADM). The cyber range also includes a scenario focused on the work role of a vulnerability assessment analyst, which covers the topic of vulnerability assessment and packet capturing.

Table 2 Proposed scenarios coverage of the cyber range per workforce categories, speciality areas and work role

Workforce categories from NICE	Num. of scenarios
Protect and defend (PR)	7
Operate and maintain (OM)	10
Specialty areas	
Cybersecurity defence analysis (CDA)	7
Systems administration (ADM)	9
Cybersecurity defence infrastructure support (INF)	3
Vulnerability assessment and management (VAM)	1
Network services (NET)	1
Work roles	
Cyber defence analyst (PR-CDA-001)	7
System administrator (OM-ADM-001)	9
Cyber defence infrastructure support specialist (PR-INF-001)	3
Vulnerability assessment analyst (PR-VAM-001)	1
Network operations specialist (OM-NET-001)	1

4.2 Architecture and Scenario Design

The architecture of the cyber range has been defined based on the potential specialty areas that are more relevant. However, as the scenario design progresses, adjustments to the architecture will be necessary.

4.2.1 Topology and Equipment Configuration

The cyber range was developed using two dedicated HP ProLiant servers with VMware ESXi 6.5 as the hypervisor. This approach enabled the efficient creation of multiple virtual machines on each server, optimizing resource usage and cost-effectiveness. The servers were configured with RAID1 for redundancy, ensuring continuity and minimizing the risk of hardware defects. This setup made the cyber range flexible and reliable for simulating and testing cybersecurity scenarios. For further details, see Fig. 2.

Table 3 provides an overview of its equipment, deployment options, and relevant scenarios specifying each equipment's purpose, role, operating system version, and applicable scenarios. More specifically, the following hardware and software/services are utilized:

- *AttackVM (Kali Linux):* An external virtual machine running KALI Linux, a widespread Linux distribution for offensive security, was used as the primary endpoint for trainees in most scenarios.

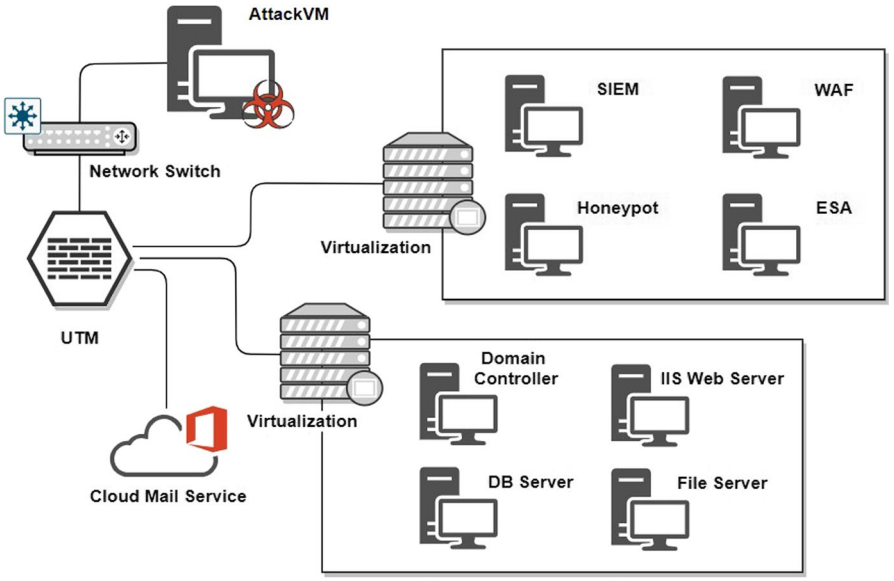

Fig. 2 Topology of the developed cyber range focused on SOC and blue teams

Table 3 Equipment configuration and the relevant scenarios

Equipment type	Deployment option	Relevant scenarios
Hardware	HP ProLiant servers with VMware ESXi 6.5	All scenarios
	Network Switch: Cisco 2960	SOC01
	Unified Threat Management: Checkpoint	SOC02
Appliance	AttackVM: Kali Linux	All scenarios
	Web Application Firewall: Apache Mod Security	SOC05-07
	Domain Controllers (x2): MS Server 2016	SOC03, 04
	Web Servers (x2): Internet Information Server (IIS), File Servers (x2): MS Server 2012	SOC06-09
	Database Servers: MS SQL Server 2012 (x2)	SOC10, 11
	Mail Gateway: MS Server 2008 R2 (x2)	SOC13
	Email Security Appliance: Cisco ESA	SOC12
	Honeypot: T-Pot	SOC14
	Security Information and Event Management (SIEM): IBM QRadar	SOC15
Cloud services	Cloud-based Email Service: MS Office 365	SOC12

- *Network Switch (Cisco 2960):* A hardware network switch was used to offer a more immersive experience and replicate a realistic environment. It can be replaced by a virtual switch in a more cost-effective approach, but this may have some functional limitations. It was used in the SOC01 scenario.

- *UTM—Unified Threat Management (Checkpoint UTM 2200):* Check Point UTM 2200 combines networking technologies with high-performance multicore capabilities to enable security features in a small office. It was used in the SOC02 scenario.
- *Virtualization (VMware ESXi):* VMware ESXi is a virtualization technology that maintains flexibility and portability features. Its ability to efficiently use virtual images to recover and retrieve a snapshot of deployed systems is crucial and was used in all scenarios.
- *SIEM (IBM Qradar):* IBM Qradar is a SIEM that helps security teams detect, prioritize, and respond to threats throughout the cyber range.
- *Honeypot (T-Pot):* T-Pot is a collection of honeypots brought together by T-Mobile, with easy management and a user-friendly interface.
- *WAF—Web Application Firewall (Apache Mod Security):* Apache Mod Security is an open-source Apache Module that offers protection against web application attacks and relies on pattern matching with a list of rules and the corresponding Rule IDs.
- *AESA—Email Security Appliance (Cisco ESA):* Cisco ESA is a solution for email protection, providing modules such as anti-spam and antivirus.
- *Domain Controller, DB Server, File Server, and IIS web server protection (MS Server 2008 R2, 2012 and 2016):* A cluster of virtual ESXi images used to maintain the core functionalities of the cyber range. These included a Domain Server running MS Server 2016, an IIS web server running MS Server 2012, and a Mail Gateway running Windows Server 2008 R2.
- *Cloud Mail Service (MS Office 365):* The trial version of Office 365 was selected for use in the cyber range as a cloud mail service. This allows trainees to engage in the setup of email services and see how administrators create new mailboxes and take actions to mitigate attacks from incoming emails.

4.2.2 Scenario Design Using the NICE Framework

The cyber range consists of 16 scenarios (SOC01–SOC16) designed to increase in difficulty progressively, considering any prerequisites necessary for understanding foundational learning topics. This allows trainees to gradually build up, starting with basic concepts and moving on to more advanced topics.

Cyber range scenario 01 (SOC01)—network configuration and analysis. SOC01 regards configuring a network switch and trunk ports and defining various network groups in a Virtual Local Area Network (VLAN). The scenario also includes an introduction to net flows and instructions on how to forward the data to the SIEM for further analysis (Table 4).

The scenario involves network topology analysis and an understanding of data flows and requires an understanding of network security, traffic analysis, and secure network architecture. The scenario addresses how configurations could affect network security.

Table 4 Scenario 01 (SOC01)—network configuration and analysis

NICE	Matching to the scenario
Workforce category	Protect and defend (PR), operate and maintain (OM)
Specialty area	Cybersecurity defence analysis (CDA), network services (NET), cybersecurity defence infrastructure support (INF)
Work role name/ID	Cyber defence analyst (PR-CDA-001), network operations specialist (OM-NET-001), cyber defence infrastructure support specialist (PR-INF-001)
Tasks (T)	Understand the structure and layout of networks, analyze and interpret network traffic, understand different networking protocols and technologies, and identify potential issues or vulnerabilities (T0291, T0035, T0081, T0125, T0126, T0129, T0153, T0232)
Knowledge (K)	Network security, through traffic analysis and implementing security policies, design secure network architectures. Technical and organizational aspects of network security to protect networks from cyber threats (K0001, K0033, K0059, K0060, K0061, K0075, K0098, K0104, K0111, K0112, K0113, K0157, K0179, K0221, K0300, K0303, K0318, K0332)
Skills (S)	Analyze network traffic, implement security policies, manage network security incidents, apply cybersecurity principles and technologies, conduct vulnerability assessments (S0027, S0036, S0041, S0056, S0084, S0162)
Extra coverage	Evaluate the network architecture and identify software vulnerabilities to enhance security (K0011, K0029, K0255, K0296, K0516, K0555)

Table 5 Scenario 02 (SOC02)—unified threat management (UTM)

NICE	Matching to the scenario
Workforce category	Protect and defend (PR)
Specialty area	Cybersecurity defence analysis (CDA), cybersecurity defence infrastructure support (INF)
Work role name/ID	Cyber defence analyst (PR-CDA-001), cyber defence infrastructure support specialist (PR-INF-001)
Tasks (T)	Examine and evaluate intrusion alerts, vulnerabilities, and malware to determine their potential impact (T0023, T0088, T0160, T0259, T0260, T0290, T0295, T0296, T0297, T0310, T0438)
Knowledge (K)	Evaluate the network security and topology, understand the OSI model, and implement intrusion detection-prevention systems (IDS/IPS) and firewalls to enhance security (K0001, K0005, K0013, K0046, K0049, K0058, K0059, K0060, K0061, K0070, K0075 K0098, K0104, K0106, K0110, K0112, K0113, K0157, K0160, K0161, K0179, K0191, K0221, K0300, K0318, K0324, K0332, K0624)
Skills (S)	Analyze network vulnerabilities and intrusions (S0020, S0025, S0027, S0036, S0076, S0078, S0079, S0081, S0084, S0096, S0131, S0156)
Extra coverage	Application, technology, network and file vulnerabilities, IT architecture, malware detection (K0009, K0100, K0115, K0187, K0189, K0314, K0326, K0392, K0471, K0481, K0488)

Deployment: The deployment uses physical and virtual components and utilizes Cisco's VLAN trunking protocol (VTP) for management and user authentication. VTP simplifies VLAN management by centrally distributing information

Table 6 Scenarios 03 and 04 (SOC03, SOC04)—domain controller

NICE	Matching to the scenario
Workforce category	Operate and maintain (OM)
Specialty area	Systems administration (ADM)
Work role name/ID	System administrator (OM-ADM-001)
Tasks (T)	Manage and maintain systems and servers, conduct system and security maintenance, implement and enforce local network usage policies, manage system resources, monitor and system configuration, oversee installation and support of system components (T0136, T0144, T0186, T0418, T0420, T0431, T0435, T0461, T0498, T0501, T0507)
Knowledge (K)	Understand authentication methods, security policies, shielding the systems of the organization, network protocols, protocols and vulnerability management used in Windows systems (K0005, K0007, K0019, K0033, K0059, K0060, K0070, K0106, K0157, K0167, K0192, K0224, K0332)
Skills (S)	Implement cybersecurity and privacy measures that meet the confidentiality, integrity, availability, authentication, and non-repudiation needs of an organization (S0007, S0121, S0367, S0043, S0153) -
Extra coverage	system, network and OS hardening, security policies, network tools (K0077, K0158, K0205)

to all switches and streamlining configuration and administration tasks. It also provides user management features and authentication log files for tracking changes in VLAN configuration.

Cyber range scenario 02 (SOC02)—unified threat management (UTM). UTM (unified threat management) refers to a security device or service that protects a network by providing multiple security features, such as antivirus, content filtering, email filtering, and web filtering. SOC02 focuses on the configuration of a firewall and the differences between network protection, intrusion prevention, and sandboxing (Table 5).

The scenario provides a realistic environment for intrusion detection, vulnerability analysis, and malware. It also offers hands-on experience in network security and topology, theoretical concepts of the OSI model, firewall configuration, and the utilization of intrusion detection and prevention systems.

Deployment: The deployment involves a firewall that has several security features enabled, including port and traffic filtering, IDS/IPS, anti-bot protection, antivirus protection, threat emulation, monitoring, and Quality of Service (QoS).

Cyber range scenarios 03 and 04 (SOC03, SOC04)—domain controller. In SOC03 and SOC04, a domain is created for participants to learn about user management and configure security policies and security groups. Security groups are essential for maintaining appropriate access rights to sensitive data. The configuration options related to the domain enable trainees to comprehend the significance of security hardening and learn the security and privacy principles that should govern system processes. These scenarios focus on security hardening, security configuration assessments, and other fundamental concepts from the specialty area, operate and maintain (OM).

Table 7 Scenario 05 (SOC05)—web application firewall (WAF)

NICE	Matching to the scenario
Workforce category	Protect and defend (PR)
Specialty area	Cybersecurity defence analysis (CDA), cybersecurity defence infrastructure support (INF)
Work role name/ID	Cyber defence analyst (PR-CDA-001), cyber defence infrastructure support specialist (PR-INF-001)
Tasks (T)	Identify and analyze vulnerabilities and how to exploit them in web applications (T0088, T0259, T0260, T0438)
Knowledge (K)	Cyberattacks on web applications and ways to address them (K0001, K0005, K0013, K0042, K0049, K0058, K0059, K0060, K0061, K0070, K0075, K0098, K0106, K0110, K0112, K0157, K0160, K0161, K0192, K0318, K0624)
Skills (S)	Understand the functionality of a security system to deal with attacks on web applications (S0027, S0036, S0078)
Extra coverage	Exploits and network threats, packet analysis (K0115, S0120, K0129, K0326, K0612, S0046, S0084)

SOC03 and SOC04 focus on domain controllers and the role of system administrator. This includes an understanding of authentication methods, security policies, and methods to protect the systems of an organization, as well as familiarity with network protocols and vulnerability management in Windows systems. It also covers system, network, OS hardening, and security policy enforcement.

Deployment: In this scenario (Table 6), domain controllers are installed on server hosts with active directories enabled. A domain controller manages network access and security policies, authenticating and authorizing users and devices. Active Directory stores and manages network object information, facilitating resource access management and security policy enforcement. When installed on a server host with Active Directory enabled, a domain controller regulates network access, enforces security policies, and stores network object data.

Cyber Range Scenario 05 (SOC05)—Web Application Firewall (WAF). SOC05 focus on Web Application Firewall (WAF), which safeguards web applications by filtering and monitoring HTTP traffic. The scenario involves identifying and analyzing vulnerabilities in web applications, providing additional coverage on web exploits, network threats, and packet analysis (Table 7).

Potential cyberattacks targeting web applications could include cross-site forgery, cross-site scripting (XSS), file inclusion, and SQL injection. A shield of protection is placed between the web application and the Internet when a WAF is deployed. Finally, the differences between signature-based detection and pattern-based attacks are covered in this scenario.

Deployment: Enabling logging on a web server for monitoring and detecting cyberattacks is the primary step of the deployment. Security logs provide valuable insights into potential threats, allowing administrators to take necessary actions to protect servers and networks. Regularly reviewing these logs helps identify suspicious activity, like failed login attempts or unauthorized access, aiding in preventing cyberattacks and identifying vulnerabilities. It is essential to establish a process for

Table 8 Scenarios 06 and 07 (SOC06, SOC07)—web server

NICE	Matching to the scenario
Workforce category	Operate and maintain (OM)
Specialty area	Systems administration (ADM)
Work role name/ID	System administrator (OM-ADM-00)
Tasks (T)	Management and maintenance of systems and servers (T0054, T0144, T0418, T0501, T0507)
Knowledge (K)	Security hardening of the organisation's systems. Understand protocols, network ports and vulnerability management (K0005, K0059, K0060, K0070, K0077, K0088, K0100, K0106, K0130, K0158, K0167, K0280, K0192)
Skills (S)	Analyze and interpret data and information, identify trends and patterns, and make informed decisions based on that analysis (S0016, S0043, S0073, S0076, S0143, S0144, S0151, S0154, S0155, S0121)
Extra coverage	system, network and OS hardening techniques, server and client OS, web services and network tools (K0077, K0105, S0121, K0205, K0318, K0332, K0398)

regularly reviewing logs and collaborating with security professionals or incident response teams to investigate and address potential threats.

Cyber Range scenarios 06 and 07 (SOC06, SOC07)—web server. SOC06 and SOC07 regard the Internet Information Server (IIS) and the best practices for configuring its services. Security hardening on IIS involves going beyond default settings, such as enhancing cookie security and blocking non-HTTPS connections. Properly configuring cryptography settings is also considered important. The details of this scenario are provided in Table 8.

These scenarios (SOC06, SOC07) focus on the role of the system administrator and the maintenance of the web server. This includes understanding the security hardening of an organisation's systems and familiarity with protocols, network ports, and vulnerability management. Additional coverage for this scenario includes system, network, and OS hardening techniques, familiarity with server and client OS, and web services.

Deployment: A web server with IIS enabled is a server running Microsoft's Internet Information Services software, allowing it to host and serve web content over the Internet. IIS facilitates hosting various types of content, including static pages, images, and dynamic applications or APIs. Enabling IIS involves installing and configuring the software on the server.

Cyber range scenarios 08 and 09 (SOC08, SOC09)—file server. SOC08 and SOC09 regard configuring security privileges and shared folders. They also learn about the importance of auditing and monitoring access rights and methods for detecting potential data leakage or ransomware infections. This may involve monitoring active directories for signs of compromise and using a solid event log system to detect cybersecurity incidents early in a cyberattack. The details of these scenarios are provided in Table 9.

The focus of these scenarios (SOC08, SOC09) is on the role of the system administrator and the maintenance of a file server. This includes an understanding of how to secure the systems of an organization, as well as familiarity with network

Table 9 Scenarios 08 and 09 (SOC08, SOC09)—file server

NICE	Matching to the scenario
Workforce category	Operate and maintain (OM)
Specialty area	Systems administration (ADM)
Work role name/ID	System administrator (OM-ADM-001)
Tasks (T)	Administer test beds, test and evaluate components, including applications, hardware, and access controls (T0054, T0144, T0418, T0420, T0435, T0501)
Knowledge (K)	Secure the systems of the organization, understand network protocols, execute vulnerability management (K0005, K0059, K0060, K0070, K0106, K0117, K0167, K0192)
Skills (S)	Manage and maintain systems, with account maintenance, data backups, and installation or configuration of software (S0043, S0158)
Extra coverage	System, network and OS hardening, Knowledge (K) on network services (K0077, K0205)

Table 10 Scenarios 10 and 11 (SOC10, SOC11)—database server

NICE	Matching to the scenario
Workforce category	Operate and maintain (OM)
Specialty area	Systems administration (ADM)
Work role name/ID	System administrator (OM-ADM-001)
Tasks (T)	Maintain database systems performing backups and administer test beds (T0137, T0152, T0162, T0420, T0490, T0867)
Knowledge (K)	Security features on database systems, secure systems of the organization, understand network protocols, vulnerability management (K0005, K0023, K0024, K0059, K0060, K0070, K0095, K0106, K0167, K0192, K0419)
Skills (S)	Maintain databases using backup, restore, or other mechanisms and maintain the relevant software packages (S0042, S0292)
Extra coverage	Query languages and basic system, network, and OS hardening techniques (K0069, K0205)

protocols and vulnerability management. Extra coverage for this scenario regards system, network, OS hardening, and familiarity with network services.

Deployment: Setting up a file server involves configuring access rights to manage file sharing securely. This includes creating user accounts, assigning permissions, and implementing security measures like encryption and authentication.

Cyber range scenarios 10 and 11 (SOC10, SOC11)—database server. SOC10 and SOC11 focus on hands-on experience with SQL databases and learn about various cyberattacks, such as SQL injection and response actions. To do this, they use server-level audits to extract log files and events from the SQL Server, which are stored in the default data directory of the SQL service. They also use the log file viewer to examine the retrieved log files. The details of these scenarios are provided in Table 10.

The scenarios (SOC10, SOC11) focus on the role of the system administrator and the maintenance of a database server. They involve an understanding of the security

Table 11 Scenario 12 (SOC12)—Email service

NICE	Matching to the scenario
Workforce category	Operate and maintain (OM)
Specialty area	Systems administration (ADM)
Work role name/ID	System administrator (OM-ADM-001)
Tasks (T)	Administer test beds, test and evaluate components, including applications, hardware, and access controls (T0420)
Knowledge (K)	Collect, view, and analyze metadata from internet applications like email, common networking and routing protocols, services, and how they facilitate communication within networks (K0131, K0059, K0136, K0444, K0447, K0565)
Skills (S)	Identify data such as usernames, passwords, email addresses, and IP ranges, analyze SMTP header information and other data about domain servers and mail servers (S0054, S0264, S0295)
Extra coverage	Not defined

features of database systems, as well as familiarity with the security systems of the organization, network protocols, and vulnerability management. Additional coverage can be relevant to network and OS hardening and familiarity with query languages and network tools.

Deployment: SQL server, a Microsoft RDBMS, are to be deployed on the infrastructure with enabled logs. These logs track activity, aiding in identifying issues and security breaches and facilitating troubleshooting and maintenance.

Cyber range scenario 12 (SOC12)—Email service. SOC12 provides the opportunity to practice with mail servers using audit logs to detect potential cyber threats. The scenario includes integrating with Threat Intelligence, involving a SIEM, analysis of the SMTP protocol, and demonstrating phishing incidents. Trainees must enable audit logs, configure SIEM integration, and analyze relevant log files. Cloud-based email services with centralized audit logging support the training process. Overall, the scenario aims to illustrate the significance of audit logs in detecting and preventing cyber threats (Table 11).

The scenario concerns understanding modern and emerging information technology and cybersecurity technologies. It also requires additional information regarding cookie management, webmail, attack methods, and exploitation tools.

Deployment: A cloud-based service configures and enables audit logs while verifying other security options. Examples include: (1) Amazon Web Services (AWS) with AWS Config for tracking resource configuration changes. (2) Microsoft Azure with Azure Monitor for enabling audit logs and tracking resource changes. (3) Google Cloud Platform with Cloud Audit Logs for enabling audit logs and tracking resource changes. Properly configuring and enabling audit logs is crucial for tracking resource changes and detecting security issues.

Cyber range scenario 13 (SOC13)—Email gateway. SOC13 involves implementing email communication defence mechanisms and utilizing Harmony Email and Collaboration to create a dashboard for threat monitoring and enterprise security enhancement. Harmony Email and Collaboration is a software platform offering email and collaboration services. Its use suggests the configured email gateway is

Table 12 Scenario 13 (SOC13)—Email gateway

NICE	Matching to the scenario
Workforce category	Protect and defend (PR)
Specialty area	Cybersecurity defence analysis (CDA) and infrastructure support (INF)
Work role name/ID	Cyber defence analyst (PR-CDA-001), Cyber Defence Infrastructure Support Specialist (PR-INF-001)
Tasks (T)	Analyze data from various sources and identify security events and issues, discover security vulnerabilities and overall security posture (T0088, T0259, T0260, T0420, T0438)
Knowledge (K)	Understand the latest technologies for protecting organizations from attacks on the cloud (K0001, K0013, K0049, K0059, K0060, K0061, K0075, K0098, K0106, K0110, K0112, K0116, K0157, K0318)
Skills (S)	Engage to mail gateway services and how the security systems affect the organization (S0027, S0036)
Extra coverage	Not defined

Table 13 Scenario 14 (SOC14)—honeypots/deception traps

NICE	Matching to the scenario
Workforce category	Protect and defend (PR)
Specialty area	Cybersecurity defence analysis (CDA)
Work role name/ID	Cyber defence analyst (PR-CDA-001)
Tasks (T)	Detect, analyze and mitigate threats before they affect the infrastructure (T0088, T0138, T0259)
Knowledge (K)	Detection and analysis of cyber threats before infecting the organization (K0001, K0013, K0040, K0046, K0049, K0059, K0060, K0061, K0070, K0075, K0098, K0106, K0110, K0112, K0160, K0161, K0192, K0318)
Skills (S)	Engage in security systems or software tools that the organizations use (S0027, S0036)
Extra coverage	Not defined

likely a cloud-based service by Harmony. The dashboard tracks identified threats like malware, spam, and phishing attempts, enabling actions to mitigate these threats and enhance enterprise security (Table 12).

The scenario covers the understanding of the latest technologies for protecting organizations from attacks on the cloud. The participants should be able to engage with mail gateway services and apply defending mechanisms relevant to email services. A dashboard is created using Harmony Email and Collaboration [55] to monitor identified threats and improve enterprise security.

Deployment: A Virtual Image to host the Checkpoint Harmony Cloud Service, configured to interact with the hosted email service. The Checkpoint Harmony Cloud Service is a security software platform that provides a variety of security features, such as firewall protection, IDS/IPS, and content filtering, for cloud-based environments.

Table 14 Scenario 15 (SOC15)—security information and event management (SIEM)

NICE	Matching to the scenario
Workforce category	Protect and defend (PR)
Specialty area	Cybersecurity defence analysis (CDA)
Work role name/ID	Cyber defence analyst (PR-CDA-001)
Tasks (T)	Collect and analyze security logs from various sources, create security alerts and identify potential security threats. Evaluate the impact of these threats and implement appropriate measures as mitigation (T0023, T0088, T0155, T0164, T0166, T0187, T0198, T0214, T0258, T0259, T0260, T0261, T0290, T0291, T0293, T0294, T0295, T0297, T0299, T0310, T0332, T0469, T0470, T0504)
Knowledge (K)	Collect and analyze security logs from various sources and create security alerts, and utilize Knowledge (K) of operating systems, malware analysis, and threat detection to effectively secure a network (K0001, K0013, K0040, K0042, K0046, K0058, K0059, K0060, K0061, K0070, K0075, K0098, K0106, K0107, K0110, K0142, K0143, K0160, K0161, K0177, K0192, K0224, K0301, K0318, K0332)
Skills (S)	Examination of network traffic and performance using network management tools to identify patterns, as well as utilizing log correlation techniques to detect potential security incidents (S0004, S0027, S0036, S0056, S0063, S0078, S0079, S0054)
Extra coverage	IT architecture, event correlation, hacking methods, root cause analysis, vulnerability and threat analysis (K0100, K0145, K0310, K0343, K0493, K0612, S0001, S0092)

Cyber range scenario 14 (SOC14)—honeypots. SOC14 focuses on honeypots and, more specifically, on using T-Pot and TRAPX-Deception Grid [56] as tools to detect and attract potential cyberattacks. These tools create a virtual trap to identify and track potential threats and are used to enhance the overall security of the system. This scenario focuses on the configuration and use of these security mechanisms (Table 13).

This scenario requires enabling the detection, analysis, and mitigation of threats before they can affect the infrastructure. The requirements are to understand how to detect and analyze cyber threats before they infect the organization.

Deployment: A virtual image with a honeypot is a virtual environment running honeypot software to attract and trap malicious actors. It is a standalone system organisations use to monitor and detect cyber threats. A best practice is to deploy the honeypot only on the specific virtual image without additional services unless necessary for security reasons, ensuring its effectiveness. Proper configuration and maintenance are also crucial regarding threat detection.

Cyber range scenario 15 (SOC15)—security information and event management. SOC15 focuses on the SIEM to collect and analyze security logs, aiding in threat detection through alert generation. Trainees must understand SIEM usage and management, which integrates with other scenarios for a comprehensive security approach (Table 14).

This scenario requires collecting and analyzing security logs from various sources and creating security alerts. It requires understanding operating systems, malware analysis, and threat detection using security logs and recognising

Table 15 Scenario 16 (SOC16)—vulnerability assessment and packet capturing

NICE	Matching to the scenario
Workforce category	Protect and defend (PR)
Specialty area	Cybersecurity defence analysis (CDA), vulnerability assessment and management (VAM)
Work role name/ID	Cyber defence analyst (PR-CDA-001), vulnerability assessment analyst (PR-VAM-001)
Tasks (T)	Use Kali Linux, identify and apply security countermeasures (T0023, T0259, T0291, T0292, T0295, T0297, T0299)
Knowledge (K)	Understand attack methods and familiarize with Unix (K0005, K0013, K0059, K0060, K0070, K0106, K0110, K0111, K0116, K0160, K0161, K0177, K0192, K0290, K0300, K0301, K0318, K0332, K0339, K0342, K0344, K0624)
Skills (S)	Vulnerability enumeration and monitoring network traffic to analyze and reconstruct network activity (S001, S0056, S0057, S0078, S0079, S0081, S0137, S0156, S0167, S0241, S0294, S0364)
Extra coverage	Hacking methods, obfuscation, webmail, file-type abuse, malware detection and network vulnerabilities (K0009, K0115, K0119, K0129, K0131, K0187, K0189, K0234, K0296, K0310, K0314, K0362, K0392, K0480, K0481, K0493, K0536)

Table 16 Matching coverage of the cyber range with the NICE framework for the most relevant work roles, namely PR-CDA-001, OM-ADM-001, OM-NET-001, PR-INF-001, PR-VAM-001

Work role	Tasks (T)	Knowledge (K)	Skills (S)
PR-CDA-001	67.64%	64.28%	73.33%
OM-ADM-001	55.55%	44.82%	78.57%
OM-NET-001	72.72%	30.76%	54.54%
PR-INF-001	33.33%	54.16%	44.44%
PR-VAM-001	00.00%	45.71%	50.00%

security incidents through log correlation. Additional areas relevant to this scenario include IT architecture, event correlation, hacking methods, root cause analysis, vulnerability and threat analysis.

Deployment: A virtual image with a SIEM system is likely a virtual environment running SIEM software configured to collect logs from monitored services. SIEM serves as a central platform to aggregate and analyze security-related log data from various sources, aiding in threat detection and response. Organizations deploy and configure SIEM on virtual images to collect and analyze security logs from monitored services, enhancing threat detection capabilities.

Scenario 16 (SOC16)—vulnerability assessment and packet capturing. SOC16 specializes and presents the most common software tools and techniques attackers use, including recognising and categorising different vulnerabilities and associated attacks (Table 15).

The scenario provides an understanding of how attackers operate and how to defend against potential attacks. It could involve training or exercises focused on identifying and responding to vulnerabilities and cyberattacks. Additionally,

it can cover obfuscation methods, webmail, file-type abuse, malware detection, and network vulnerabilities.

Deployment: A laptop or virtual image with Kali Linux pre-installed offers a cybersecurity offensive toolkit for learning about vulnerabilities and responding to attacks. Kali Linux is designed for security testing and forensic analysis, providing various cybersecurity tools and resources.

4.3 Evaluation

In this section, we present the evaluation results of the presented scenarios. As shown in Table 16, numerical results were derived based on Eq. (1), presenting which Work Roles were adequately covered in the cyber range according to the TKS taxonomy.

We observe that the proposed NICE-by-design cyber range covers sufficiently the Work Role PR-CDA-001 and OM-ADM-001. For example the Work Role PR-CDA-001 is covered by 7 NICE-by-design scenarios (SOC01, SOC02, SOC05, SOC13-SOC16). The total Tasks (T) covered by these 7 scenarios include 23 Tasks (T) from the total number of 34 that the Work Role PR-CDA-001 has, and therefore, according to Eq. (1), the coverage reaches 23/34 = 67.64%. On the other hand, the cyber range does not cover the Work Role PR-VAM-001.

We conclude that updating the scenarios and including the missing TKS seems necessary to cover the above Work Roles completely. For example, the cyber range could include more Tasks (T) regarding threat and vulnerability management (e.g., T0178, T0292, T0526), malware removal (e.g., T0296), network forensics (e.g., T0043, T0298), reporting, and risk mitigation (e.g., T0178, T0548). The above can be easily integrated into the cyber range by including business operations and non-technical tasks. However, Tasks (T) that are challenging to embed on the cyber range involve those requiring hardware work to be done. For example, in OM-ADM-001, the tasks that require hardware include: i) T0514—Diagnose faulty system/server hardware and ii) T0515—Perform repairs on faulty system/server hardware.

Furthermore, the missing TKS also focus on collaboration and requires a narrative, which we did not cover in the cyber range. For example, non-technical procedures are needed for the Work Role OM-ADM-001, such as "T0458—Comply with organization systems administration standard operating procedures". To include this Task (T), the scenarios should involve inter-team interaction or a narrative to define the standards since the standards derive from operational procedures and relevant business processes.

In summary, the complete coverage of the Work Roles is challenging; however, by incorporating human aspects and narrative and updating the scenarios using the missing TKS, the cyber range could provide a more comprehensive and realistic simulation, covering a broader range of capability indicators. In this regard, the NICE framework has proved helpful in identifying gaps or missing points.

5 Conclusions

In this paper, we presented the NICE-by-design cyber range, which consists of 16 scenarios aligned with 5 Specialty Areas from the NICE framework. The cyber range provides realistic context and was developed using the proposed methodology from this paper to give a well-structured design approach. The NICE framework was used to evaluate and improve the learning outcomes of cyber range scenarios. Specifically, the NICE framework provides guidance across diverse cybersecurity topics, facilitating updates to address evolving threats and identifying necessary upgrades within the scenarios.

Educators can use the results and methodology to structure their exercises better, as the design methodology presented in this research can be broadly applied. More specifically, it can be applied to design cybersecurity scenarios, CTF challenges, virtual labs or, as presented, to develop cyber ranges. Furthermore, the results of this research could help organizations and academic institutes align the educational needs of their curricula with more technical aspects of cybersecurity in a more constructed and systematic manner. By systematically identifying educational requirements, institutions can effectively prepare individuals for cybersecurity careers, addressing the evolving threat landscape and the growing demand for skilled professionals.

Appendix 1: Cyber Defense Analysis (CDA)

Workforce category: protect and defend (PR)	
Specialty area	Relevant work role
Cyber defense analysis (CDA)	Cyber defense analyst (PR-CDA-001)
Tasks (T): Network traffic analysis; Enable security and change configurations to reduce risks; Document incidents and Event correlation; Identify malicious activities; Validate intrusion detection systems and network signatures; Assess adequate access controls (T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548, T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260)	
Knowledge (K): Computer networks; Risk management; Regulations, laws and principles related to security and privacy; Access control mechanisms; Vulnerability assessment tools; Computer algorithms, databases and encryption; Incident handling and intrusion detection; Network traffic analysis; Operating systems; Cyber threats and adversarial tactics; System, network hardening, and security testing (K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624)	

Workforce category: protect and defend (PR)	
Specialty area	Relevant work role
Skills (S): Intrusion detection; Security design; Incident handling; Collect data from cyber defense resources; Vulnerability management; Interpret network signatures; Security controls based on regulations (S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370)	

Appendix 2: Systems Administration (ADM)

Workforce category: operate and maintain (OM)	
Specialty area	Relevant work role
Systems administration (ADM)	System administrator (OM-ADM-001)
Tasks (T): Functional tests; System administration, group policies and access controls; System recovery, availability and optimization (T0418, T0431, T0435, T0458, T0461, T0498, T0501, T0507, T0514, T0515, T0531, T0029, T0054, T0063, T0136, T0144, T0186, T0207)	
Knowledge (K): Local and wide area networking; Performance metrics; Server/ client operating systems and system administration; Hardware maintenance; File systems; Virtualization techniques; Access Controls; Diagnostic tools; Integration principles (K0001, K0002, K0003, K0004, K0005, K0006, K0049, K0050, K0053, K0064, K0077, K0088, K0100, K0103, K0104, K0117, K0130, K0158, K0167, K0179, K0260, K0261, K0262, K0274, K0280, K0289, K0318, K0332, K0346)	
Skills (S): Software configuration and of protection tools; Connection diagnosis; Active directories; Virtualization; Server maintenance, administration and management; System upgrades (S0073, S0076, S0111, S0143, S0144, S0151, S0153, S0154, S0155, S0157, S0158)	

Appendix 3: Network Services (NET)

Workforce category: operate and maintain (OM)	
Specialty area	Relevant work role
Network services (NET)	Network operations specialist (OM-NET-001)
Tasks (T): Network hardware configuration; Network diagnostics; Integration and management of new devices; Patch network vulnerabilities (T0129, T0035, T0065, T0081, T0121, T0125, T0126, T0153, T0160, T0200, T0232)	
Knowledge (K): Network communication protocols, media and hardware; Remote access and server administration; Data management controls (K0001, K0002, K0003, K0004, K0005, K0006, K0010, K0011, K0029, K0038, K0049, K0050, K0053, K0061, K0071, K0076, K0093, K0104, K0108, K0111, K0113, K0135, K0136, K0137, K0138, K0159, K0160, K0179, K0180, K0200, K0201, K0203, K0260, K0261, K0262, K0274, K0287, K0332, K0622)	
Skills (S): Traffic Analysis; Routing schemas and subnets; Network security practices; Configuration of network protection tools (S0004, S0035, S0040, S0041, S0056, S0077, S0079, S0084, S0150, S0162, S0170)	

Workforce category: operate and maintain (OM)	
Specialty area	Relevant work role
Abilities (A): Network equipment; Network commands; Communication standards; Network flows monitoring (A0052, A0058, A0059, A0063, A0065)	

Appendix 4: Cyber Defense Infrastructure Support (INF)

Workforce category: protect and defend (PR)	
Specialty area	Relevant work role
Cyber defense infrastructure support (INF)	Cyber defense infrastructure support specialist (PR-INF-001)
Tasks (T): Update network signatures; Cyber defense hardware and related security controls (T0042, T0180, T0261, T0335, T0348, T0420, T0438, T0483, T0486)	
Knowledge (K): Data and backup recovery; Packet-level analysis and web filtering; System, host and network hardening (K0001, K0002, K0003, K0004, K0005, K0006, K0021, K0033, K0042, K0044, K0058, K0061, K0062, K0104, K0106, K0135, K0157, K0179, K0205, K0258, K0274, K0324, K0332, K0334)	
Skills (S): Apply host and network controls; Secure network communications; Malware protection; System, host and network hardening (S0007, S0053, S0054, S0059, S0077, S0079, S0121, S0124, S0367)	

Appendix 5: Vulnerability Assessment and Management (VAM)

Workforce category: protect and defend (PR)	
Specialty area	Relevant work role
Vulnerability assessment and management (VAM)	Vulnerability assessment analyst (PR-VAM-001)
Tasks (T): Compliance and penetration testing; Deploy cyber defense audit toolkit; Audit reports; Risk management and mitigation actions (T0010, T0028, T0138, T0142, T0188, T0252, T0549, T0550)	
Knowledge (K): Application vulnerabilities; Programming language structures, cryptology, and diagnostic tools; Ethical hacking; System administration (K0001, K0002, K0003, K0004, K0005, K0006, K0009, K0019, K0021, K0033, K0044, K0056, K0061, K0068, K0070, K0089, K0106, K0139, K0161, K0162, K0167, K0177, K0179, K0203, K0206, K0210, K0224, K0265, K0287, K0301, K0308, K0332, K0342, K0344, K0624)	
Skills (S): Vulnerability scan, network analysis and threat environment; Penetration test, social engineering and mimicking of threat behaviors; Review past logs; (S0001, S0009, S0025, S0044, S0051, S0052, S0081, S0120, S0137, S0171, S0364, S0367)	

Author Contributions SK contributed to the conceptual design of the research by identifying the problem and the design of the evaluation and experiments. EM has led the work in terms of investigating details of the research and offering detailed supervision and guidance. EK and AK have also contributed to the

conceptual design of the approach and conducted the experiments. SK, EM and CN led the writing of the paper with ongoing and detailed feedback from EK and AK. MNN has reviewed the manuscript, and EM and CN edited the paper and provided feedback to improve the technical aspects of the paper.

Funding Open access funding provided by HEAL-Link Greece. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Data Availability Not applicable.

Materials Availability Not applicable.

Code Availability Not applicable.

Declarations

Conflict of interest The authors declare they have no financial interests.

Ethics Approval and Consent to Participate Not applicable.

Consent for Publication Not applicable.

References

1. Herath, T.C., Herath, H.S.B., Cullum, D.: An information security performance measurement tool for senior managers: balanced scorecard integration for security governance and control frameworks. Inf. Syst. Front. (2022). https://doi.org/10.1007/s10796-022-10246-9
2. Petersen, R., Danielle Santos, M.C.S., Wetzel, K.A., Witte, G.: National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST Spec. Publ. **800**, 181 (2020). https://doi.org/10.6028/NIST.SP.800-181r1
3. Paulsen, C., McDuffie, E., Newhouse, W., Toth, P.: NICE: creating a cybersecurity workforce and aware public. IEEE Secur. Priv. **10**, 76–79 (2012). https://doi.org/10.1109/MSP.2012.73
4. Shoemaker, D.: The NICE framework: why you need to understand this important initiative. EDPACS **51**, 1–7 (2015). https://doi.org/10.1080/07366981.2015.1054241
5. González-Manzano, L., de Fuentes, J.M.: Design recommendations for online cybersecurity courses. Comput. Secur. **80**, 238–256 (2019). https://doi.org/10.1016/j.cose.2018.09.009
6. NICE—National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. https://niccs.cisa.gov/workforce-development/nice-framework. Accessed 11 Jan 2024
7. The Workforce Framework for Cybersecurity (NICE Framework - Latest Updates). https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/latest-updates. Accessed 07 Jan 2024
8. Blažič, B.J.: The cybersecurity labour shortage in Europe: moving to a new concept for education and training. Technol. Soc. **67**, 101769 (2021). https://doi.org/10.1016/j.techsoc.2021.101769
9. Furnell, S.: The cybersecurity workforce and skills. Comput. Secur. **100**, 102080 (2021). https://doi.org/10.1016/j.cose.2020.102080

10. Crumpler, W., Lewis, J.A.: The cybersecurity workforce gap Center for Strategic and International Studies (CSIS) Washington, DC, USA, 2019). https://www.csis.org/analysis/cybersecurity-workforce-gap
11. Furnell, S., Bishop, M.: Addressing cyber security skills: the spectrum, not the silo. Comput. Fraud Secur. **2020**, 6–11 (2020). https://doi.org/10.1016/S1361-3723(20)30017-8
12. Švábenský, V., Čeleda, P., Vykopal, J., Brišáková, S.: Cybersecurity knowledge and skills taught in capture the flag challenges. Comput. Fraud Secur. **102**, 102154 (2021). https://doi.org/10.1016/j.cose.2020.102154
13. Erdogan, G., et al.: Developing cyber-risk centric courses and training material for cyber ranges: a systematic approach, pp. 702–713 (2021). https://doi.org/10.5220/0010393107020713
14. Vielberth, M., Böhm, F., Fichtinger, I., Pernul, G.: Security operations center: a systematic study and open challenges. IEEE Access **8**, 227756–227779 (2020). https://doi.org/10.1109/ACCESS.2020.3045514
15. Vykopal, J., Čeleda, P., Seda, P., Švábenský, V., Tovarňák,D.: Scalable learning environments for teaching cybersecurity hands-on, pp. 1–9 (2021). https://doi.org/10.1109/FIE49875.2021.9637180
16. Leitner, M., et al.: Ait cyber range: flexible cyber security environment for exercises, training and research (2020). https://doi.org/10.1145/3424954.3424959
17. Yamin, M.M., Katt, B.: Modeling and executing cyber security exercise scenarios in cyber ranges. Comput. Secur. **116**, 102635 (2022). https://doi.org/10.1016/j.cose.2022.102635
18. Votipka, D., Zhang, E., Mazurek, M.L.: Hacked: a pedagogical analysis of online vulnerability discovery exercises, pp. 1268–1285 (2021). https://doi.org/10.1109/SP40001.2021.00092
19. Vykopal, J., Švábenský, V., Chang, E.-C.: Benefits and pitfalls of using capture the flag games in university courses, pp. 752–758 (2020). https://doi.org/10.1145/3328778.3366893
20. Burley, D., et al.: Special session: Joint task force on cybersecurity education, pp. 918–919 (2018). https://doi.org/10.1145/3159450.3159635
21. HTB—Hack The Box. https://www.hackthebox.com/. Accessed 07 Jan 2024
22. TryHackMe. https://tryhackme.com/. Accessed 07 Jan 2024
23. Vulnerable By Design—VulnHub. https://www.vulnhub.com/. Accessed 07 Jan 2024
24. ENISA Online Training Material. https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/technical-operational/. Accessed 11 Jan 2024
25. Vielberth, M., et al.: A digital twin-based cyber range for soc analysts, pp. 293–311 (2021). https://doi.org/10.1007/978-3-030-81242-3_17
26. Reisser, A., Vielberth, M., Fohringer, S., Pernul, G.: Security operations center roles and skills: A comparison of theory and practice, pp. 316–327 (2022). https://doi.org/10.1007/978-3-031-10684-2_18
27. Chouliaras, N., et al.: Cyber ranges and testbeds for education, training, and research. Appl. Sci. **11**, 1809 (2021). https://doi.org/10.3390/app11041809
28. Langner., G., Skopik., F., Furnell., S., Quirchmayr., G.A.: Tailored model for cyber security education utilizing a cyber range, pp. 365–377 (2022). https://doi.org/10.5220/0010834000003120
29. D Karjalainen, M., Puuska, S., Kokkonen, T.: Measuring learning in a cyber security exercise, pp. 205–209 (2020). https://doi.org/10.1145/3436756.3437046
30. Vykopal, J., Vizvary, M., Oslejsek, R., Celeda, P., Tovarnak, D.: Lessons learned from complex hands-on defence exercises in a cyber range, pp. 1–8 (2017). https://doi.org/10.1109/FIE.2017.8190713
31. Yamin, M.M., Katt, B., Gkioulos, V.: Cyber ranges and security testbeds: scenarios, functions, tools and architecture. Comput. Secur. **88**, 101636 (2020). https://doi.org/10.1016/j.cose.2019.101636
32. Hallett, J., Larson, R., Rashid, A.: Mirror, mirror, on the wall: what are we teaching them all? Characterising the focus of cybersecurity curricular frameworks (2018). https://www.usenix.org/conference/ase18/presentation/hallett
33. Furnell, S., Bishop, M.: Education for the multifaith community of cybersecurity, pp. 32–45 (2020). https://doi.org/10.1007/978-3-030-59291-2_3
34. Knapp, K.J., Maurer, C., Plachkinova, M.: Maintaining a cybersecurity curriculum: professional certifications as valuable guidance. J. Inf. Syst. Educ. **28**, 101 (2017)
35. Jones, K.S., Namin, A.S., Armstrong, M.E.: The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: results from interviews with cybersecurity professionals. ACM Trans. Comput. Educ. **18**, 1–12 (2018). https://doi.org/10.1145/3152893

36. Nestler, V., Coulson, T., Ashley, J.D.: The NICE challenge project: providing workforce experience before the workforce. IEEE Secur. Priv. **17**, 73–78 (2019). https://doi.org/10.1109/MSEC.2018.2888784
37. Dawson, M., Taveras, P., Taylor, D.: Applying software assurance and cybersecurity NICE job tasks through secure software engineering labs. Procedia Comput. Sci. **164**, 301–312 (2019). https://doi.org/10.1016/j.procs.2019.12.187
38. Hajny, J., et al.: Framework, tools and good practices for cybersecurity curricula. IEEE Access **9**, 94723–94747 (2021). https://doi.org/10.1109/ACCESS.2021.3093952
39. Saharinen, K., Karjalainen, M., Kokkonen, T.A.: Design model for a degree programme in cyber security, pp. 3–7 (2019). https://doi.org/10.1145/3369255.3369266
40. Pham, C., Tang, D., Chinen, K.-i., Beuran, R.: Cyris: a cyber range instantiation system for facilitating security training, pp. 251–258 (2016). https://doi.org/10.1145/3011077.3011087
41. Beuran., R., et al.: Cytrone: An integrated cybersecurity training framework, pp. 157–166 (2017). https://doi.org/10.5220/0006206401570166
42. Scarfone, K., Souppaya, M., Cody, A., Orebaugh, A.: Technical guide to information security testing and assessment. NIST Spec. Publ. **800**, 2–25 (2008). https://doi.org/10.6028/NIST.SP.800-115
43. NICE Challenge. https://nice-challenge.com/. Accessed 10 Jan 2024
44. Fowler, J., Evans, N.: Using the NICE framework as a metric to analyze student competencies. J. Colloq. Inf. Syst. Secur. Educ. **7**, 18–18 (2020)
45. Cyberbit. https://www.cyberbit.com/platform/cyber-range/. Accessed 10 Jan 2024
46. Virginia Cyber Range. https://www.virginiacyberrange.org/courseware/. Accessed 11 Jan 2024
47. Burley, D., et al.: ACM joint task force on cybersecurity education, pp. 683–684 (2017). https://doi.org/10.1145/3017680.3017811
48. CIISec Skills Framework. Version 2.4. https://www.ciisec.org/frameworks/skills-framework/. Accessed 10 Jan 2024
49. The Cyber Security Body of Knowledge. Version 1.0. https://www.cybok.org/media/downloads/CyBOK-version-1.0.pdf. Accessed 06 Jan 2024
50. National Centers of Academic Excellence in Cybersecurity. https://www.caecommunity.org/. Accessed 11 Jan 2024
51. JTF Cybersecurity Curriculum (2017). https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf/. Accessed 06 Jan 2024
52. European Cybersecurity Skills Framework (ECSF). https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework/. Accessed 06 Jan 2024
53. The Workforce Framework for Cybersecurity (NICE Framework - Current Version). https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/workforce-framework-cybersecurity-nice. Accessed 07 Jan 2024
54. Hudnall, M.: Educational and workforce cybersecurity frameworks: comparing, contrasting, and mapping. Computer **52**, 18–28 (2019). https://doi.org/10.1109/MC.2018.2883334
55. Harmony Email and Collaboration. https://www.checkpoint.com/harmony/email-security/email-office/. Accessed 07 Jan 2024
56. TrapX - Deception Grid. https://softprom.com/vendor/trapx-security/product/deceptiongrid. Accessed 07 Jan 2024

Dr. Stylianos Karagiannis holds a Ph.D. from the Department of Informatics from Ionian University (2022) and, an M.Sc. in Informatics and Information Systems (2017) from the same institution. He holds a B.Sc. and diploma in Computer Science, Informatics, and Telecommunications from the Department of Digital Systems at the University of Thessaly. (2013). Since 2019, he has been working as a Senior Researcher for EU Horizon research projects in the cybersecurity domain. He specializes in areas such as Capture the Flag (CTF) challenges, Gamification, Game-Based Learning (GBL), Threat Intelligence, Red/Blue/Purple Teaming, Adversary Emulation, Threat Hunting, and Alternate Reality Games). His postdoctoral research focuses on integrating Cyber Ranges, Digital Twins, and Artificial Intelligence to enhance cybersecurity education.

Dr. Emmanouil Magkos (Manos Magkos) received his first degree in Computer Science from the University of Piraeus, Greece in 1997. In April 2003 he received a Ph.D. in Information Security and Cryptography from the University of Piraeus, Greece. Since 2007 he has been affiliated with the Department of Informatics of the Ionian University, Corfu, Greece, where he holds the position of Professor in Cryptography and Computer Security. He has (co-) authored more than 100 papers in international journals, conferences, and book chapters related to Information Security and Cryptography. He also acts as a reviewer for several international journals and conferences. His current research interests mainly involve the use of Cybersecurity education, as well as cryptographic techniques for protecting security and privacy in networks, computer systems, and distributed applications.

Eleftherios Karavaras is an experienced Information Security Engineer with a demonstrated history of working in the information technology and services industry. Skilled in Endpoint Security with different Vendor Solutions (Checkpoint, Microsoft, Cisco, McAfee, Fortinet) as well as proven experience with SIEM Solutions (IBM QRadar, Microsoft Sentinel). Strong information technology professional and completing the Bachelor of Science (B.Sc.) from the Department of Informatics from Ionian University.

Antonios Karnavas is a skilled Software Engineer with a strong background in programming and software development. He has a proven track record in designing and implementing robust solutions, with expertise in various programming languages and development tools. He is now completing the Bachelor of Science (B.Sc.) from the Department of Informatics at Ionian University.

Maria Nefeli Nikiforos was born in Corfu in 1997. She graduated from the Department of Informatics, Ionian University, Corfu, Greece, in 2019. She received her M.Sc. (Research Directions in Information Technology) from the same department in 2021. She is currently a Ph.D. Candidate at the Department of Informatics, Ionian University, Corfu, Greece, and System Administrator at the Department of Tourism, Ionian University, Corfu, Greece. She has participated as a researcher in several research programs. Her research interests include Natural Language Processing, Linguistic Data Mining, Machine Learning, Artificial Intelligence, and their application on Vocational Education and Language Learning. Mrs. Nikiforos is a reviewer for several international journals and conferences. She and her co-authors have received the 2021 Best Paper Award from Computation journal, MDPI, for their paper "Deep Learning for Fake News Detection in a Pairwise Textual Input Schema", https://doi.org/10.3390/computation9020020.

Dr. Christoforos Ntantogian received his B.Sc. degree in Computer Science and Telecommunications in 2004 and his M.Sc. degree in Computer Systems Technology in 2006 both from the Department of Informatics and Telecommunications of the University of Athens. In 2009 he received his Ph.D. from the University of Athens (Department of Informatics and Telecommunications). Currently, he is an assistant professor at the Department of Informatics of the Ionian University. He has participated in numerous projects realized in the context of EU Programs and currently, he is the technical coordinator of the NITRO DIGITAL Europe Project. He is an editorial board member of the International Journal of Information Security, Springer. His research interests lie in system and network security.