Received 5 August 2022, accepted 28 September 2022, date of publication 25 October 2022, date of current version 31 October 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3216711

RESEARCH ARTICLE

Gamification of Cybersecurity for Workforce Development in Critical Infrastructure

TRAVIS D. ASHLEY[1], (Member, IEEE), ROGER KWON[1], SRI NIKHIL GUPTA GOURISETTI[1], (Senior Member, IEEE), CHARALAMPOS KATSIS[2], CHRISTOPHER A. BONEBRAKE[1], (Member, IEEE), AND PAUL A. BOYD[1]

[1]Pacific Northwest National Laboratory, Richland, WA 99354, USA
[2]Department of Computer Science, Purdue University, West Lafayette, IN 47907, USA

Corresponding author: Travis D. Ashley (travis.ashley@pnnl.gov)

This work was supported by the Pacific Northwest National Laboratory, which is operated for the U.S. Department of Energy by the Battelle Memorial Institute, under Contract DE-AC05-75RL01830.

ABSTRACT Critical infrastructure has become a focal point of cyberattacks, as previously isolated operational technology networks that were once perceived to be air-gapped are becoming Internet-exposed through increased connectivity with informational technology networks. Recent adversarial tendencies have led to an increase in targeted cyberattacks against both industrial control systems (ICS) and building automation systems. Furthermore, the insufficient supply of a cyber workforce exacerbates the challenges for organizations to defend their systems. Game-based learning is gaining traction and studies have shown that it is an effective educational element. Training facility operators responsible for critical services can be achieved through gamification of security policies and controls. The Network Defense Training Game (NDTG) is a cybersecurity training platform that encompasses a series of cybersecurity events that the player must assess and react to throughout the scenario to defend the network by thwarting the adversary's attack. The NDTG uses scenario narratives based on historical cyber incidents that affect ICS. It is designed to train facility owners and operators to evaluate their cybersecurity posture and to apply cybersecurity frameworks before and during the process of addressing cyber events and incidents. This study provides a detailed technical overview and design architecture of NDTG and demonstrates its capability in advancing the ICS cybersecurity workforce.

INDEX TERMS Cybersecurity framework, cybersecurity gamification, cybersecurity training, experimental learning, game-based training, ICS cybersecurity, NICE framework, workforce development.

I. INTRODUCTION

Critical infrastructure (CI) consists of disparate services that are vital to a nation's operations and serve as the backbone of societal and economic functions. The resiliency of the CI is essential for empowering the continuity of the critical services required for national security. CI resiliency is crucial to a nation's livelihood and continues to receive significant attention from researchers and legislatures to produce administrative requirements that aid facility operators in fortifying their networks that remain exposed and vulnerable. The U.S. Department of Homeland Security (DHS) has an agency dedicated exclusively to securing the nation's infrastructure, called the Cybersecurity and Infrastructure Security Agency (CISA), which is dedicated to creating a resilient defense against complex, nonlinear, and evolving threats to the U.S. infrastructure. The CISA categorizes CI into 16 sectors [1], each with a distinct function and provides unique critical services to a nation (e.g., energy, healthcare, wastewater, transportation, communications). One facet that all sectors have in common is that they rely on federal facilities that house the networks that they require to conduct operations. However,

The associate editor coordinating the review of this manuscript and approving it for publication was Songwen Pei.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

the attack surface of CI continues to expand as facilities are being integrated with modern technologies. For example, the electric grid is now dependent on cyber-physical systems when mechanical components were once sufficient [2]. The benefits of data-driven performance on operational productivity are in constant battle with the limitations and restrictions imposed by implementing additional security controls. It is often an ambiguous decision as to which productivity is the most measurable metric on which to base a decision.

This paper introduces a new feature to the Facility Cybersecurity Framework (FCF) [3] tool suite, the Network Defense Training Game (NDTG). The novel contributions of this tool include: 1) developed and demonstrated gamification-based cybersecurity training for the resilience of OT in critical infrastructure facilities, 2) modeled real-world industrial control system (ICS) cyberattack scenarios applying the NICE Framework workforce roles as defined by the National Institute of Standards and Technology (NIST), and 3) designed and depicted the implementation of autonomous cyberattacks to create an adaptive response to the player's decisions to facilitate formative learning. The primary research question involved in making these contributions is.

A scenario named "Quartet" was created in which four cyberattacks were modeled to attack a fictitious OT network. In Quartet, the player assumes the role of facility manager and must defend the operational technology (OT) network from adaptive attackers by configuring the physical network environment and implementing security policies in a turn-based cyberattack simulation. The player is presented with a facility's network architecture, which they must defend; however, it contains misconfigurations (e.g., segmentation flaws, rogue devices, and missing firewalls). The attacker is preprogrammed to follow a sequence of steps to launch several cyberattacks against the player's network, forcing them to allocate their budget to improve only relevant defenses. Quartet was designed to test players' skills in identifying protective measures in the face of an active cybersecurity incident, and to reflect on what could happen realistically. Additional training scenarios shall aim to inform facility operators and other OT network managers that the described network topologies are common implementation examples of good security practices.

The remainder of this paper is organized as follows. Section II provides a literature review of how gamification has been used in education and explores how this method can be applied to cybersecurity training. Section III describes how gamification can be used in workforce development and the drivers of improved cybersecurity in facility-related control systems. Section IV provides a detailed overview of the methodology used for game mechanics in the NDTG. Section V contains a use case for the application of this methodology. Section VI discusses the scenario described in the use case to demonstrate the application of NDTG to cyber-workforce development. Finally, Section VII concludes this paper.

II. BACKGROUND

Gamification of learning resources is a method that is not fully understood. A review [4] of 11 studies was done that evaluated the effect of gamification on education and in most cases, it was found that participants felt more engaged and considered it to be more effective and fun. In these studies, various gamification elements were utilized to achieve learning objectives. Simulation, competition, and puzzles resulted in positive feedback from the participants. A characteristic that all these elements share is that it makes gamification highly interactive. Additionally, these elements may motivate participants because they enhance their interest, and positive results would require stimulated cognitive functioning. The NDTG employs each of these gamification elements (i.e., simulation, competition, and puzzles) to create an effective and fun cybersecurity training tool that can be used for cyber-workforce development in federal facilities.

A. OVERVIEW

A facility's assets are grouped into two major categories: information technology (IT), which is found on the enterprise layer (e.g., employee workstations and email/printer servers), and OT which pertains to all the building's functionality-related control systems (e.g., heating and cooling, industrial control systems, and energy delivery systems). In regards to the Confidentiality, Integrity, and Availability (CIA) triad, IT tends to prioritize CIA, while OT tends to be the opposite and prioritizes AIC. Historically, in most cases, OT networks were intended to be isolated from external connections and, therefore, required less complex security controls. However, the benefits of connectivity in OT environments are continually being discovered; consequently, OT networks are becoming Internet-connected and targets of cyberattacks [5]. The dynamic OT network architecture addresses infrastructure security as a multifaceted challenge, as new threats arise through increased connectivity and new technologies become integrated into critical environments.

The DHS National Cybersecurity and Communication Integration Center reported that in 2014, the ICS attack surface included 82,000 cases in which ICS were configured in such a manner that they were directly accessible from the Internet [6]. Remote accessibility is one of the driving factors for the adoption of Internet connectivity in ICS. Therefore, OT devices that are directly accessed from the Internet are not necessarily unintended weaknesses. However, network misconfigurations and improper security controls lead to inadvertent exposure to OT devices, which often have security vulnerabilities. The ICS Cyber Emergency Response Team reported in 2016 that a total of 2,282 vulnerabilities pertaining to ICS were reported [7], a significant increase from the 427 vulnerabilities reported in the previous year. Since 2015, these vulnerabilities could have led to undesirable cyberattacks on misconfigured facility OT networks, which could have been largely mitigated if security controls were implemented in accordance with the industry's best practices.

Cyberattacks on facilities providing critical services demonstrate the necessity of the requirements for strengthened security in critical infrastructure mandated in legislation, notably in March 2021 executive order (EO) 14017 [8] and the house bill ''Industrial Control Systems Capabilities Enhancement Act of 2021'' (H.R.1833) passed by the House in July 2021 [9]. EO 14017 mandates strengthening the resilience of U.S. supply chains to guard national security by securing ICS and explicitly cautions against supply chain compromises. Supply chain threats are a significant concern for resilience because they are frequently introduced into supply chains by injecting malicious code and hardware into products deployed in OT networks by trusted third parties. For example, a supply chain compromise cyberattack was launched in December 2020 against SolarWinds Orion, in which malicious code was injected into software updates and spread to customers as a Trojan horse [10]. Many of these customers included government facilities and other CI processes. On the other hand, H.R.1833 charged the CISA to identify and mitigate threats to both IT and OT networks of facilities, with the goal of protecting the ICS of facilities supplying critical services.

In May 2020, a cyberattack targeted the energy sector of the CI that used ransomware on business systems belonging to a major oil pipeline company, which ultimately led to the shutdown of oil pipelines that supplied the lower eastern seaboard of the United States [11]. This attack exemplifies the need to secure CI because the OT network itself was never infected; instead, it was taken offline because of the interconnected networks between the OT network and the infected IT networks. The primary impact of the attack was on the IT network in which ransomware was deployed. However, the industrial environment was preemptively shut down, highlighting the symbiotic relationship between IT and OT in a CI environment. In both scenarios, the U.S. CI was disrupted because of a lack of resilience built into the design of the networks and a shortage of security policies that prevent intrusions from occurring. The crux is that both cyberattacks were preventable had network security been adequately hardened; however, the risks were accepted without implementing substantial security controls to defend against adversaries.

These cyberattacks demonstrate the necessity for enhanced cybersecurity practices built into the CI processes to protect the national security of the United States. The Industrial Control System Initiative [12] was established in July 2021 to strengthen the relationship between the federal government and private sector to improve critical infrastructure protection. This was a voluntary initiative that required participation from the private sector to engage in information-sharing and compliance with cybersecurity frameworks. Emphasizing cybersecurity inadequacies of infrastructure security, EO 13800 [13] mandated that all CI comply with the NIST Cybersecurity Framework (CSF). The CSF [14] provides a wide range of defense mechanisms using 100+ cyber defense controls in five domains (Identify, Protect, Detect, Respond, and Recover), and each domain is split into various categories with a narrower scope. The CSF was designed to be used in conjunction with the security policies and risk management processes that an organization already has in place.

The DOE Office of Cybersecurity, Energy Security, and Emergency Response directed each sector of the CI to tailor the CSF to fit their unique cybersecurity objectives [15]. The FCF [16] does just this by adapting the CSF to tailor it to the needs of federal facilities belonging to the government facilities sector of the CI. The FCF tool suite was developed to bolster the cybersecurity maturity of the CI in compliance with the CSF by training facility operators such that the five domains apply to commercial and government buildings. FCF is a free web tool sponsored and featured by the Federal Energy Management Program's (FEMP) in the Solution Center Toolbox [17].

There are many different training platforms, assessments, security tools, and other features of the FCF. The fundamental feature of the FCF is the core assessment tool that enables facility operators to go through every security control in the FCF to self-assess their facility's security posture. The FCF core assessment [18] is valuable for facility operators to: 1) discover their current cybersecurity posture, 2) identify tailored security gaps, 3) describe their target cybersecurity state, 4) identify and prioritize opportunities for improvement within the context of a continuous and repeatable process, 5) assess progress toward the target state, and 6) communicate about cybersecurity risks among internal and external stakeholders.

B. SUMMARY

Despite its efficacy, the FCF did not encompass cybersecurity training tools pertinent to managing cybersecurity at the network layer. An additional tool was required in the FCF suite to provide training for OT network policy implementation within the FCF suite deployment environment. Therefore, the NDTG was designed to train the cyber workforce in an operational environment.

III. RELATED WORKS

This section reviews previous studies that have incorporated gamification of cybersecurity into educational training. The primary purpose of this review was to identify how gamification has been applied to cybersecurity training in previous studies. In addition, this review evaluated the effectiveness of the gamification elements used so that the most useful mechanisms could be built into NDTG. This section is not meant to serve as a comprehensive literature review to propose research questions. Rather, a comparison was made between the most similar related studies (based on gamification elements and learning objectives) to identify the gaps in the current capabilities of existing cybersecurity training tools that NDTG proposes to fulfil. Many additional game-based tools are available for cybersecurity training. However, the only related studies reviewed were within the scope of network security, and targeted professional audiences.

A. CYBER THREAT DEFENDER

The Cyber Threat Defender (CTD) is a competitive tabletop card game developed by the Center for Infrastructure Assurance and Security at the University of Texas, San Antonio. The player builds their network by placing assets and defenses down in front of them and can also play attack cards to beat their opponent [19]. The card deck used by each player can be customized to use different strategies to win the game. While this started as a tabletop, it has also been virtualized [20]. A potential enhancement to the CTD would be the implementation of time constraints between player turns. A highly effective gamification element for cybersecurity game-based training is the reduction of time to observe, orient, decide, and act (T_{OODA}) [21]. Training exercises that engage the player by limiting their decisions using T_{OODA} can be a motivating force which may increase learning outcomes. However, because the cards are randomly drawn from the deck, there may be no direct connection to scenarios with structured learning objectives.

B. CYBERCIEGE

CyberCIEGE [22] is a game-based training tool for teaching IT cybersecurity concepts to students. This is a 3D simulation of an office space, in which the user manages a security policy to maintain a balance between employee performance and improved security. A core component of CyberCIEGE mechanics is that, within the simulation, the player interacts with virtual employees to understand their unique requirements while implementing security policies. Feedback on students' performance is primarily provided through formative evaluation using messages detailing observations about the status of the network. A potential enhancement of CyberCIEGE is the integration of teaching metrics and assessments. This could be done by using established cybersecurity frameworks to base scenarios, such that the learning objectives of scenarios can be directly mapped to the roles and responsibilities of the workforce. Another enhancement of CyberCIEGE is the use of formative evaluations to improve student education [23]. This can be achieved by making the cyberattack unfold dynamically based on the actions taken by the student, so that the steps taken to launch the cyberattack are reactive toward the student's decisions.

C. CYBER PROTECT

In the Department of Defense Cyber Exchange game, Cyber Protect [22], a player defends the network by purchasing and deploying tools. As cyberattacks occur, a behind-the-scenes module indicates what the attackers have done and provides feedback on applicable defenses and mitigation. A potential enhancement to Cyber Protect would introduce the player to the organizational security policy. In addition, the network can emphasize an OT network with components for building automation and control for a more robust network architecture.

D. CYBERNEXS

CyberNEXS [24] was not freely available but was included, as it is claimed to be the de facto standard for cybersecurity training games. Therefore, the evaluation of this tool was based solely on academic sources and was not an independent review. It has several modes, with varying capabilities and gamification elements. CyberNEXS Computer Network Defense Centralized is an emulation with the objective of defending the emulated network against a cyberattack with the primary objective of maintaining the availability of critical services [25]. The player must identify threats to the network, implement mitigation measures, and communicate them to the network administrator. There may be room to enhance CyberNEXS by structuring the learning objectives based on the CSF so that the game can be designed around a holistic cybersecurity framework, instead of primarily focusing on maintaining availability.

E. AGENT SUREFIRE

Agent Surefire [26] is not freely available, and only a few academic studies have reviewed this tool. However, the Mavi Interactive website provides detailed specifications regarding game mechanics. Mavi Interactive created a series of network defense simulation games called Agent Surefire. This platform is a highly immersive 3D simulation platform that allows the user to roam freely around a building. This methodology uses real-world cyberattack scenarios and formative teaching through adaptive endings, based on player performance. However, it was not observed that Agent Surefire incorporated cybersecurity frameworks within the game mechanics for learning objectives. A potentially enhanced learning objective can be achieved by mapping the learning outcomes to established cybersecurity frameworks.

F. SUMMARY

A comparison was made between these related works using several gamification elements, which were evaluated for various aspects of the game design and educational approach: 1) simulation was evaluated as the tool emulating an organization's network, 2) resource constraints were based on the game's requirement for budgeting, 3) scenarios indicates that the tool provides a storyline or some explanations of what is happening in the cyberattack so that the player is responding to a realistic situation, 4) free to play means that it was publicly accessible over the Internet and was trialed without charge, 5) the criteria for T_{OODA} was that the player's decisions had a time constraint, such as a countdown timer or not a turn-based design, 6) OT concepts means that the primary scope of the game is designed for technology and attack techniques found in the OT environment, 7) learning metrics were identified by whether the core component of the design emphasizes learning objectives based on criteria set by an established taxonomy or model, 8) formative teaching was evaluated by assessing if the attack vectors changed based on the player's decisions, 9) card-based was

TABLE 1. Capabilities in game-based cybersecurity training.

Element	CTD	CyberCIEGE	CyberProtect	CyberNEXS	Agent Surefire	NDTG
Simulation	X	X	X	X	X	X
Resource constrains		X	X	X	X	X
Scenarios		X	X	X	X	X
Free to play	X	X	X			X
T_{OODA}				X	X	X
OT concepts				X	X	X
Learning metrics				X	X	X
Formative teaching					X	X
Card-based	X					X
EO 13800						X
NICE Framework						X

not limited to a physical deck, rather it was in any implementation in which cards were played, 10) the EO 13800 metric evaluated whether the NIST CSF is incorporated in either the game mechanics or the progress report, and 11) the workforce roles metric focuses on if the lessons or scenarios are tailored to specific cybersecurity roles. A summary of the metrics examined in related studies is presented in Table 1.

Related studies used effective gamification elements for game-based learning in cybersecurity. However, there is room to enhance the design standards in these studies. Furthermore, game-based training for the critical infrastructure workforce is yet to be fully explored. To address this gap, the NDTG was developed as a gamification of cybersecurity training tools tailored to the critical infrastructure workforce. Formative teaching was achieved in NDTG by cyberattack modeling using several attack vectors such that the attacker's move depends on the defense setup of the player. Both learning metrics and EO 13800 were integrated into NDTG by framing the game mechanics around the CSF to walk the user through the framework process and implemented defenses based on the CSF categories. The NDTG learning objectives were aligned with the Workforce Framework for Cybersecurity (NICE Framework) [27] to emphasize specific cybersecurity knowledge, skills, and abilities (KSAs) for different scenarios. Therefore, cybersecurity workforce roles can be defined in the learning objectives based on the KSAs explored in a scenario. In addition, a sequence of scenarios can be created to build upon each other to create a structured course. As NDTG is sponsored by the FEMP, this tool can be freely used by the public by accessing the FEMP Solution Center Toolbox website.

In the next section, the methodology is described in terms of how NDTG was designed to encompass capabilities that were not widely observed in related works (i.e., formative teaching, learning metrics, NIST CSF, and the NICE Framework).

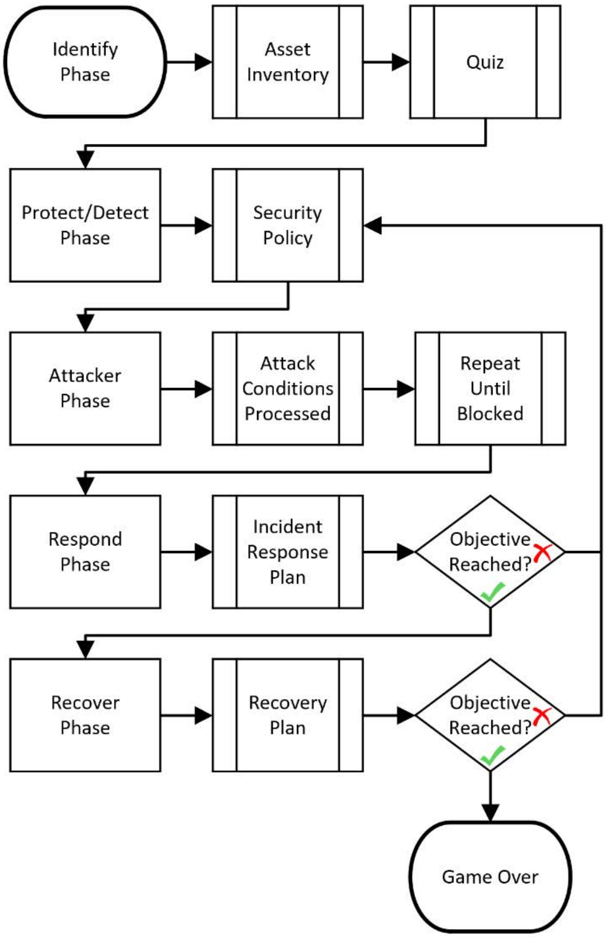


FIGURE 1. Overview of game mechanics in NDTG. The structure of the game phases aligns with the NIST CSF functions. The cyberattack is successful when the objective is reached and therefore the player loses. The player wins after five rounds and no objectives are reached.

IV. METHODOLOGY

A fictitious OT network architecture was created, and several security weaknesses were incorporated into the design. Cyberattack scenarios were then storyboarded based on the misconfigured network, and the cyberattack was aligned with the Cyber Kill Chain (CKC) model, MITRE ATT&CK®for ICS matrix (ATT&CK), and FCF security controls. NDTG consists of five phases. The first is the identification phase, in which the player performs a hardware inventory that lists each asset. Then the player must analyze the network configuration and decide how to implement security policies, and they can build or remove network devices. An automated attacker then can attack the critical systems. After the attacker moves, the player has the chance to respond to the attack. If they fail to respond and the attacker makes it to the objective of their cyberattack, then they have the last chance to recover their network and keep playing, but they lose the game if they cannot recover from the attack. The player wins by preventing the adversary from reaching the cyberattack objectives for five rounds. Fig. 1 shows an overview of the mechanics of the NDTG.

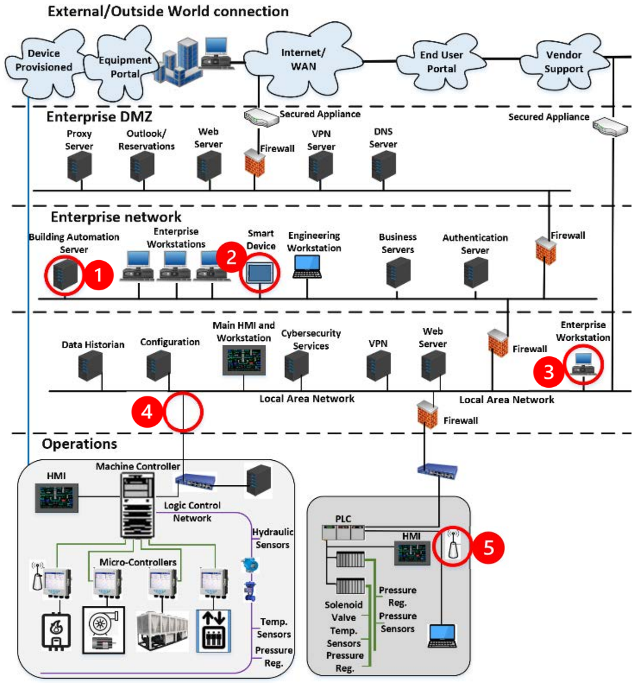


FIGURE 2. Misconfigured network architecture. There are five points of weaknesses purposely included in this design. These weaknesses include added or missing assets, and assets in the wrong network zone.

A. CYBERATTACK MODELING

A baseline network employing good practices was represented using the Purdue model [28]. The Purdue network architecture model is widely accepted in OT environments and is often used to develop and evaluate the architecture of ICS networks. According to the Purdue model, a network can be divided into three primary categories: field devices, supervisory controllers, and IT equipment. An adaptation of the Purdue model was created to use ICS and SCADA applications, including subnets for building management, fire safety, access control, lighting security, and energy management. The NDTG leveraged the adapted network as a representation of what a real-world implementation would look like.

Five weaknesses were then inserted into the baseline network to create a misconfigured network with noticeable vulnerabilities. The misconfigured network was then used to model cyberattacks that would be simulated during the NDTG. The misconfigured network is illustrated in Fig. 2. The misconfigured network map was labelled as follows: (1) building automation server (BAS) in IT, (2) employee's personal smart device connected to IT, (3) IT workstation in OT DMZ, (4) no firewall to OT, and (5) cellular modem in OT. A BAS was added to the enterprise with bidirectional communication and administrative privileges, which could allow excessive access to the OT demilitarized zone (DMZ). IT workstations may be placed in other zones either by accident or for convenience. This could create a bidirectional communication between the two zones. The workstation may also be able to access the OT systems directly.

Cellular modems are sometimes added without informing the owner. These are often used to enable third parties to have remote access for maintenance, and are meant as temporary solutions, but sometimes they are not removed. This can create a backdoor to OT that bypasses all security features, resulting in a rogue access point. A firewall was removed between OT and the OT DMZ. This implies that all traffic is permitted between the two layers. The lack of a firewall for OT is inconsistent with the NIST 800-82R2 recommendations for the separation of zones.

Cyberattacks can be modeled using the CKC [29], developed by Lockheed Martin. The CKC is widely recognized by security practitioners and is used to identify and prevent cyber intrusions. The CKC describes a high-level process in which attackers launch cyberattacks. There are seven steps of the CKC (i.e., Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, Action on Objectives) that establish a framework for security analysts to understand the methods used by an attacker during the entirety of an incident. The development of NDTG included mapping out different attack vectors using the CKC model, so that each phase of the attack was described in detail in relation to the misconfigured network.

B. IDENTIFY PHASE

In the Identify phase, the player is presented with the misconfigured network in Fig. 2, and they are given an incomplete asset inventory. The player must identify assets on the network that have not yet been inventoried. Assets in the inventory have a unique IPv4 address and a qualitative risk assessment score for the impact and severity metrics. New assets are entered into the inventory by the player, who selects the device type, asset name, and asset location. Before moving on to the next step, the player must add all new devices to the hardware inventory. Note that the player may only add new entries to the asset inventory based on the preconfigured network in Fig. 2, and the player does not make any configuration changes. A multiple-choice quiz is then used to evaluate the player's knowledge of the network diagram, including the risk assessment levels.

C. PROTECT AND DETECT PHASE

In the Protect and Detect phase, the goal is for the player to use the knowledge gained during the Identify phase by interacting with the network to harden its security against the five weaknesses. The player begins with 2500 credits and must carefully manage their budget to make configuration changes. The player can add firewalls and intrusion detection systems (IDSs) or remove devices that they have identified in the incorrect zone. They must also implement cybersecurity policies and procedures through investment cards. The implementation tiers for investment cards are basic for 75 credits, improved for 150 credits, or advanced for 230 credits. The effect of improved investments is based on NIST's Framework Implementation Tiers of Partial, Risk Informed and Repeatable, and Adaptive [14]. Basic investments are implemented using default security rules or partially informed by risk. Improved investments are implemented with security rules that are informed by risks and repeatable across additional instances. Advanced investments are implemented with adaptive capabilities for new information-sharing platforms.

A major gamification element for cybersecurity game-based training is the reduction of information ambiguity or the fog of war [21]. To achieve this, specific actions taken by attackers are not revealed until the end of the game. Instead, network technicians made observations to provide details about the symptoms. There are four different technicians, each located within a different zone of the misconfigured network (i.e., Enterprise DMZ, Operations DMZ, Building Machine Automation, and Automation Controllers). Each of the four cyberattack progressions is reflected by a single technician by issuing messages to the user based on the stage of the attack and serves as an alert to the user about what is happening in their network. Technicians may issue alerts for active scanning attempts, network enumeration, anomalous user activity, suspicious logs, network packet capture, spearphishing attempts, or compromised systems. These messages are intended to inform the user of the network status to aid in the decisions they make regarding investments.

Choosing investments to spend the budget on is one of the core components of the educational aspects of NDTG because the attacker's ability to spread through the network depends on which security controls have been implemented. Therefore, it is critical for the player to understand the implications of investing in security to know it's effects. When the player has finished investing in policy, procedure, and detection cards, it is in the attack phase, and the attacker turns to launch cyberattacks against the network.

D. ATTACK PHASE

After investments have been made, it is the attacker's turn to launch cyberattacks. Based on the five different vulnerabilities designed in the misconfigured network architecture, a multitude of cyberattacks can be modeled as abuse cases that exploit these vulnerable exposures. Each cyberattack is modeled using the CKC, which provides details at each stage in the progression of the attack. The ability of a cyberattack to advance to the next stage of the CKC is chance based, depending on whether the user has implemented security controls that are countermeasures for that phase of the attack.

Based on which security controls the user has invested in, a percentage is used to roll a Boolean value, with true moving the attacker forward one CKC stage and false being the end of the attacker's turn. If the security control has not been implemented, it gives the attacker a 100 percent chance of rolling true. If the security control is implemented, rolling true has a 90 percent chance for basic tier, an 80 percent chance for improved tier, and a 70 percent chance for advanced tier. This provides the user with a maximum incentive of 30 percent to implement security controls at the defined implementation levels. These percentages change based on difficulty levels, but the odds favor the player toward the earlier stages of the CKC, so that they have a better chance of getting through the first few rounds. The attacker continues to roll until they roll false or until they reach the Objective stage of the CKC for the modeled cyberattack. When the cyberattack objective is reached, the player enters the Respond phase to attempt to mitigate the cyberattack and remove intrusion.

E. RESPONSE AND RECOVER PHASE

The Respond and Recover phase begin after the attacker has either rolled false or the cyberattack has reached the objective system. In this phase, the player has a chance to mitigate the progress of the attack that was just made in the Attack phase by spending the budget on the Respond or Recovery cards. The Respond cards are actions that can be performed on the network to stop a cyberattack before they reach the Objective stage of the CKC, and the Recover cards are used when the attacker has already reached the objective. If the player's response is the expected mitigation for the current attack stage, then the cyberattack is rolled back to the previous stage; otherwise, it remains in its current stage.

The process of investments, cyberattack progression, and responding to alerts is repeated for a total of five rounds. If the player survives all five rounds without the cyberattacks reaching their objective, then the player wins. If during this time the attacker reaches an objective and the player is unable to mitigate the attack during the Respond and Recover phase, then the game ends and the computer wins. A report is then generated for the player to review their progress and understand why the cyberattacks were successful. The report includes items such as the executive summary, learning objectives, detailed round analysis, spending charts, and timeline for abuse cases.

F. SCORING

The score can be calculated based on player performance. A scoring of at least 70% can be used as a pass/fail criterion. To obtain the overall score, the score of each round must first be calculated. A weighted average is then used to account for the earlier rounds being easier to pass based on the difficulty level of the Boolean rolls for cyberattacks to progress. Equation (1) shows the calculation of the overall score.

$$\frac{\sum_{i=1}^{n=5} S_i W_i}{n \sum_{i=1}^{n=5} W_i} * 100 \tag{1}$$

where S = Equation (2)
W = Weight of round [1, 1, 1, 3, 5]

For a round score to be calculated, it depends on whether the initial access devices for each attack vector are in the network or if they have been removed. If it had been removed, it must have been removed prior to the cyberattack reaching the Exploitation phase of the CKC to obtain 100% for that attack vector for that round. Therefore, if the attack vector is on the network, or if it had been removed, but the cyberattack is post-exploitation, then the round is scored based on whether the expected investments were made. Equation (2) shows the calculation of round scores.

$$\frac{\sum_{i=1}^{n=4} (A \vee (\neg A \wedge (P > 3))) \supset \frac{I(i) \cap C(i)}{C(i)} * 100}{n} \tag{2}$$

where $A =$ Attack vector exists (Boolean)
$P =$ Phase of cyberattack
$I(n) =$ Set of implemented policies
$C(n) =$ Set of attack conditions

V. USE CASE

A scenario named "Quartet" was created and is publicly available and free to use [3]. Cyberattacks were modeled based on a misconfigured network diagram. Attack vectors were mapped to the CKC to show which devices in the network were affected. The vectors were also mapped to the NICE Framework to indicate some of the KSAs in the learning objectives. Attack conditions were then defined to describe the security controls that should be implemented as potential mitigations for cyberattacks. In addition, a quiz was created for the identification phase to target some of the key concepts that could be highlighted based on the attack vectors in this scenario.

A. ATTACK VECTORS

Four potential cyberattacks were identified and modeled for use in the game within the misconfigured network diagram. These cyberattacks were first modeled using the CKC. Then, the learning objectives were defined based on the events within each cyberattack to map responsibilities. Using these learning objectives, KSAs were mapped using the NICE Framework. The four attack vectors are shown in Fig. 3 and described in detail in the following sections.

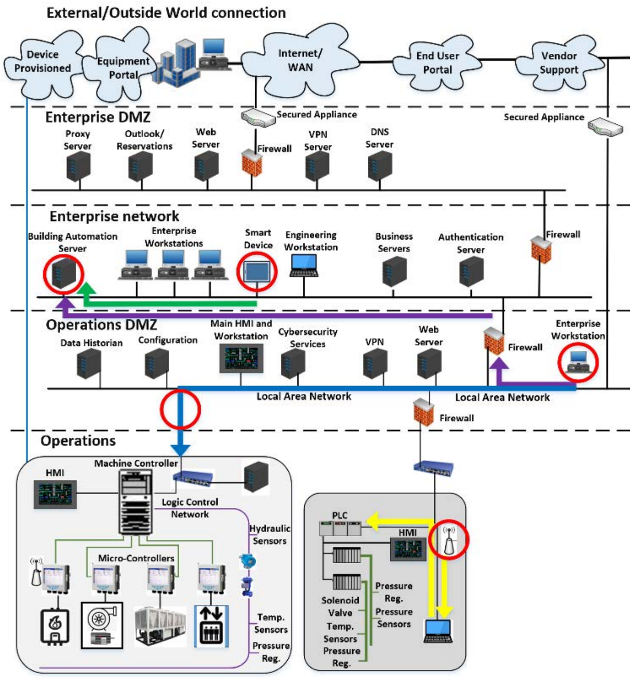


FIGURE 3. The four cyberattack paths in Quartet. The initial access points use the weaknesses shown previously in Fig. 2. Each of the arrows point to the assets that need to be traversed and end with the main objective.

1) ROGUE DEVICE ATTACK VECTOR

This attack vector is indicated by purple arrows in Fig. 3 and extends from the IT workstation to the building automation server. The emphasis of this attack vector is that the IT workstation should not be in the OT DMZ. This is problematic because it is exposed to the Internet, but security has not been sufficiently hardened on this device to withstand attacks because this device was never meant to be in the OT DMZ. The threat actor discovered an Internet-exposed device on the OT DMZ, an IT workstation, which was likely to have been connected to it either accidentally or intentionally. The device was not intended to be in this network. Therefore, the security of this device was not sufficiently hardened in this environment.

Attackers found this workstation was vulnerable to the Common Vulnerability and Exposures (CVE) identified as CVE-2019-1291, which allows remote code execution (RCE) [30]. The firewall was misconfigured to allow sensitive packets. This could have occurred during testing, and they forgot to set the configurations back. This creates a problem because anyone can send packets, and, more importantly, Internet Control Message Protocol ping requests can go through for the discovery of all devices on the network. Therefore, threat actors were able to create a link from the workstation between the OT DMZ and IT network, rendering the firewall between the two zones ineffective. Through network discovery, threat actors have also identified a building automation server in IT. This is not completely rare, but it would require specific security implementations for this setup to be secure.

2) MISCONFIGURED SECURITY ATTACK VECTOR

This attack vector, which extends from the IT workstation to the OT network, is indicated by the blue arrow in Fig. 3. There were no firewalls between the two zones. The attackers realized this error in the network and were able to take advantage of it to discover a vulnerability in Windows Server 2008, known as CVE-2020-1350, which allows for RCE [31]. The attackers installed a backdoor on the system and performed network discovery, thereby revealing the best way to take over the entire system.

3) THIRD-PARTY ATTACK VECTOR

This attack vector is indicated by yellow arrows in Fig. 3, extending from the cellular modem to the Programmable Logic Controller (PLC). A Techroutes TR 1803-3G wireless cellular router/modem 2.4.25 is in the OT network. This is a critical disposition of the modem, as it bypasses all the security infrastructure, thus providing a backdoor. After the procedure, the staff forgot to uninstall the cellular modem. As an access point to the core of the facility network, the cellular modem introduces a significant threat as it bypasses all security defenses in place. Threat actors have identified the presence of the device in the network and have discovered that the device is a Techroutes TR 1803-3G wireless cellular router/modem 2.4.25, which is vulnerable to Cross-Site Request Forgery (CSRF) attacks [32]. This vulnerability was filed as CVE-2017-11648 [33]. The workstation had a pre-established trust in the modem.

Using social engineering techniques, the threat actors convince the workstation user to complete an online form that seems legitimate according to the user's perception. Submission of the web form forges a legitimate packet to be sent to the modem. The payload of the packet is a command that disables the modem's defense. By leveraging the user's cybersecurity ignorance, the adversary can send malicious code through the defenseless modem and run code on the user's workstation, allowing them to control the workstation remotely. With simple network discovery, they recognized that the workstation was connected to a PLC. Thus, the objective of the threat actor is to control the PLC.

4) INSIDER THREAT ATTACK VECTOR

This attack vector is indicated by the green arrow in Fig. 3, which extends from the smart device to the building automation server. Because of the Bring Your Own Device (BYOD) policy, personal devices can be used in the office. Employees used to bring their own devices, such as laptops, smart light-emitting diode lamps, non-cleared universal serial bus (USB) memory sticks, and others to the workplace. Threat actors recognized that the facility allowed BYOD in advance and deliberately left a USB memory stick containing malware in the facility's underground parking lot. A careless employee without proper cybersecurity training picked up the malicious USB memory stick and inserted it into his personal laptop connected to the facility network. As soon as the USB was plugged in the laptop, the implanted malware was executed. Through network scanning from the laptop, threat actors found a smart lamp with the CVE-2020-3119 vulnerability attached to the facility network [34]. The vulnerability enabled the malware to move laterally to reach the machine controller sitting on the Enterprise network.

B. ATTACK CONDITIONS

Attack conditions were created to describe the actions that the attacker could take to step through the CKC of each attack vector. Subsequently, defenses were mapped to the attack conditions for what the play would be expected to implement while playing the scenario. The method to make the attack conditions was through an attack-defense tree (ADTree) [35]. In an ADTree, there are attack and defense nodes as cyberattacks progress from left to right.

Fig. 4 shows an example ADTree for the Quartet scenario. The attack conditions were mapped using AND/OR logic to indicate the security controls that could be implemented to protect against each attack vector. For example, the root of the tree is the attack vector in which the attacker scans the network. If the attacker is successful at scanning the network, they will then proceed to either send an email attachment, bypass detection, or plant a flash drive. However, there are two defenses that can be played to make scanning the network unsuccessful and will prevent the attack: hardware inventory and risk assessments. These defenses are joined by an AND gate and therefore both must be implemented to prevent the attack; otherwise, only one of them would be required. Nodes on the furthest right signify the end of an attack path, meaning that if these nodes are reached then the attacker has accomplished their goals and there may not be any further defenses applied.

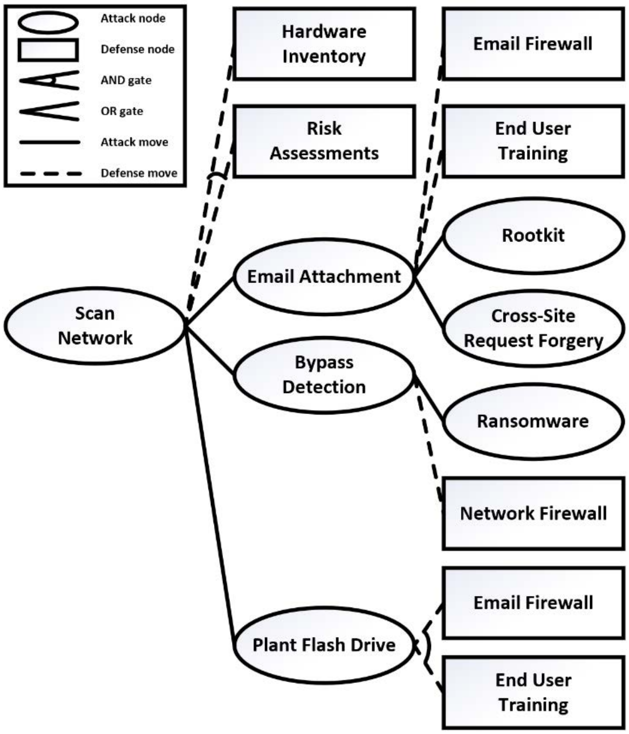


FIGURE 4. ADTree for Quartet. Attack techniques used for all four cyberattack paths are shown as attack nodes. Mitigations are linked to attack techniques in defense nodes to demonstrate how defenses against these cyberattacks could potentially be implemented.

C. LEARNING OBJECTIVES

The learning objectives and NICE Framework KSAs for the Quartet scenario are presented in Table 2. For this scenario, the learning objectives targeted the NIST NICE Framework workforce role PR-CIR-001 [36] for cyber defense incident responder. The learning objectives behind purposely misconfiguring the IT workstation to be located in the OT DMZ, and the Building Automation Server (BAS) in the IT network, are to teach the player about basic network architecture and segmentation. This is categorized as ''network topology'' and is designed to teach about the various network zones and the fundamentals of network segmentation between these zones. Attackers finding CVEs during Quartet is designed to teach about how known vulnerabilities can be used to exploit a weakness in a system. CVEs have nuanced applications, and therefore, could have several unique learning objectives based

TABLE 2. Learning objectives for quartet.

Key Concepts	Learning Objective KSA
Network Topology	K0179: Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).
	K0221: Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).
Vulnerability Scanning	K0005: Knowledge of cyber threats and vulnerabilities.
	S0078: Skill in recognizing and categorizing types of vulnerabilities and associated attacks.
Traffic Analysis	K0058: Knowledge of network traffic analysis methods.
	S0077: Skill in securing network communications.
	A0128: Ability to apply techniques for detecting host and network-based intrusions using intrusion detection technologies.
Remote Access	K0033: Knowledge of host/network access control mechanisms (e.g., access control list, capabilities list).
BYOD	K0157: Knowledge of cyber defense and information security policies, procedures, and regulations.
	S0079: Skill in protecting a network against malware.

on the scope of the vulnerability. This key concept was categorized as "vulnerability scanning". The missing firewall was purposely misconfigured to make a learning objective around traffic analysis and network segregation. This was categorized as "traffic analysis". The cellular modem being accidently left in the OT network is categorized as "remote access", and this was meant to introduce concepts such as access control and insider threats. The employee's personal smart device being plugged into the IT network is categorized as "BYOD", and this is designed to include learning objectives on how to use removable media devices securely. Note that the learning objectives in Quartet only partially achieve the KSAs listed in Table 2 by introducing the player to these key concepts.

VI. DEMONSTRATION

This section will discuss each of the attack vectors in the NDTG to show various strategies to defend the network. All the attack vectors have the same identity phase. Therefore, only the subsequent phases are discussed in this section. Finally, the game report is analyzed to identify potential improvements to the strategies employed in this demonstration.

A. ROUND ONE

In the rogue device attack vector and the insider threat attack vector there are three devices that are located within the incorrect network zone. Fig. 5 shows the position of these three devices on the network in the IT network and OT DMZ. Only two of these devices have the option to be removed (i.e., smart device, enterprise workstation). The first action taken in round one was to remove these two devices. Additionally, all the policy and detection cards were set to basic tier.

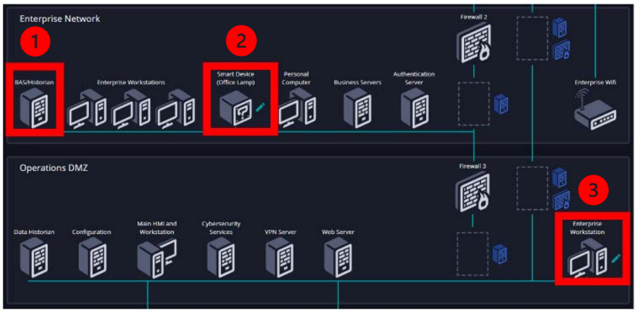
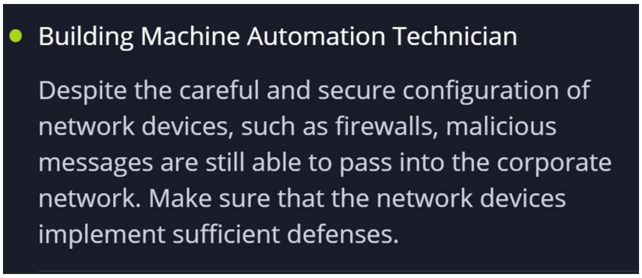


FIGURE 5. Network assets installed in incorrect zone. (1) The BAS should be located in Operations, while conversely the Enterprise Workstation (3) should be in the Enterprise Network. The Smart Device (2) should not be connected to the network according to the BYOD security policy.



● Building Machine Automation Technician

Despite the careful and secure configuration of network devices, such as firewalls, malicious messages are still able to pass into the corporate network. Make sure that the network devices implement sufficient defenses.

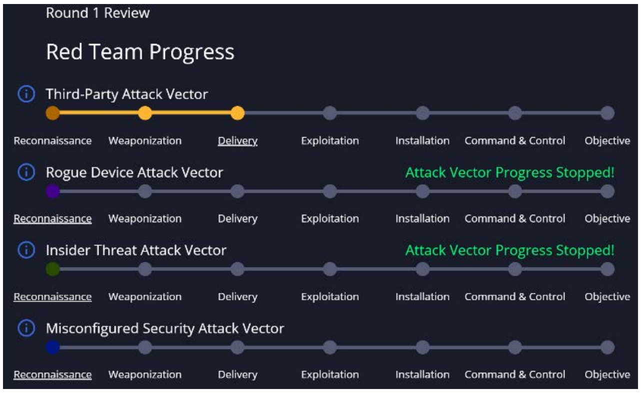
FIGURE 6. Round one technician's feedback. A firewall was missing between the Enterprise DMZ and the Enterprise Network. The player would have needed to add a firewall to prevent this warning message.

Upon implementing these changes, the technicians on the network offered advice about the third-party attack vector. The message indicated that attempts have been made to breach the network through bypassing network defenses, as shown in Fig. 6. An improvement to the security policy would be to improve network and information security monitoring, but only network monitoring was available in the response phase. Therefore, based on this feedback, the implementation in the response phase in round one was network monitoring for advanced tier.

A review is conducted at the end of each round. This module indicates the progression of cyberattacks for each attack vector during this round. A review of the first round is shown in Fig. 7. The third-party attack vector progressed from reconnaissance to the delivery phase. Both the rogue device attack vector and insider threat attack vector were completely protected against. Therefore, the progress of these two cyberattacks ceased. This was achieved by removing the personal smart device from the IT network and the IT workstation from the OT DMZ.

B. ROUND TWO

In this misconfigured security attack vector, the firewall is missing between the Operations DMZ and Operations zones.



Round 1 Review

Red Team Progress

Third-Party Attack Vector

Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Objective

Rogue Device Attack Vector

Attack Vector Progress Stopped!

Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Objective

Insider Threat Attack Vector

Attack Vector Progress Stopped!

Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Objective

Misconfigured Security Attack Vector

Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Objective

FIGURE 7. Round one cyberattacks progression. The third-party cyberattack progressed to delivery phase because there was no firewall between the Enterprise DMZ and Enterprise Network.

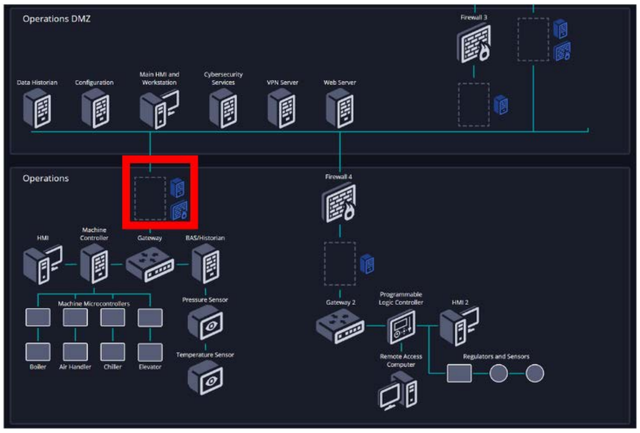
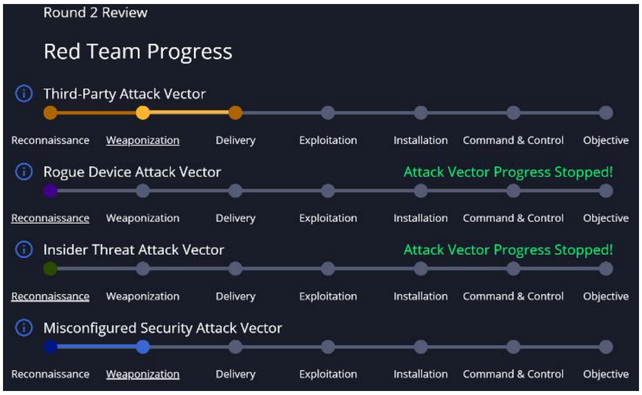


FIGURE 8. No firewalls were observed between operations DMZ and a portion of the operations zones.



Round 2 Review

Red Team Progress

Third-Party Attack Vector

Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Objective

Rogue Device Attack Vector

Attack Vector Progress Stopped!

Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Objective

Insider Threat Attack Vector

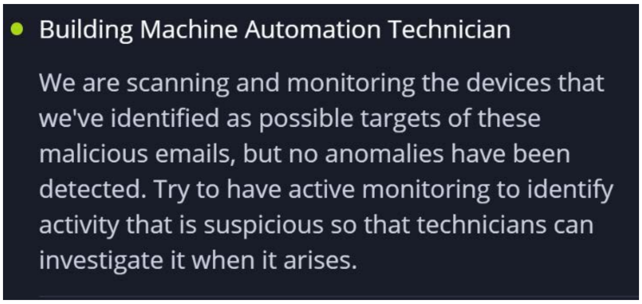
Attack Vector Progress Stopped!

Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Objective

Misconfigured Security Attack Vector

Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Objective

FIGURE 9. Round two technician's feedback. There is no firewall between operations DMZ and operations zone.



Building Machine Automation Technician

We are scanning and monitoring the devices that we've identified as possible targets of these malicious emails, but no anomalies have been detected. Try to have active monitoring to identify activity that is suspicious so that technicians can investigate it when it arises.

FIGURE 10. Round two cyberattacks progression. Both the remaining cyberattacks progressed one stage of the attack.

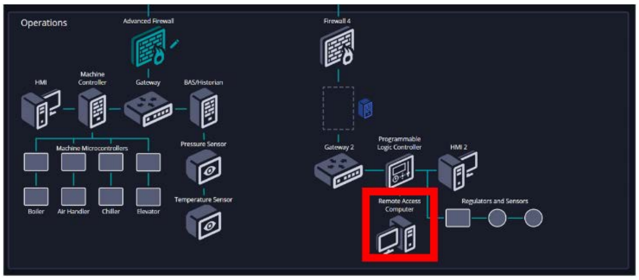


FIGURE 11. Third-party access point. Remote access computer located in the Operations network. This asset was directly connected to both the Internet and critical devices used for building controls.

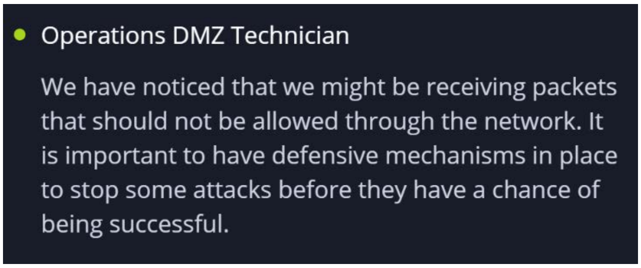
The firewall location is shown in Fig. 8. During round two, a firewall was added to this position to mitigate this threat. Additionally, the same message from round one was displayed indicating that the response was successful in preventing cyberattack from progressing. Therefore, the budget was used to advance the information security monitoring policy card. Additionally, there was a sufficient budget to implement two of the procedure cards to the basic tier (i.e., setup active directory and deploy firmware patches).

In the response phase of round two, the technician messages indicated that the third-party attack vector remained the same. However, the misconfigured security attack vector progressed to the installation phase. The technician's feedback for the round two response phase is shown in Fig. 9. The response to this was to implement patch management to advanced tier. The policy that should be implemented would be perform system updates.

A review of round two is shown in Fig. 10. The third-party attack vector was set back from the delivery phase to the weaponization phase. This was set back because the network monitoring card was implemented to advanced tier during round one. The misconfigured security attack vector progressed from the reconnaissance phase to the weaponization phase.

C. ROUND THREE

In the third-party attack vector, the remote access computer placed by a third party was identified as an issue because it allowed for remote access to the building automation zone without having adequate security controls implemented. The position of the remote access computer is shown in Fig. 11. Performing system updates was implemented to advanced tier. Both the information security policy and network monitoring were already implemented to advanced tier in the previous rounds.



● Operations DMZ Technician

We have noticed that we might be receiving packets that should not be allowed through the network. It is important to have defensive mechanisms in place to stop some attacks before they have a chance of being successful.

FIGURE 12. Round three technician's feedback. Abnormal network packets were discovered. These were originating from the remote access computer, i.e., coming from the attacker over the Internet.

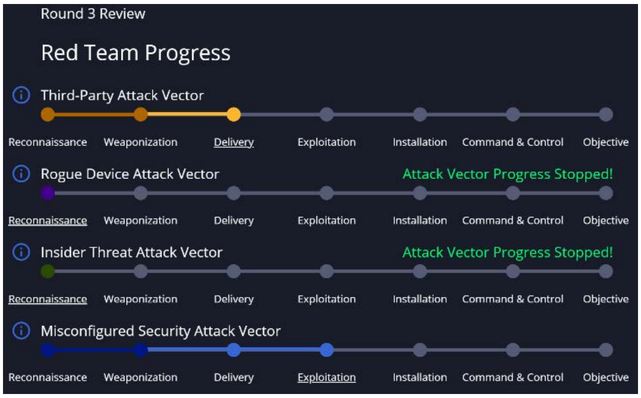


FIGURE 13. Round three cyberattacks progression. Both remaining cyberattacks progressed the stage of attack.

In the response phase of round three, a technician noticed that the firewall was not configured to block the malicious traffic that was allowed to pass. The technician feedback for round three for the misconfigured security attack vector is shown in Fig. 12. The response was the advanced tier of security control for blacklist malware. The response and policies for the third-party attack vector have already been implemented to advanced tier in the previous rounds.

A review for round three is show in Fig. 13. The third-party attack vector progressed from the weaponization phase to the delivery phase. The misconfigured security attack vector progressed from the weaponization phase to the exploitation phase.

D. ROUND FOUR

In round four, the insider threat attack vector did not progress, but the misconfigured security attack vector was set back from exploitation to weaponization, as shown in Fig. 14. The mitigations had already been implemented to advanced tier for the misconfigured security attack vector's weaponization phase in round two, so the only action taken in protect and detect phase was to implement several procedure cards to basic tier (i.e., setup incident response team, setup forensics team, setup data encryption). In the response phase, neither cyberattack progressed from the protection and detection phase, and all applicable responses were implemented to advanced tier in previous rounds; therefore, no action was taken.

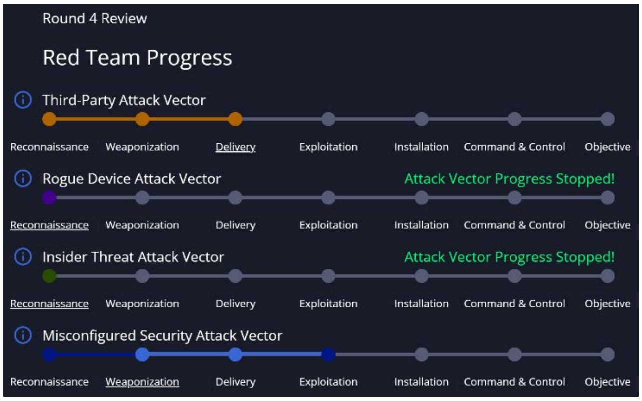
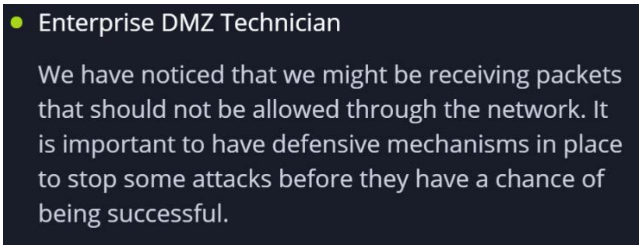


FIGURE 14. Round four cyberattacks progression. The third-party attack did not progress, and the misconfiguration cyberattack was set back two stages.



● Enterprise DMZ Technician

We have noticed that we might be receiving packets that should not be allowed through the network. It is important to have defensive mechanisms in place to stop some attacks before they have a chance of being successful.

FIGURE 15. Round five technician's feedback. Similar abnormal network packets were discovered like those in round three.

E. ROUND FIVE

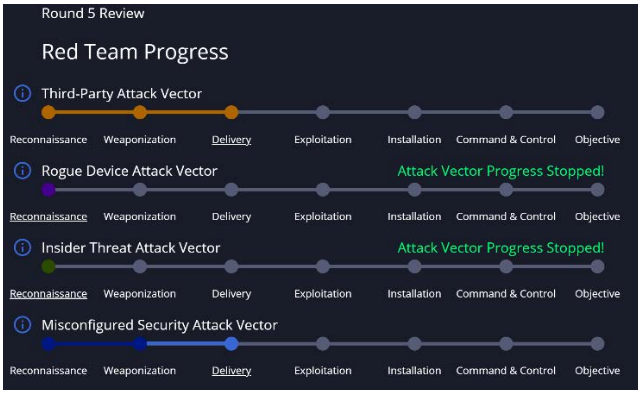
In the final round, technician feedback during the response phase of round five is shown in Fig. 15. The mitigation that could be implemented was an advanced network firewall. However, this is a policy card and is not available in the response round. Therefore, no action was taken.

The final review in round five is shown in Fig. 16. The third-party attack vector was in the delivery phase, both the rogue device and insider threat attack vectors were stopped in the reconnaissance phase, and the misconfigured security attack vector progressed from weaponization to delivery.

F. GAME REPORT

A game report was generated for this demo. The score for each round was a silver star, as shown in Fig. 17. The silver star rating means that each round had expected mitigations implemented to protect the network from attack conditions. Opening any of the rounds opens the review modules and shows which implementations are effective. This provides feedback to the user so that they can learn which strategies they used were ineffective in protecting the network from various cyberattack vectors.

The spending bar chart is shown in Fig. 18. This indicates the number of credits spent on each domain. The deployment



Round 5 Review

Red Team Progress

Third-Party Attack Vector

Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Objective

Rogue Device Attack Vector

Attack Vector Progress Stopped!

Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Objective

Insider Threat Attack Vector

Attack Vector Progress Stopped!

Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Objective

Misconfigured Security Attack Vector

Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Objective

FIGURE 16. Round five cyberattacks progression. The misconfiguration attack progressed one stage of attack.

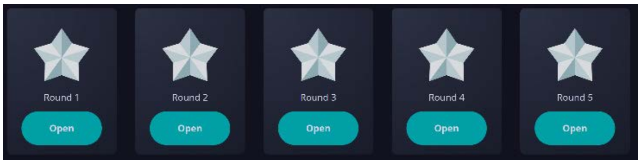


FIGURE 17. Scores for each round. These were all silver star ratings. The cyberattacks progressed too many stages to be gold stars.

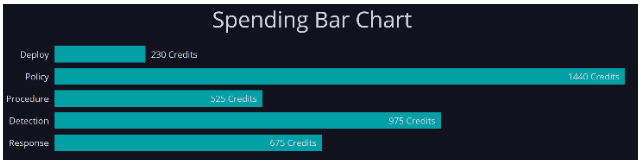


FIGURE 18. Spending chart disaggregated by the types of cards that investments were made with the number of credits spent for each.

phase involves building devices on the network, such as the firewall built between the OT DMZ and the OT network. The policy, procedure, and detection domains were used for the cards played in the protection and detection phases. The response domain was the response cards played in the response phase. Feedback is provided on how much was spent in each of the domains versus how much was expected to have spent.

The report ends with a scenario timeline that has all the events the happened during the cyberattacks. The timeline is separated by the CKC, so each step taken by the attackers is revealed to the player and is easily distinguishable.

VII. CONCLUSION AND FUTURE WORK

As computer networks enter an era of complex interconnectivity that supports the communication between users and network resources, securing computer networks has never been more critical to address. However, cybersecurity awareness of users and network practitioners is an essential factor for securing networks. This study proposes a game-based approach to cultivating cybersecurity training in the workforce using widely adopted frameworks for network security. Each cyberattack was described in a scenario with a timeline that followed Lockheed Martin CKC. NDTG simulates realistic cyberattack scenarios designed to teach learning objectives for specific cybersecurity workforce roles, as defined in the NICE Framework. Finally, the game provides the player with a wide range of defensive strategies as per the NIST CSF, which may thwart the cyberattack. Our approach combines the knowledge derived from these frameworks and offers it to users through a fun and interactive game.

This study provides a foundation for several future research directions. First, users of the game could provide valuable feedback. Game designers may assume another level of knowledge of the users that a product is targeting. Moreover, it would be interesting to investigate how the game's design decisions affect the player's learning curve. Another direction is to use the players' learning curve and skills to provide them with more customized scenarios that would help improve their weaknesses. Such a problem would require collecting several statistics, such as the time taken to respond to an attack, or the details of the attack that they were able to thwart. Additional scenarios can be built to target specific KSAs, and a series of evolving scenarios can be developed to develop a course of learning. Finally, another direction is to develop a method for building dynamic scenarios based on several factors such as attack vector trends, level of difficulty, sophistication of the attack, and the importance of users being aware of this scenario.

REFERENCES

[1] Cybersecurity and Infrastructure Security Agency. (Nov. 2019). *A Guide to Critical Infrastructure Security and Resilience*. Accessed: Oct. 22, 2021. [Online]. Available: https://www.cisa.gov/publication/guide-critical-infrastructure-security-and-resilience

[2] C. Glenn, D. Sterbentz, and A. Wright. *Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector*. Accessed: Oct. 22, 2021. [Online]. Available: http://dx.doi.org/10.2172/1337873

[3] Department of Energy. Network Defense Training Game. Pacific Northwest National Laboratory. Accessed: Oct. 22, 2021. [Online]. Available: https://facilitycyber.labworks.org/training/networkDefenseTrainingGame/landing

[4] F. A. Nieto-Escamez and M. D. Roldán-Tapia, "Gamification as online teaching strategy during COVID-19: A mini-review," *Frontiers Psychol.*, vol. 12, p. 1644, May 2021.

[5] Federal Energy Management Program. (Dec. 2017). *Cyber-Securing Facility Related Control Systems*. Accessed: Oct. 22, 2021. [Online]. Available: https://www.energy.gov/sites/prod/files/2018/01/f46/cyber_securing_facilities.pdf

[6] National Cybersecurity and Communication Integration Center. *Seven Steps to Effectively Defend Industrial Control Systems*. Accessed: Oct. 22, 2021. [Online]. Available: https://us-cert.cisa.gov/sites/default/files/documents/Seven%20Steps%20to%20Effectively%20Defend%20Industrial%20Control%20Systems_S508C.pdf

[7] Industrial Control Systems Cyber Emergency Response Team. (2016). *ICS-CERT Annual Vulnerability Coordination Report*. Accessed: Oct. 22, 2021. [Online]. Available: https://us-cert.cisa.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf

[8] Executive Office of the President. (Feb. 24, 2021). *America's Supply Chains*. Accessed: Oct. 22, 2021. [Online]. Available: https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains

[9] Department of Homeland Security. (Jul. 20, 2021). *H.R.1833—DHS Industrial Control Systems Capabilities Enhancement Act of 2021*. Accessed: Oct. 22, 2021. [Online]. Available: https://www.congress.gov/bill/117th-congress/house-bill/1833

[10] United States Computer Emergency Readiness Team. (May 21, 2021). *Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise*. Accessed: Oct. 2022. [Online]. Available: https://us-cert.cisa.gov/ncas/analysis-reports/ar21-134a

[11] Government Accountability Office. (May 18, 2021). *Colonial Pipeline Cyberattack Highlights Need for Better Federal and Private-Sector Preparedness (Infographic)*. Accessed: Oct. 22, 2021. [Online]. Available: https://www.gao.gov/blog/colonial-pipeline-cyberattack-highlights-need-better-federal-and-private-sector-preparedness-infographic.

[12] J. R. Biden. (Jul. 28, 2021). *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems*. Accessed: Oct. 22, 2021. [Online]. Available: https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/

[13] Executive Office of the President. (May 11, 2017). *Executive Order 13800 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Accessed: Oct. 22, 2021. [Online]. Available: https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure

[14] National Institute of Standards and Technology. (Apr. 16, 2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Accessed: Oct. 22, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[15] Office of Cybersecurity, Energy Security, and Emergency Response. (Jan. 6, 2016). *Energy Sector Cybersecurity Framework Implementation Guidance*. Accessed: Oct. 22, 2021. [Online]. Available: https://www.energy.gov/ceser/downloads/energy-sector-cybersecurity-framework-implementation-guidance

[16] S. N. G. Gourisetti, H. Reeve, J. A. Rotondo, and G. T. Richards. (Aug. 2020). *Facility Cybersecurity Framework Best Practices*. Accessed: Oct. 22 2021. [Online]. Available: http://dx.doi.org/10.2172/1660771

[17] Federal Energy Management Program. *FEMP Solution Center Toolbox*. Accessed: Oct. 22, 2021. [Online]. Available: https://www.energy.gov/eere/femp/femp-solution-center-tool-box

[18] R. Kwon, T. Ashley, J. Castleberry, P. Mckenzie, and S. Gourisetti, "Cyber Threat dictionary using MITRE ATT&CK matrix and NIST cybersecurity framework mapping," in *Proc. Resilience Week (RWS)*, Salt Lake City, UT, USA, 2020, pp. 106–112, doi: 10.1109/RWS50334.2020.9241271.

[19] Center for Infrastructure Assurance and Security. *Overview of How To Play CTD*. Accessed: Oct. 24, 2022. [Online]. Available: https://cias.utsa.edu/wp-content/uploads/2022/05/CTD_Basic-Game-Play.pdf

[20] Center for Infrastructure Assurance and Security. Cyber Threat Defender. University of Texas San Antonio. Accessed: Oct. 22, 2021. [Online]. Available: https://cias.utsa.edu/ctd_cards.php

[21] N. L. Crabtree and J. A. Orr, "Cyber red/blue and gamified military cyberspace operations," *Lincoln Lab. J.*, vol. 23, no. 1, pp. 1–12, 2019.

[22] C. E. Irvine, M. F. Thompson, and K. Allen. (Nov. 2005). *CyberCIEGE: An Information Assurance Teaching Tool for Training and Awareness*. Accessed: Oct. 22, 2021. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA443469

[23] M. F. Thompson and C. E. Irvine, "CyberCIEGE: A video game for constructive cyber security education," *Call Signs*, vol. 6, no. 2, pp. 4–8, 2015.

[24] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, "Exploring game design for cybersecurity training," in *Proc. IEEE Int. Conf. Cyber Technol. Automat., Control, Intell. Syst. (CYBER)*, May 2012, pp. 256–262, doi: 10.1109/CYBER.2012.6392562.

[25] R. Lavanya and V. Thanigaivelan, "Cyber secured surveillance next-generation unmanned ground vehicle through Internet of Things," *J. Pure Appl. Math.*, vol. 120, no. 6, pp. 6879–6891, 2018.

[26] MAVI Interactive. *Products Page*. Accessed: Oct. 22, 2021. [Online]. Available: https://www.maviinteractive.com/products.html

[27] R. Petersen, D. Santos, M. C. Smith, K. A. Wetzel, and G. Witte. (Nov. 2020). *Workforce Framework for Cybersecurity (NICE Framework)*. Accessed: Oct. 22, 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

[28] T. Williams, "The Purdue enterprise reference architecture," *IFAC Proc. Volumes*, vol. 26, no. 2, pp. 559–564, Jul. 1993, doi: 10.1016/S1474-6670(17)48532-6.

[29] Lockheed Martin Corporation. (2015). *Seven Ways to Apply the Cyber Kill Chain® With a Threat Intelligence Platform*. Accessed: Oct. 22, 2021. [Online]. Available: https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf

[30] MITRE. (Nov. 26, 2018). *CVE-2019-1291*. Accessed: Oct. 22, 2021. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1291

[31] MITRE. (Nov. 4, 2019). *CVE-2020-1350*. Accessed: Oct. 22, 2021. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1350

[32] N. Jovanovic, E. Kirda, and C. Kruegel, "Preventing cross site request forgery attacks," in *Proc. Securecomm Workshops*, Aug. 2006, pp. 1–10.

[33] MITRE. (Jul. 25, 2017). *CVE-2017-11648*. Accessed: Oct. 2021. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11648

[34] MITRE. (Dec. 12, 2019). *CVE-2020-3119*. Accessed: Oct. 22, 2021. [Online]. Available: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3119

[35] X. Ji, H. Yu, G. Fan, and W. Fu, "Attack-defense trees based cyber security analysis for CPSs," in *Proc. 17th IEEE/ACIS Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distributed Comput. (SNPD)*, May 2016, pp. 693–698.

[36] Cybersecurity and Infrastructure Security Agency. *NICE Cybersecurity Workforce Framework Work Roles: Cyber Defense Incident Responder*. Accessed: Oct. 22, 2021. [Online]. Available: https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/workroles?name=Cyber+Defense+Incident+Responder&id=All

TRAVIS D. ASHLEY (Member, IEEE) was born in Yakima, WA, USA, in 1993. He received the B.S. degree in cybersecurity from the Columbia Basin College. He is currently pursuing the M.S. degree in cybersecurity with Western Governors University, Salt Lake City, UT, USA.

Since 2017, he has been a Cyber Security Engineer at the Pacific Northwest National Laboratory. His research interest includes critical infrastructure resilience, specializing in cyber risk management of operational technology and building controls environment. He led project tasks for the Department of Energy (DOE) Facility Cybersecurity Framework, including developing cyberattack scenarios and training courses for cyber workforce development in critical infrastructure. He contributed to the development of DOE's MEEDS platform using Python to perform web spider banner grabbing to fingerprint building control systems. He supported DOE's Solid-State Lighting Program by performing vulnerability and threat assessments of networked lighting systems and controllers.

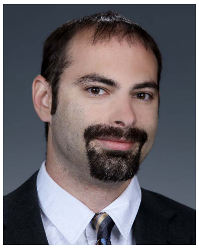
ROGER KWON received the master's degree in computer science and cyber security from the Georgia Institute of Technology.

He is currently a Cyber Security Engineer with the Pacific Northwest National Laboratory. He plays a key role in the development of cybersecurity maturity models, the application of augmented reality to cybersecurity using Microsoft HoloLens 2, and cybersecurity vulnerability testing. He supports the development of the Department of Energy Facility Cybersecurity Framework, including training for cyberattack scenarios and a network defense simulation to mitigate cyberattacks against building control systems. He developed the Cyber Threat Dictionary to define relations between the Facility Cybersecurity Framework and mitigations to defend a network. He is fluent in Korean and was recently nominated to support the Department of Energy's Office of International Nuclear Security's technical exchange with South Korea.

SRI NIKHIL GUPTA GOURISETTI (Senior Member, IEEE) is currently a Cyber Security Researcher with a focus on smart grid and connected buildings projects addressing the resiliency and interoperability challenges. During his time with the Pacific Northwest National Laboratory, he was the PI for multiple DOE projects, including blockchain explorations in power and energy, non-intrusive cybersecurity tools to enumerate vulnerabilities and threats, and physics-based power systems modeling to detect anomalies and forecast failures in complex quasi-distributed sensor networks. He advised on the EERE project that is developing digital twins for hydropower systems. He led the cybersecurity task force under the IEEE P2418.5 Blockchain Standards Working Group and was an Active Member of the DOE's C2M2 Working Group.

CHARALAMPOS KATSIS received the bachelor's and master's degrees (Hons.) from the Department of Information and Communication Systems Engineering, School of Engineering, University of the Aegean, Greece. He is currently pursuing the Ph.D. degree with the Department of Computer Science, Purdue University, advised by Prof. Elisa Bertino.

During his time at Purdue University, he also worked on efficient message authentication techniques for named data networks. While pursuing his Ph.D., he worked as a Research Intern at the Pacific Northwest National Laboratory and Cisco Research. His research interests include network security, focusing on zero-trust network architectures, and machine learning techniques for network security.



CHRISTOPHER A. BONEBRAKE (Member, IEEE) received the bachelor's and master's degrees in electrical engineering from Washington State University, in 2002 and 2004, respectively.

He has been working at the Pacific Northwest National Laboratory, since 2002, on a wide range of areas that include analog and digital electronics, chemical and radiation detection, industrial control systems, SCADA equipment, and cyber security of operational technologies. He is currently an Electrical Engineer. His research interests include power, control systems, and electromagnetic theory.

PAUL A. BOYD is currently a Senior Research Electrical Engineer in cybersecurity and electricity infrastructure with the Grid Operations Research Team, Pacific Northwest National Laboratory. He is also working on establishing cybersecurity requirements for renewable energy, and providing recommendations for the U.S. Air Force, Army, and Army Reserves site for electrical infrastructure, which may include renewable energies, electricity storage, microgrids with energy management systems, utilizing various secure communication protocols, and networking configuration. His research interests include smart grid integration of microgrids and renewable energy.