Ontology-Driven Cybersecurity Learning Factory: A Use Case for Securing Electrical Company Networks

Zubeida C. Khan[1,*,†], Matshidiso Marengwa[2,*,†]

[1] *Council for Scientific and Industrial Research, Pretoria, 0184, South Africa*
[2] *Council for Scientific and Industrial Research, Pretoria, 0184, South Africa*

Abstract

As cyber threats continue to evolve in complexity and frequency, there is an urgent need for effective cybersecurity education and training methodologies. Traditional approaches often fall short in providing learners with personalized and immersive experiences that closely mimic real-world scenarios. In response to this challenge, we propose the development of a Cybersecurity Learning Factory (CLF), leveraging ontology integration to tailor learning experiences for students. By harnessing the power of ontologies, the learning factory can dynamically adapt to the individual skill levels and learning styles of each student, ensuring optimal knowledge acquisition and retention. The use case presented in this paper centers around the cybersecurity challenges faced by an electrical company. By focusing on a practical use case within the electrical industry, this initiative aims to equip students with the knowledge and skills necessary to effectively protect critical infrastructure against cyber threats.

Keywords

Cybersecurity, learning factory, cybersecurity awareness, cybersecurity training, learning, ontology, training, networks

1. Introduction

Cybersecurity risks are increasing in South Africa and pose a threat to critical infrastructure, especially in the electrical industry. Recent studies indicate that ransomware and data breaches have increased in South Africa, impacting the country's critical infrastructure's vulnerability [17], [23]. Traditional cybersecurity training approaches are not sufficient in offering students tailored experiences that simulate real-world situations. To solve this and improve upon traditional methods for cybersecurity training, we propose an ontology-driven Cybersecurity Learning Factory (CLF). With the CLF, students' learning will be tailored to adjust to their skill levels and preferences. The CLF will be demonstrated with use-cases from the electrical domain. This will result in improving learners' knowledge and skills against evolving cyber threats for the aforementioned domain.

The remainder of the paper is as follows. Section 2 reviews related works on ontologies in cybersecurity, electrical sector cybersecurity awareness approaches, and Learning Factories in the context of cybersecurity training. The foundational architecture alongside experiential process of the CLF follows in Section 3. Section 4 demonstrates usage of the architecture and experiential learning process. Finally, in Section 5 we conclude.

2. Related Works

The problem at hand, that traditional cybersecurity training approaches are not sufficient to enable learners to defend infrastructure against cyber threats, requires an understanding of various disciplines, i.e., ontologies in cybersecurity, learning factories, and cybersecurity awareness approaches.

2.1. Ontologies in the Cybersecurity domain

Ontologies are structured frameworks that help organize knowledge, define concepts, and specify relationships within a specific domain [8]. They provide a formal representation of knowledge using a hierarchical structure of classes, subclasses, properties, and instances [6], [8]. This structured representation allows machines to understand, reason about, and manipulate information within a particular context [6].

In the field of knowledge representation, ontologies are crucial for promoting interoperability between different systems and applications by establishing a common vocabulary and shared understanding of a domain [5], [7]. They are fundamental for various artificial intelligence applications, such as semantic web technologies, natural language processing, and expert systems, by facilitating knowledge sharing, integration, and reuse. [7], [22]. Additionally, ontologies improve information retrieval, inference, and decision-making processes by organizing and formalizing knowledge in a machine-readable format [22].

In the ever-changing landscape of cybersecurity, where threats evolve rapidly and attack vectors become more sophisticated, ontologies offer a strategic advantage in enhancing security defenses and protecting digital assets. By providing a structured framework for organizing and representing cybersecurity knowledge, ontologies play a crucial role in improving security operations, from threat detection to incident response. Some benefits of using ontologies in cybersecurity include [10], [18], [19]:

- **Standardization**: Establishing a common vocabulary and conceptual framework within the cybersecurity domain to enhance communication and understanding.
- **Interoperability**: Enabling seamless integration and exchange of information between different security systems.
- **Knowledge Sharing and Collaboration**: Facilitating the sharing of cybersecurity knowledge, best practices, and threat intelligence.
- **Automated threat detection and response**: Automating threat detection and response processes using machine-readable representations of threats, attack patterns, and security controls.
- **Semantic Enrichment of Security Data**: Enhancing the quality and relevance of security analytics, incident response, and decision-making processes by adding contextual information and relationships to security data.

- **Enhanced Situational Awareness**: Improving situational awareness for security analysts and decision-makers by structuring and organizing cybersecurity information effectively.
- **Adaptive and Scalable Security Solutions**: Providing a flexible framework that can adapt to evolving cybersecurity requirements and scale to meet the growing complexity of security landscapes.

Existing cybersecurity ontologies play a crucial role in organizing and representing knowledge about cybersecurity concepts, threats, and defenses in a structured manner [14],[18]. These ontologies provide a standardized framework for describing and categorizing various elements of cybersecurity, facilitating information sharing, analysis, and decision-making in the field. Examples of some notable cybersecurity ontologies are as follows:

- **Unified Cybersecurity Ontology (UCO)**: A comprehensive ontology developed by researchers to represent cybersecurity-related entities, relationships, and attributes. It aims to integrate diverse cybersecurity data sources and enable interoperability between different cybersecurity tools systems [20].
- **Cybersecurity Vulnerability Ontology (CVO)**: A structured framework that categorizes and organizes information related to cybersecurity vulnerabilities in a systematic manner [19]. By utilizing semantic technologies, the CVO aims to provide a comprehensive and standardized representation of vulnerabilities, thereby enhancing communication, analysis, and decision-making processes within the cybersecurity community [19].
- **Cyber Ontology and Conceptual Framework (CYBOK)**: An upp ontology for cybersecurity education, research, and practice, which covers various topics, from risk management to incident response [18].
- **Cybersecurity Framework Ontology (CSFO)**: This ontology is based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework. It provides a structured representation of cybersecurity functions, categories, and subcategories defined by the framework, helping organizations assess and improve their cybersecurity posture [15].

By using ontologies, organizations can strengthen their cybersecurity defenses, adapt to emerging threats, and manage risks more effectively in the complex digital environment. There are a number of ontologies for the cybersecurity domain; these vary in content and terminology.

2.2. Electrical Sector Cybersecurity Awareness

The electrical industry is facing a significant problem due to the widespread lack of awareness about cybersecurity among its stakeholders. As the industry adopts more digital technologies and interconnected systems, the risk of cyber threats targeting critical infrastructure is increasing rapidly [13]. Unfortunately, many professionals in the electrical

sector are not familiar with cybersecurity risks and best practices needed to protect these systems [13]. This lack of awareness is mainly because the industry has historically focused more on physical safety rather than cybersecurity, leaving vulnerabilities unaddressed and systems open to potential cyber-attacks [2], [3].

Furthermore, the complexity of electrical infrastructure, which includes legacy systems and various stakeholders, makes the cybersecurity challenge even more difficult. Many components of the electrical grid were not initially designed with cybersecurity in mind, making them easy targets for malicious actors [4], [13]. Additionally, the interconnected nature of the electrical sector, which relies on other critical infrastructure sectors like telecommunications and transportation, increases the potential impact of cyber-attacks [4]. Without a concentrated effort to enhance cybersecurity awareness and resilience in the electrical sector, the industry remains at risk of cyber threats that could disrupt operations, compromise safety, and cause widespread economic damage.

2.3. Learning Factories

The concept of learning factories originated from the manufacturing sector. These educational environments aim to provide hands-on training, experiential learning opportunities, and facilitate continuous improvement and innovation [24], [25].

2.3.1. Manufacturing Learning Factories

Learning factories in the manufacturing domain were traditionally used as educational facilities that simulated real-world production environments for training purposes. These facilities integrate various technologies, such as automation systems, robotics, and data analytics, to provide hands-on experience in manufacturing processes and operations [12], [21]. They serve as experiential learning platforms where students and professionals can gain practical skills, problem-solving abilities, and insights into industry best practices, preparing them for careers in manufacturing.

2.3.2. Cybersecurity Learning Factories

The use of learning factories in the cybersecurity domain is relatively new. In 2023, researchers proposed learning factories for the cybersecurity domain [24]. By utilizing newer techniques for knowledge development, learning factories offer a fresh perspective on cybersecurity training, removing barriers and fostering a nurturing learning environment [25]. Learning factories provide simulated environments where individuals can gain hands-on experience in solving real-world cybersecurity challenges, aiming to prepare them for actual workplace scenarios.

The purpose of CLFs is to provide practical, experiential learning opportunities for cybersecurity professionals to develop critical skills and competencies required in the industry. By simulating realistic cybersecurity scenarios and environments, CLFs enable participants to practice applying concepts, tools, and cognitive skills to solve actual cybersecurity problems. These simulated environments facilitate hands-on experience in a controlled setting, preparing individuals for the complexities of the cybersecurity landscape

[25]. Additionally, CLFs leverage Information and Communication Technology (ICT) to offer innovative teaching methodologies, such as gamification, virtual or hybrid collaborative platforms, animation, and simulation techniques, to enhance learning outcomes and engagement [1]. Through the use of dynamic and interactive ICT platforms, CLFs provide a rich learning experience that promotes knowledge retention, skills development, and practical application in the field of cybersecurity [24]. By immersing students and practitioners in simulated cyber threat scenarios, CLFs offer a safe and controlled environment for developing skills in threat detection, incident response, and cybersecurity strategy development.

Despite the numerous advantages of learning factories for practical skills development in various domains, their application in cybersecurity training remains limited. While the recent proposal in 2023 by Veerasamy et al. introduced the concept of learning factories for cybersecurity, their use in this field is still in its early stages [24].

2.4. Concluding Remarks

Traditional cybersecurity approaches emphasize technical skills such as penetration testing and vulnerability assessment skills. These skills may not enable learners to handle the human aspects of cyberattacks such as continuous social engineering [9]. Furthermore, existing cybersecurity training approaches usually omit learners' knowledge levels and tailored content for specific roles and levels (operational vs. executive) within the electrical company. These oversights could lead to inadequate cybersecurity training [3].

In terms of learning factories, most of them focus on general manufacturing processes, lacking the domain-specific knowledge required for cybersecurity and the electrical sector. Hence existing learning factories can't be used for training for cybersecurity threats in this sector.

The literature review revealed various cybersecurity ontologies, Having various domain ontologies means there is a lack of standardization which makes it difficult to integrate these ontologies into cybersecurity systems. Furthermore, cybersecurity issues and terminology could vary across different sectors (e.g., electrical vs. finance), and domain ontologies might need tailoring or extension to effectively address the specific needs of a particular domain. Ontologies to be used in the electrical domain would need to refer to controls for access control mechanisms for SCADA systems, intrusion detection systems for electrical networks, and segmentation strategies to isolate critical components. The principles of ontology modularisation [11] need to be applied to existing cybersecurity ontologies for usage in the electrical domain.

3. Ontology-driven Cybersecurity Learning Factory

Traditional methods are not sufficient to deliver effective cybersecurity training as they fail to provide realistic and personalized learning experiences [3]. To address this challenge, we propose the development of an Ontology-Driven CLF. This approach introduces the use of ontologies to create a contextual and adaptable training environment specifically for the cybersecurity needs of the electrical sector.

3.1. Foundational Architecture

The effectiveness of the CLF is based on its underlying foundational architecture, which has been designed to deliver a dynamic and personalized learning experience using Semantic Web technologies and domain knowledge. This section introduces the core components of the CLF, and a visual representation is shown in Figure 1 and Figure 2.

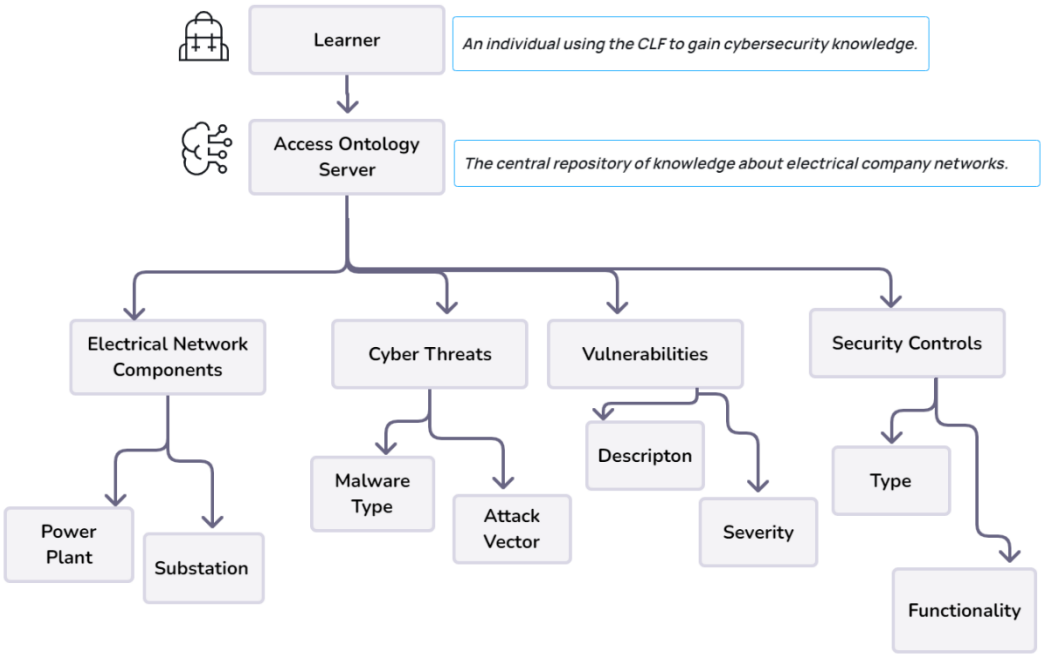

Figure 1: A learner's interaction with the ontology server.

3.1.1. Ontology Server

This acts as the central knowledge base of the CLF. It contains a collection of interlinked ontology modules that model various aspects of the training environment. These modules need to be represented in a variant of an ontology language that offers a good balance of expressivity, computational completeness and decidability.

- **Electrical Company Network Module**: This ontology module represents the domain of the structure of a typical electrical company network, including components like power plants, substations, distribution lines, and control systems. It defines the relationships between these components and their functionalities.
- **Cyber Threat Module**: This ontology describes various cyber threats relevant to electrical companies. It categorizes threats by type (e.g., malware, phishing), attack vectors (e.g., social engineering, zero-day exploits), and potential impact (e.g., data breaches, disruption of power supply, safety, monetary loss). This ontology also identifies potential vulnerabilities within the electrical company network components and systems. It describes the specific weaknesses that could be exploited by cyberattacks and the severity of each vulnerability.

- **Security Control Module**: This ontology module presents various security controls that can be implemented to mitigate cyber threats and vulnerabilities. It defines the functionalities of different controls (e.g., firewalls, intrusion detection systems, access controls) and their effectiveness against specific threats.

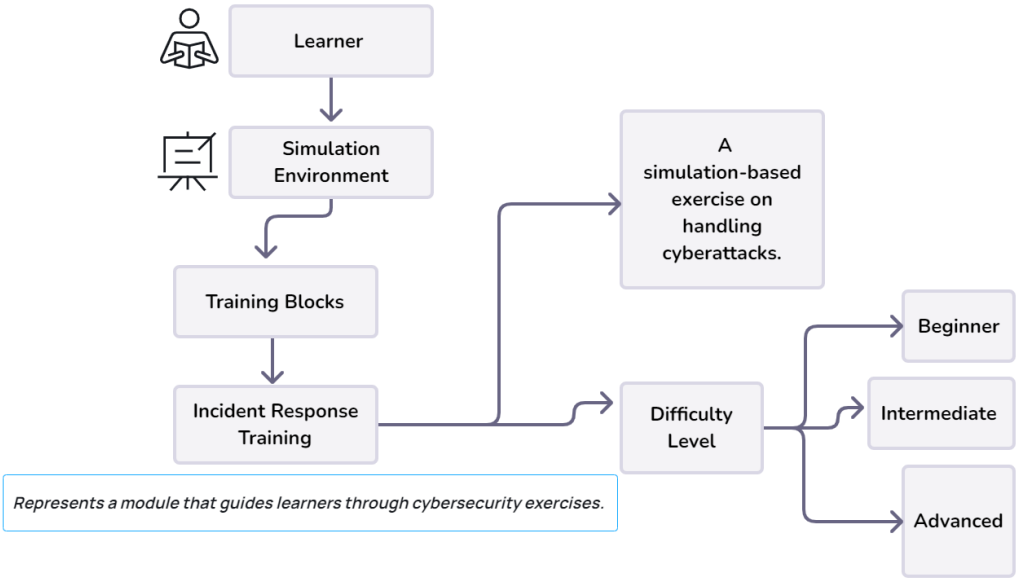

Figure 2: A learner's interaction with the simulation environment.

3.1.2. Simulation Environment

This component is a software-based replication of a realistic electrical company network environment. It uses software to simulate the behavior of network components, including normal operations and potential security incidents. The simulation environment interacts with the ontologies to dynamically adjust scenarios based on learner actions.

3.1.3. Training Blocks

The CLF uses a collection of interactive training blocks that guide learners through various cybersecurity tasks. Training blocks are pieces of content (activities, exercises, labs etc.) that a learner engages with. These blocks use the ontology modules to create content and difficulty based on individual needs. Examples include:

- **Incident Response Training**: Blocks simulate cyberattacks and guide learners through the general incident response process of detection, containment, eradication, and recovery.
- **Vulnerability Assessment and Penetration Testing (VAPT)**: These blocks provide hands-on experience with identifying vulnerabilities within the simulated network and attempting to exploit them in a controlled environment.

- **Security Control Implementation**: Learners can experiment with implementing various security controls within the simulated environment and observe their impact on the overall security posture of the environment.

Relevant training blocks can be generated based on the current cybersecurity threat landscape and the domain at hand. For instance, for the electrical domain the above training blocks are applicable whereas if the domain was the finance sector, the training blocks could expand to include those for data breaches, compliance training, and whatever else is relevant. The ontology modules hold the components together. By providing a shared, machine-processable understanding of the electrical company network, threats, vulnerabilities, and controls, the modules enable the CLF to create a dynamic and adaptable training experience. Learners can interact with the simulated environment, and the system can adjust the scenario based on their actions by querying the relevant ontologies. This allows for a more engaging experiential learning process compared to traditional methods.

3.2. Experiential Learning Process

We have documented the experiential learning process to create an improved learning experience for cybersecurity training. This section outlines the steps involved in utilizing the CLF for training, demonstrating how ontologies enable adaptable training experiences for learners. A high-level overview of the process is shown in Figure 3.

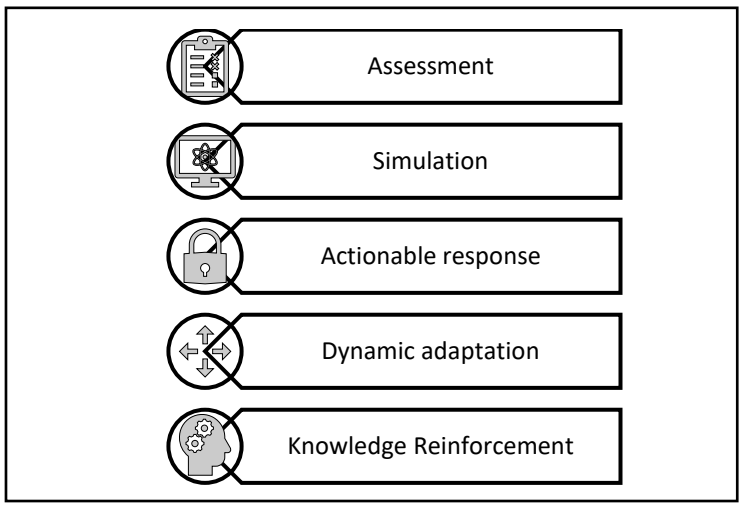

Figure 3: An overview of the experiential learning process.

- **Assessment**: The learning journey begins with an initial assessment that measures the learner's existing knowledge and skillset. This assessment uses the ontologies to generate personalized questions which supports the system to tailor the training experience. Based on the assessment results, learners can choose from various scenarios.
- **Simulation**: Once a scenario is chosen, the learner is presented with a realistic simulation environment replicating an electrical company network. The system leverages the Cyber Threat Ontology to dynamically introduce

cyberattacks based on the chosen scenario. This allows for a diverse but applicable range of threats to be simulated for the electrical domain.

- **Actionable Response**: As the learner interacts with the simulation environment, their actions are monitored. The ontology modules play a role here as well. The Security Control Ontology can suggest appropriate security controls based on the identified threat and the learner's existing security posture within the simulation (as a result of the learner's choices). Learners can then experiment with implementing these controls, observing their impact on the simulated scenario of the environment.
- **Dynamic Adaptation**: The ontology modules allow the system to adapt the training scenario based on the learner's decisions and actions. For instance, if a learner chooses to implement a firewall as a control, the simulation environment might adjust to target a different network component causing the initial control (enabling the firewall) to be bypassed. This forces the learner to adapt their approach.
- **Knowledge Reinforcement**: Following the simulated attack, the learner undergoes a debriefing session. This session again uses the ontology modules to provide feedback on the learner's choices, highlighting successful strategies and areas for improvement.

3.3. CLF's FAIR Guidelines

In adherence to the Findable, Accessible, Interoperable, Reusable (FAIR) principles, this paper's accompanying research artifacts will be made openly available through an appropriate online repository, i.e., the Repository of Ontologies for MULtiple USes (ROMULUS)[1]. The artifacts for this paper are: 1. the architecture diagram, and 2. the experiential learning process model.

4. Use-Case: Electrical Domain

Successful cyberattacks on electrical companies can have a devastating impact on critical infrastructure and public safety. As such, cybersecurity training in the electrical domain is necessary. This CLF provides a means for enhancing cybersecurity readiness in this sector and demonstrative examples follow.

4.1. Data Breach Scenario

This scenario explores a cyberattack targeting a fictional electrical company, "Volts" aimed at stealing sensitive data and manipulating internal systems.

- Assessment: The learner, Sarah, begins with an assessment that measures her knowledge of cybersecurity principles and electrical grid security measures. The ontologies personalize the assessment, focusing on areas relevant to data security

[1] thezfiles.co.za/ROMULUS/home.html

and access controls. Based on the assessment and her interests, Sarah selects a scenario titled "Data Breach" from the CLF's library.

- Simulation: Upon selection, Sarah is presented with a realistic simulation environment replicating Volt's network. The Cyber Threat Ontology introduces a layered attack. Malicious attackers might exploit vulnerabilities on a legacy software application used by Volt to access sensitive data about the power grid.
- Actionable Response: As Sarah interacts with the simulation, the Security Control Ontology identifies potential mitigation strategies. She can choose to implement measures like enabling multi-factor authentication to strengthen login security. Additionally, the ontology might suggest reviewing the security posture of the vulnerable application and implementing software patches to address known vulnerabilities. Sarah can experiment with these controls within the simulation, observing their effectiveness in preventing the data breach attempt.
- Dynamic Adaptation: The ontology modules enable the CLF to adapt the scenario dynamically. For instance, if Sarah successfully implements multi-factor authentication, the attackers might shift tactics, attempting to exploit a different user vulnerability, such as social engineering an employee to gain access. This forces Sarah to consider alternative security measures beyond just technical controls.
- Knowledge Reinforcement: Following the simulation, Sarah participates in a debriefing session. The debriefing utilizes the ontologies to highlight the importance of a layered security approach, combining technical controls with other controls.

4.2. Ransomware Scenario

This scenario also explores a cyberattack targeting the same fictional electrical company, "Volts", in the previous example, with the intention of gaining money.

- Assessment: Continuing with the learner, Sarah, the CLF initiates with an assessment tailored to measure her understanding of ransomware threats, incident response procedures, and backup strategies within the sector. The ontologies generate questions relevant to these areas, as her personalized assessment.
- Simulation: After the assessment, Sarah explores the Ransomware Attack block from the CLF's repository. The simulation environment immerses Sarah into the virtual infrastructure of Volts, where a ransomware strain has infiltrated the company's systems. The Cyber Threat Ontology plays a role in simulating the attack vectors, such as email phishing campaigns, and compromised vendor software.
- Actionable Response: Sarah is tasked with responding to the ransomware attack within the simulation. The Security Control Ontology suggests various response actions, such as isolating infected systems, initiating data recovery from backups, and communicating with stakeholders about the incident. Sarah implements the control of isolating infected systems.
- Dynamic Adaptation: The CLF dynamically adjusts the scenario based on Sarah's response to isolate the infected system. The simulation shows that the attacker had already embedded malicious code within the network, and that these files have

spread the ransomware elsewhere. This dynamic adaptation encourages Sarah to adapt her response strategy.

- Knowledge Reinforcement: Following the simulation, Sarah engages in a debriefing session where the ontologies provide detailed feedback on her response actions. The session emphasizes the importance of regular data backups, software patch management, data loss prevention etc. for mitigating ransomware attacks.

4.3. Discussion: Experiential learning using ontologies

Through these scenarios, learners are able to gain valuable insights into data security and the importance of a comprehensive approach to cybersecurity within the electrical sector. The dynamic adaptation of the scenarios, based on learner choices, are a true reflection of the nature of cyberattacks. Learners encounter more complex situations as they progress, forcing them to change their strategies regarding potential attacker tactics.

Ontologies allows for personalized assessments to measure a learner's existing knowledge specific to cybersecurity principles and the accompanying domain, i.e., an electrical grid security. This ensures the training focuses on areas where the learner needs the most improvement. The context-specific recommendations for security controls and response actions within the electrical grid domain ensures that the suggested controls are relevant for mitigating cyber attacks. By combining experiential learning with dynamic adaptation, personalized assessments, and ontology-driven guidance, the CLF equips learners like Sarah with the skills required to effectively address cyber threats in the electrical domain.

It is also important to note the benefit offered with the ontological approach in leu of a regular database or knowledge graph. Ontologies are expressed in logical languages like OWL which allow for automated reasoning. This enables the CLF to draw inferences and conclusions based on the knowledge stored in it. For example, if the ontology defines that "firewalls mitigate malware attacks" and the simulation environment detects a malware attack, the CLF can infer and suggest that a firewall activation is a recommended security response.

5. Conclusion

In this paper, we presented a foundational architecture and experiential learning process for an Ontology-Driven CLF, which can be adapted for specific training needs within the electrical sector or potentially serve as a starting point for developing CLFs in other domains. This novel approach addresses the limitations of traditional training methods that often fail to provide a realistic learning experience. The CLF's dynamic adaptation feature, driven by ontologies, mimics the ever-evolving nature of cyberattacks, forcing learners to adapt their strategies and think critically about potential attacker tactics as they progress through increasingly complex scenarios.

Using ontologies allows for fixing knowledge gaps specific to cybersecurity principles and electrical grid security for learners. This ensures that the training focuses on areas where individual learners need improvement; a typical cybersecurity engineer may not be an expert on the electrical domain. Additionally, the ontologies provide context-specific

recommendations for security controls, ensuring that the suggested solutions are relevant and effective against the specific cyber threats faced within the electrical domain.

Future work includes operationalizing the proposed architecture and learning process. This would involve exploring existing ontologies in the cybersecurity domain such as UCO, CVO, etc. It is also worthwhile to explore best practice threat frameworks and models in the cybersecurity domain such as the Mitre Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK), towards developing and maintaining the ontology modules for the CLF.

References

[1] Abele, E. M. (2019). Best Practice Examples. In Learning Factories: Concepts, Guidelines, Best-Practice Examples (pp. 335-459). Springer.

[2] Chowdhury, N., & Gkioulos, V. (2021). Cyber security training for critical infrastructure protection: A literature review. Computer Science Review, pp. 40, 100361.

[3] Chowdhury, N., Nystad, E., Reegård, K., & Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. International Journal of Safety and Security Engineering, 299-310.

[4] de Azevedo, G. P. (2020). Addressing the cybersecurity challenges of electrical power systems of the future. In 12th International Conference on Cyber Conflict (CyCon) (pp. Vol. 1300, pp. 293-308). IEEE.

[5] Deloule, F., & Roche, C. (1995). Ontologies and knowledge representation. IEEE International Conference on Systems, Man and Cybernetics. Intelligent Systems for the 21st Century (pp. Vol. 5, pp. 3857-3862)). IEEE.

[6] Gangemi, A. G. (2002). Sweetening ontologies with DOLCE. International conference on knowledge engineering and knowledge management (pp. pp. 166-181). Berlin, Heidelberg: Springer.

[7] Grimm, S. (2009). Knowledge representation and ontologies. In Scientific data mining and knowledge discovery: Principles and foundations (pp. pp. 111-137). Berlin, Heidelberg: Springer.

[8] Gruber, T. R. (1993). A translation approach to portable ontology specifications. Knowledge acquisition, 5(2), 199-220.

[9] Hatzivasilis, G. I. (2020). Modern aspects of cyber-security training and continuous adaptation of programmes to trainees. Applied Sciences, 10(16), 5702.

[10] Kagal, L. F. (2003, October). A policy based approach to security for the semantic web. International semantic web conference (pp. pp. 402-418). Berlin, Heidelberg: Springer.

[11] Khan, Z. C., & Keet, M. (2015). An empirically-based framework for ontology modularisation. Applied Ontology, 10(3-4), 171-195.

[12] Lamancusa, J. S.-C. (1997). The learning factory—A new approach to integrating design and manufacturing into the engineering curriculum. Journal of engineering Education, 86(2), 103-112.

[13] Leszczyna, R. (2019). Cybersecurity in the electricity sector. Managing Critical Infrastructure. Gdansk, Polonia.: Springer.

[14] Oltramari, A., Cranor, L. F., Walls, R. J., & McDaniel, P. D. (2014). Building an ontology of cyber security. STIDS, 2014, 54-61.

[15] Pascoe, C., Quinn, S., & Scarfone, K. (2024). The NIST Cybersecurity Framework (CSF) 2.0, NIST Cybersecurity White Papers (CSWP). Retrieved from National Institute of Standards and Technology: https://doi.org/10.6028/NIST.CSWP.29

[16] Pease, A. N. (2002). The suggested upper merged ontology: A large ontology for the semantic web and its applications. AAAI-2002 workshop on ontologies and the semantic web, (pp. Vol. 28, pp. 7-10).

[17] Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. The African Journal of Information and Communication, 28, 1-21.

[18] Rashid, A. N. (2021, February 2). CyBOK Mapping Framework How to map concepts in academic and professional programmes to the Cyber Security Body of Knowledge. Retrieved from Cyber Security Body of Knowledge: https://www.cybok.org

[19] Syed, R. (2020). Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. Information & Management,, 57(6), 103334.

[20] Syed, Z., Padia, A., Finin, T., Mathews, L., & Joshi, A. (2016). UCO: A unified cybersecurity ontology. Proceedings of the AAAI Workshop on Artificial Intelligence for Cyber Security. Phoenix: AAAI Press.

[21] Tisch, M. R. (2015). Learning factory morphology–study of form and structure of an innovative learning approach in the manufacturing domain. Turkish online journal of educational technology, 14(Special Issue 2), 356-363.

[22] Uschold, M. &. (1996). Ontologies: Principles, methods and applications. The knowledge engineering review, pp. 11(2), 93-136.

[23] Van Niekerk, B. (2017). An analysis of cyber-incidents in South Africa. The African Journal of Information and Communication, 20, 113-132.

[24] Veerasamy, N., Mkhwanazi, T., & Dawood, Z. (2023, February). Towards the usefulness of learning factories in the cybersecurity domain. International Conference on Cyber Warfare and Security, (pp. Vol. 18, No. 1, pp. 412-419).

[25] Veerasamy, N., Mkhwanazi, T., & Khan, Z. C. (2023, September). Digital Innovation Through Cybersecurity Learning Factories. ECKM 2023 24th European Conference on Knowledge Management Vol 2. Academic Conferences and publishing limited.