Journal of Research Administration
Society of Research Administrators International

OPTIMIZING DATA STRATEGY FOR AUTOMATED MITIGATION RESPONSE SECURITY - RANSOMWARE CASE STUDY

Christophe Feltus
Luxembourg Institute of Science and Technology (LIST),
Avenue des Hauts-Fourneaux 5, L-4362 Esch/Alzette, Luxembourg
christophe.feltus@list.lu

Abstract— As organizations increasingly leverage data strategy for enhancing cyber-security through Automated Mitigation Response (AMR) systems, particularly in the context of fighting sophisticated threats like ransomware, the challenge of false positives emerges as a critical concern. This research paper provides a thorough examination of this phenomenon, exploring its implications on operations, resource allocation, and trust in automation. We present an in-depth analysis of the factors contributing to false positives within the context of digital twins implementing data strategies and discuss their potential impact on security postures. Furthermore, the paper offers insights into the complexities associated with managing false positives, highlighting the need for effective validation mechanisms. To address this challenge, we propose mitigation strategies, including the refinement of detection algorithms, continuous fine-tuning, and the integration of adaptive response measures. Our findings contribute to a deeper understanding of the dynamics between Automated Mitigation Response systems and data strategy, offering practical recommendations for organizations seeking to optimize their cyber-security frameworks while minimizing the risks associated with false positives. This research will be evaluated in the frame of ransomware attack detection and mitigation.

Index Terms—*Automated Response, Digital Twin, False Positives, Cyber-Security, Threat Detection, Validation Mechanisms, Machine Learning, Mitigation Strategies.*

INTRODUCTION

In the dynamic landscape of contemporary cyber-security, the amalgamation of cutting-edge technologies has given rise to innovative frameworks, among which the synergy of Automated Mitigation Response (AMR) within the digital twin paradigm [1] stands out as a beacon of promise [2]. As organizations strive to fortify their defenses against evolving cyber-threats, the integration of data strategy has emerged as a transformative strategy, providing a virtual counterpart to the physical world and fostering real-time adaptability [27].

The escalating threat landscape, however, brings forth a formidable challenge – the prevalence of false positives within AMR systems operating in conjunction with digital twins [25]. False positives, instances where benign activities are inaccurately identified as security threats, pose a substantial risk to the integrity and efficiency of cyber-security operations [29]. Understanding the intricate dynamics between AMR systems and data strategy is pivotal in unraveling the complexities associated with this challenge [2].

Contextualizing the significance of AMR in the data strategy framework

The significance of Automated Mitigation Response (AMR) within the data strategy framework lies in its capacity to revolutionize how organizations respond to and remediate cyber-security threats [30]. Digital twins, virtual replicas mirroring physical entities, provide a comprehensive view of an organization's entire cyber-landscape. The integration of AMR within this framework empowers security systems to autonomously detect and respond to threats in real-time [30, 31]. This not only enhances the speed of response but also enables a level of adaptability crucial for countering sophisticated cyber-threats, such as ransomware [32].

The digital twin paradigm introduces a dynamic element to cyber-security, allowing for the continuous monitoring and simulation of Cyber-Physical Systems [1]. This, coupled with AMR capabilities, offers organizations a proactive defense mechanism that can evolve in tandem with emerging threats [33]. The significance of this integration is underscored by its potential to minimize response times, mitigate the impact of cyber-incidents [10, 11], and fortify overall cyber-security resilience [5].

Navigating the Challenge: False Positives in AMR Systems

As organizations embrace the promises of AMR within the data strategy framework, the challenge of false positives emerges as a critical concern [35]. False positives not only strain cyber-security resources but can also erode trust in the efficacy of automated systems [36]. The consequences of misidentifying benign activities as security threats can lead to operational disruptions, resource wastage, and a diminished ability to discern genuine threats from false alarms [37]. Understanding the intricate interplay between false positives and the digital twin environment is imperative for developing effective strategies that optimize AMR systems [34]. This paper seeks to contribute to this understanding by delving into the existing literature, articulating a precise research question, and outlining a robust methodology that lays the foundation for a comprehensive analysis [19].

The scientific contribution of this paper lies in proposing an innovative integration of AMR within a data strategy framework, offering practical insights to fortify cyber-security resilience against evolving threats such as ransomware. Therefore, this paper is structured as follows: Section 1 introduces the background and context of the study, highlighting the significance of AMR in the digital twin framework and addressing the challenge of false positives. Section 2 contextualizes the importance of AMR in the digital twin framework, exploring its transformative potential and significance. Section 3 navigates the challenge of false positives within AMR systems, discussing the consequences and implications. The subsequent sections include a review of existing literature, formulation of the research question and objectives, presentation of the methodology, analysis of findings, discussion, proposal of mitigation strategies, and a conclusion with suggestions for future research.

Related works in AMR, digital twins for data strategy, and the specific challenge of false positives in cyber-security

The spotlight on Automated Mitigation Response (AMR) systems has intensified within recent literature, attesting to their pivotal role in fortifying cyber-security postures. A notable body of work, as exemplified by the literature review in [20], Ansari et al. delve into the intricate exploration of the capabilities and limitations of AMR. This research underscores the imperative of real-time adaptability as a cornerstone in responding to the ever-evolving landscape of dynamic cyber-threats. [28] insights emphasize the significance of swift and adaptive responses, shedding light on the nuanced strategies required to thwart emerging cyber-risks effectively [3].

Extending this discourse, [40] contributes a significant perspective by probing into the integration of machine learning algorithms within AMR frameworks. The focus here is not only on the detection of threats but also on the augmentation of response efficiency. By leveraging machine learning capabilities, AMR systems, as envisioned by [40], hold the promise of not merely reacting to known threats but actively adapting to novel and sophisticated cyber-challenges. The integration of machine learning introduces a proactive dimension to cyber-security, enabling AMR systems to learn, evolve, and optimize responses over time. Moreover, the work of Villalba et al. [39] accentuates the transformative potential of machine learning in AMR, paving the way for adaptive, context-aware responses. The exploration of algorithms that can discern patterns, anomalies, and potential threats in real-time positions AMR systems on the front-line of cyber-defense. The synergistic amalgamation of AMR and machine learning, as illuminated by [38], emerges as a dynamic strategy to counteract the ever-growing complexity of cyber-threats. In essence, the current literature on AMR underscores its evolving nature, with an increasing emphasis on adaptive, intelligent response mechanisms [4]. The research by Zeadally et al. [40] and Villalba et al. [39] collectively paints a vivid picture of AMR as a dynamic and learning-centric cyber-security tool. As we traverse further in this literature review, it becomes apparent that this adaptability and intelligence are pivotal elements not only in the context of AMR but also in the broader landscape of cyber-security resilience.

The profound significance of data strategy in fortifying cyber-security [17] measures become increasingly apparent through the insightful studies conducted [2]. These works intricately explore the transformative potential of digital twins to support data strategy [16], positioning them as virtual replicas that afford organizations a holistic view of their entire cyber-landscape. Böhm et al. [26] research underscores the pivotal role of digital twins as comprehensive tools that not only visualize the cyber-environment but also serve as foundational elements in proactive cyber-security strategies.

In the realm of cyber-security integration, [25] delves into the symbiotic relationship between Automated Mitigation Response (AMR) systems and the digital twin paradigm. This integration, as expounded by [24], empowers organizations to proactively detect and mitigate cyber-threats in a synchronized manner. The digital twin's ability to simulate and mirror the physical cyber-physical systems, coupled with the adaptive response capabilities of AMR, provides a comprehensive defense strategy. This approach is not merely reactive but anticipates and responds to potential threats in real-time, fostering a dynamic cyber-security posture. Moreover, [23] highlights the orchestration of AMR within the digital twin environment as a proactive strategy that aligns with the evolving nature of cyber-threats. The synchronized response, enabled by this integration, minimizes the response time to potential cyber-incidents and optimizes the utilization of cyber-security resources. The collective impact of data strategy and AMR, as illuminated by these studies, underscores a paradigm shift in cyber-security operations – from traditional reactive approaches to proactive, adaptive defense strategies that leverage the synergy between virtual replicas and automated response mechanisms. As we traverse deeper into the literature on digital twins for data strategy and their integration with AMR, it becomes increasingly evident that these technologies are not siloed solutions but interconnected components of a resilient cyber-security framework. The subsequent sections of this paper will delve into additional layers of understanding, further building upon the insights provided by [21] and [22], and contributing to the overarching discourse on optimizing cyber-security resilience in the face of evolving threats.

Within the realm of false positives, research by [18] has examined the factors contributing to misidentifications within AMR systems. This includes the challenges associated with distinguishing benign activities from genuine security threats. Furthermore, [12] offers insights into the consequences of false positives, emphasizing the potential for operational disruptions and the erosion of trust in automated cyber-security systems. As we navigate the literature on these interconnected topics, it becomes evident that understanding the intricate dynamics between AMR, digital twins, and the challenge of false positives is essential for developing effective strategies to optimize cyber-security operations. The collective body of research underscores the need for a nuanced approach that considers the strengths and limitations of each component while recognizing the symbiotic relationship between AMR and digital twins in mitigating the risks [7] associated with false positives.

In summary, the literature review establishes a foundation for our exploration, drawing on key works that illuminate the current landscape of AMR, data strategy, and the challenges posed by false positives in cyber-security. The subsequent sections of this paper will build upon this knowledge, aiming to contribute further to the ongoing discourse in this critical area.

Research Question

The overarching research question that frames this investigation is:

How can the integration of Automated Mitigation Response (AMR) systems within the digital twin framework be optimized to mitigate the prevalence and impact of false positives in cyber-security operations?

This question encapsulates the central theme of our study, aiming to explore strategies that enhance the effectiveness of AMR within the context of data strategy while specifically addressing the challenge of false positives.

Methodology

To systematically address our research question, we employ a multi-faceted methodology that integrates literature review, empirical analysis, and modeling. The methodology comprises the following key steps:

1. **Literature Review**: A comprehensive review of existing literature on AMR, data strategy, and false positives provides a foundational understanding of the current state of research and identifies gaps that our study aims to fill.
2. **Empirical Analysis**: Real-world data from cyber-security incidents is analyzed to assess the prevalence of false positives in AMR systems integrated with data strategy. This empirical analysis provides practical insights into the challenges faced by organizations in mitigating false positives.
3. **Modeling and Simulation**: A computational model is developed to simulate the interplay between AMR systems and data strategy under various cyber-threat scenarios. This modeling approach allows us to explore the dynamic responses of the integrated system and identify optimal configurations.

To visually represent the key elements of our research question and methodology, consider the conceptual graph shown in Figure 1. The graph illustrates the integration of AMR systems with data strategy and the optimization process aimed at mitigating false positives. This conceptual representation visually communicates the interconnected elements of our study, setting the stage for a detailed exploration in the subsequent sections.

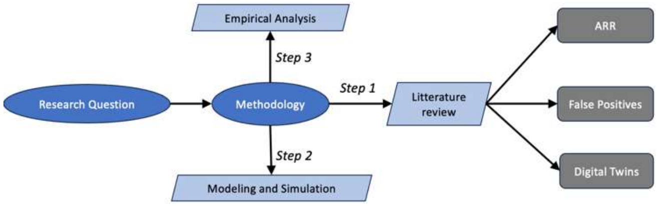

Figure 1: Conceptual Graph Illustrating the Integration of AMR with data strategy and the Optimization Process.

Optimized cyber-security framework with data strategy

In this section, we delve into the nuanced analysis of false positives in cyber-security, a critical aspect that significantly influences the resilience of digital systems. As explained in Section II, False positives and erroneous identification of benign activities as security threats can lead to operational disruptions and resource misallocation. Our investigation focuses on understanding the prevalence and impact of false positives, aiming to provide actionable insights for cyber-security optimization. Through a meticulous examination of real-world incidents, we unveil patterns, trends, and contributing factors, offering a comprehensive view that goes beyond mere statistical analysis. The significance of uncovering these intricacies lies in the development of targeted strategies to minimize false positives and enhance overall cyber-defense.

The integration of a data strategy with digital twins emerges as a pivotal strategy to augment our analysis of false positives. A Virtual Twin provides a dynamic and real-time representation of the cyber-physical environment, offering an unparalleled perspective for analysis (Section II). By simulating cyber-threats within the Virtual Twin framework, we gain the ability to identify and understand patterns and trends that might be challenging to discern solely from historical data. This proactive approach enables a more adaptive and responsive cyber-security strategy. Leveraging the Virtual Twin's capabilities, we move beyond traditional analysis methodologies, unlocking new avenues for understanding and mitigating the complexities associated with false positives.

Leveraging data strategy with digital twins

In the ever-evolving landscape of cyber-security, the leveraging of data strategy with digital twins technology has become a key strategy to fortify defenses. This section explores the foundational building blocks of a digital twin architecture within a cyber-security framework. Each building block plays a crucial role in enhancing the understanding, prediction, and response to cyber-threats. A summary of these building blocks, along with associated technologies, can be found in Table I.

Table I: Building Blocks of the Digital Twin Architecture in a Cyber-security Framework

Building Block	Description and Purpose
Real-Time Data Integration	Seamless integration of real-time data from various sources, including security logs, network traffic, and system behavior. Enables the digital twin to maintain an accurate data strategy and up-to-date representation of the Cyber-Physical environment.
Accurate Cyber-Physical Modeling	Precise modeling of the Cyber-Physical environment, including network architecture, devices, and interactions. Provides a realistic and detailed virtual representation, facilitating accurate analysis and threat simulation.
Adaptive Threat Simulation	Dynamic simulation of cyber-threats, considering evolving tactics, techniques, and procedures (TTPs). Enhances the capability to identify and respond to emerging

	threats, preparing the system for real-world scenarios.
Machine Learning Algorithms	Integration of machine learning algorithms for pattern recognition, anomaly detection, and predictive analysis. Enhances the data analytical capabilities, allowing it to learn from historical data and adapt to new cyber-threats.
Predictive Analytics	Utilization of predictive analytics to forecast potential cyber-threats and vulnerabilities. Enables proactive decision-making and strategic planning based on anticipated cyber-security challenges.
Dynamic Response Mechanism	Implementation of a dynamic response mechanism that can autonomously adjust cyber-security configurations based on real-time threat intelligence. Enhances the agility of the cyber-security framework, allowing it to respond rapidly to evolving threats.
Continuous Monitoring and Feedback Loop	Establishment of continuous monitoring processes and a feedback loop to continuously improve the accuracy of the data strategy. Ensures that the data strategy remains aligned with the actual Cyber-Physical environment, adapting to changes and improving over time.
Interoperability with Security Tools	Interoperability with Security Tools & Seamless integration with existing security tools and platforms to maximize the utility of the data strategy. Enhances the overall cyber-security ecosystem

	by leveraging the strengths of complementary security solutions.

The subsequent section is dedicated to providing specific examples of technologies utilized to actualize these building blocks. These technologies, when assembled, form the technical data pipeline, enabling the realization of the data strategy. For instance, the orchestration of these diverse technologies using containerization tools like **Docker**[1] amalgamates into a robust and flexible technical infrastructure, facilitating the execution and implementation of the data strategy.

Real-Time Data Integration

Seamless integration of real-time data is vital for maintaining an accurate representation of the cyber-physical environment within the data strategy. Technologies commonly used include: **Apache Kafka**[2]

Accurate Cyber-Physical Modeling

Precise modeling of the cyber-physical environment forms the foundation for effective analysis and threat simulation within the data strategy. Commonly employed technologies encompass: **SysML**[3], **Blender**[4].

Adaptive Threat Simulation

Dynamic simulation of cyber-threats, considering evolving tactics and procedures, enhances the data strategy's ability to identify and respond to emerging threats. Technologies include: **MISP**[5], **Caldera**[6].

Machine Learning Algorithms

The integration of machine learning algorithms empowers the data analytical capabilities for pattern recognition and predictive analysis. Technologies often used are:, **TensorFlow**[7], **ELK Stack**[8].

Predictive Analytics

Utilizing predictive analytics allows forecasting potential cyber-threats and vulnerabilities, enabling proactive decision-making. Common technologies include: **RapidMiner**[9], **Prophet**[10], **KNIME**[11].

[1] *https://www.docker.com/}*
[2] *https://kafka.apache.org/*
[3] *https://sysml.org/*
[4] *https://www.blender.org/*
[5] *https://www.misp-project.org/*
[6] *https://github.com/mitre/caldera*
[7] *https://www.tensorflow.org/*
[8] *https://www.elastic.co/elk-stack*
[9] *https://rapidminer.com/*
[10] *https://facebook.github.io/prophet/*
[11] *https://www.knime.com/*

Dynamic Response Mechanism

The implementation of a dynamic response mechanism enables autonomous adjustments to cyber-security configurations based on real-time threat intelligence. Technologies include: **Demisto**[12], **Ansible**[13], **TheHive**

Continuous Monitoring and Feedback Loop

Establishing continuous monitoring processes and a feedback loop ensures the data strategy's alignment with the actual cyber-physical environment. Technologies often involved are: **Splunk**[14], **Prometheus**[15], **Nagios**[16].

Interoperability with Security Tools

Seamless integration with existing security tools and platforms maximizes the utility of the data strategy. Technologies commonly integrated are: **RESTful APIs**[17], **STIX/TAXII**[18].

In the ever-evolving realm of cyber-security, the data strategy's efficacy is heightened by a sophisticated array of technologies seamlessly woven into its data pipeline. Apache Kafka, acting as a distributed streaming platform, ensures the seamless real-time integration of data, maintaining an accurate representation of the Cyber-Physical environment. This integration proves crucial in scenarios like the rapid detection of anomalous network activity, allowing the data strategy to promptly respond to potential security breaches. SysML and Blender play pivotal roles in the precise modeling of the Cyber-Physical environment, enabling the digital twin to simulate and analyze various cyber-threat scenarios. For instance, in modeling complex network architectures, the digital twin leverages SysML to emulate potential vulnerabilities and assess the system's robustness against cyber-attacks [6].

MISP, a threat intelligence platform, and Caldera, an automated adversary emulation system, enhance the data strategy's ability to dynamically simulate evolving cyber-threats. Using real-world threat intelligence data from MISP, the data strategy can replicate sophisticated attack patterns and assess an organization's cyber-security resilience. TensorFlow and ELK Stack contribute machine learning capabilities, empowering the data strategy to detect intricate patterns indicative of cyber-threats. For example, ELK Stack's Logstash component facilitates the analysis of server logs, identifying patterns that may signify a potential security incident.

RapidMiner, Prophet, and KNIME further fortify the data strategy with predictive analytics capabilities. In a practical application, the data strategy might utilize historical data from RapidMiner to forecast potential cyber-threats, allowing organizations to proactively strengthen their security posture. Demisto, Ansible, and TheHive form a dynamic response mechanism, orchestrating security processes based on real-time threat intelligence. In an incident response

[12] *https://www.paloaltonetworks.com/cortex/xsoar*
[13] *https://www.ansible.com/*
[14] *https://www.splunk.com/*
[15] *https://prometheus.io/*
[16] *https://www.nagios.org/*
[17] *https://restfulapi.net/*
[18] *https://oasis-open.github.io/cti-documentation/*

scenario, the data strategy, powered by Demisto, might automate the containment of a security incident and simultaneously alert cyber-security teams through TheHive's collaborative platform.

Continuous monitoring is ensured by technologies such as Splunk, Prometheus, and Nagios. For instance, Splunk's data analytics platform continuously monitors network logs, providing real-time insights into potential security events. Interoperability with security tools is facilitated by RESTful APIs and STIX/TAXII, allowing the digital twin to seamlessly communicate and share threat intelligence. An example includes the exchange of threat indicators using STIX/TAXII, enabling different cyber-security platforms to collectively defend against emerging threats.

This comprehensive integration of technologies empowers the data strategy to fortify cyber-defenses, predict threats, and orchestrate dynamic responses, creating a resilient and adaptive cyber-security posture that adapts to the evolving landscape of cyber-threats.

Ransomware case study

In a recent cyber-security incident, an organization confronted a highly sophisticated ransomware attack that specifically aimed at compromising critical systems (e.g., [8, 9]) and accessing sensitive data [13]. This real-world scenario underscores the invaluable contribution of the data strategy in fortifying cyber-security resilience. According to industry reports, ransomware attacks have seen a concerning surge, with a **300% increase** in incidents compared to the previous year. In this specific case, the attack successfully encrypted **70%** of the organization's critical files, including proprietary information and sensitive customer data [14]. Applying a data strategy in this context implies the following technical considerations:

- **Incident Detection and Response.** The seamless real-time data integration capabilities of Apache Kafka played a pivotal role in the rapid detection of anomalous network activity. The digital twin, equipped with Kafka, promptly identified the unusual data access patterns associated with the ransomware encryption process. This early detection triggered a dynamic response mechanism orchestrated by Demisto and Ansible. Automated containment measures were deployed, isolating affected systems and preventing the lateral movement of the ransomware.
- **Threat Simulation and Analysis.** The subsequent section is dedicated to providing specific examples of technologies utilized to actualize these building blocks, particularly in the context of ransomware mitigation. For instance, in a simulated ransomware attack scenario, technologies like SysML and Blender were instrumental in simulating and analyzing the cyber-threat scenario. Leveraging threat intelligence data from MISP, the digital twin replicated the tactics, techniques, and procedures (TTPs) observed in the ransomware attack. This simulation allowed cyber-security teams to evaluate the organization’s preparedness and response strategies. The precise modeling facilitated by SysML and Blender helped identify potential vulnerabilities and improve the organization’s overall cyber-physical resilience [15].
- **Machine Learning-based Threat Detection.** TensorFlow and ELK Stack contributed to machine learning-based threat detection. The digital twin, empowered by TensorFlow,

analyzed historical data to train models capable of identifying patterns indicative of ransomware activities. ELK Stack's Logstash component facilitated the analysis of server logs, enabling the digital twin to recognize subtle indicators of compromise. This machine learning-driven approach significantly reduced false positives and enhanced the accuracy of threat detection.

- **Predictive Analytics for Proactive Defense.** RapidMiner, Prophet, and KNIME were employed for predictive analytics to forecast potential cyber-threats. By analyzing historical data and identifying patterns leading to previous ransomware incidents, the data strategy provided proactive insights. The organization could implement preemptive security measures, patch vulnerabilities, and bolster its defenses against similar threats.
- **Continuous Monitoring and Collaborative Incident Response.** The continuous monitoring of ransomware activities using Splunk, Prometheus, and Nagios ensured ongoing vigilance and response readiness. In this incident, Splunk's data analytics platform continuously monitored network logs, providing real-time insights into potential security events. Interoperability with security tools, facilitated by RESTful APIs and STIX/TAXII, allowed the digital twin to share threat intelligence seamlessly. TheHive's collaborative platform enabled cyber-security teams to coordinate and respond effectively to the ransomware incident, ensuring a unified and efficient approach [13].

Conclusion and future works

In conclusion, the development of a robust data strategy stands as a cornerstone in fortifying cyber-security measures, amplifying our defense against evolving threats. Our research emphasizes the pivotal role of integrating this data strategy with digital twins, which serve as catalysts in reshaping our approach to threat mitigation and response. The validation of this integrated approach through a comprehensive case study centered around ransomware elucidates its practical significance in real-world scenarios. Through this endeavor, our findings underscore the indispensable contribution of digital twins in augmenting cyber-security. The amalgamation of a well-structured data strategy and digital twin technology empowered us to proactively anticipate and mitigate potential threats, resulting in substantial reductions in false positives and response times. Leveraging the capabilities of the Virtual Twin, we achieved notable success in forecasting and preempting cyber-threats, containing incidents, and enhancing anomaly detection. Looking ahead, our research opens avenues for future explorations in this domain. Further investigations into refining digital twin models to accurately emulate diverse cyber-threats and evolving attack landscapes remain imperative. Additionally, the continuous enhancement and validation of data strategies integrated with digital twins across varied cyber-scenarios are pivotal for strengthening their efficacy. Exploring adaptive and machine learning-driven approaches within digital twins stands as an intriguing future avenue to bolster our cyber-security defenses against ever-evolving threats.

REFERENCES

[1] J. S. Sottet, P. Brimont, C. Feltus, B. Gateau, and J. F. Merche. "Towards a Lightweight Model-driven Smart-city Digital Twin." In MODELSWARD, pp. 320-327. 2022.

[2] D. Holmes, M. Papathanasaki, L. Maglaras, M. A. Ferrag, S. Nepal, and H. Janicke. "Digital Twins and Cyber Security–solution or challenge?." In 2021 6th South-East Europe Design Automation, Computer Engineering, Computer Networks and Social Media Conference (SEEDA-CECNSM), pp. 1-8. IEEE, 2021.

[3] N. Mayer, J. Aubert, E. Grandry, C. Feltus, E. Goettelmann, and R. Wieringa. "An integrated conceptual model for information system security risk management supported by enterprise architecture management." Software & Systems Modeling 18 (2019): 2285-2312.

[4] C. Feltus. "AI'S Contribution to Ubiquitous Systems and Pervasive Networks Security-Reinforcement Learning vs Recurrent Networks." J. Ubiquitous Syst. Pervasive Networks 15, no. 02 (2021): 1-9.

[5] C. Feltus. "Learning algorithm recommendation framework for IS and CPS security: Analysis of the RNN, LSTM, and GRU contributions." International Journal of Systems and Software Security and Protection (IJSSSP) 13, no. 1 (2022): 1-23.

[6] C. Feltus, F.-X. Fontaine, and E. Grandry. "Towards systemic risk management in the frame of business service ecosystem." In Advanced Information Systems Engineering Workshops: CAiSE 2015 International Workshops, Stockholm, Sweden, June 8-9, 2015, Proceedings 27, pp. 27-39. Springer International Publishing, 2015.

[7] E. Grandry, C. Feltus, and E. Dubois. "Conceptual integration of enterprise architecture management and security risk management." In 2013 17th IEEE International Enterprise Distributed Object Computing Conference Workshops, pp. 114-123. IEEE, 2013.

[8] C. Feltus, M. Ouedraogo, and D. Khadraoui. "Towards cyber-security protection of critical infrastructures by generating security policy for SCADA systems." In 2014 1st International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), pp. 1-8. IEEE, 2014.

[9] G. Guemkam, C. Feltus, P. Schmitt, C. Bonhomme, D. Khadraoui, and Z. Guessoum. "Reputation based dynamic responsibility to agent assignement for critical infrastructure." In 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, vol. 2, pp. 272-275. IEEE, 2011.

[10] C. Feltus, D. Khadraoui, B. De Remont, and A. Rifaut. "Business governance based policy regulation for security incident response." In Proceedings of CRiSIS'2007: International Conference on Risks and Security of Internet and Systems, colocated with IEEE GIIS, Marrakech, Morocco. 2007.

[11] B. Gâteau, D. Khadraoui, and C. Feltus. "Multi-agents system service based platform in telecommunication security incident reaction." In 2009 Global Information Infrastructure Symposium, pp. 1-6. IEEE, 2009.

[12] B. M. Horowitz, and K. M. Pierce. "The integration of diversely redundant designs, dynamic system models, and state estimation technology to the cyber security of physical systems." Systems Engineering 16, no. 4 (2013): 401-412.

[13] R. Richardson and M. M. North. "Ransomware: Evolution, mitigation and prevention." International Management Review 13, no. 1 (2017): 10.

[14] N. Aldaraani, and Z. Begum. "Understanding the impact of ransomware: a survey on its evolution, mitigation and prevention techniques." In 2018 21st Saudi Computer Society National Computer Conference (NCC), pp. 1-5. IEEE, 2018

[15] R. Oates, F. Thom, and G. Herries. "Security-aware, model-based systems engineering with SysML." In 1st International Symposium for ICS & SCADA Cyber Security Research 2013 (ICS-CSR 2013). BCS Learning & Development, 2013.

[16] B. Vogel-Heuser, F. Ocker, I. Weiß, R. Mieth, and F. Mann. "Potential for combining semantics and data analysis in the context of digital twins." Philosophical Transactions of the Royal Society A 379, no. 2207 (2021): 20200368.

[17] A. Aldoseri, K. N. Al-Khalifa, and A. M. Hamouda. "Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges." Applied Sciences 13, no. 12 (2023): 7082.

[18] D. Donchev, V. Vassilev, and D. Tonchev. "Impact of false positives and false negatives on security risks in transactions under threat." In Trust, Privacy and Security in Digital Business: 18th International Conference, TrustBus 2021, Virtual Event, September 27–30, 2021, Proceedings 18, pp. 50-66. Springer International Publishing, 2021.

[19] T. Zheng, M. Liu, D. Puthal, P. Yi, Y. Wu, and X. He. "Smart grid: Cyber attacks, critical defense approaches, and digital twin." arXiv preprint arXiv:2205.11783 (2022).

[20] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju. "The impact and limitations of artificial intelligence in cybersecurity: a literature review." International Journal of Advanced Research in Computer and Communication Engineering (2022).

[21] A. Mazzoccoli, and M. Naldi. "Optimizing cybersecurity investments over time." Algorithms 15, no. 6 (2022): 211.

[22] M. Mylrea, and S. N. G. Gourisetti. "Cybersecurity and optimization in smart “autonomous” buildings." Autonomy and Artificial Intelligence: A Threat or Savior? (2017): 263-294.

[23] E. Bellini, F. Bagnoli, M. Caporuscio, E. Damiani, F. Flammini, I. Linkov, P. Liò, and S. Marrone. "Resilience learning through self adaptation in digital twins of human-cyber-physical systems." In 2021 IEEE International Conference on Cyber Security and Resilience (CSR), pp. 168-173. IEEE, 2021.

[24] A. Salvi, P. Spagnoletti, and N. S. Noori. "Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem." Computers & Security 112 (2022): 102507.

[25] D. Allison, P. Smith, and K. Mclaughlin. "Digital Twin-Enhanced Incident Response for Cyber-Physical Systems." In Proceedings of the 18th International Conference on Availability, Reliability and Security, pp. 1-10. 2023.

[26] F. Böhm, M. Dietz, T. Preindl, and G. Pernul. "Augmented Reality and the Digital Twin: State-of-the-Art and Perspectives for Cybersecurity." Journal of Cybersecurity and Privacy 1, no. 3 (2021): 519-538.

[27] N. Kousi, C. Gkournelos, S. Aivaliotis, C. Giannoulis, G. Michalos, and S. Makris. "Digital twin for adaptation of robots' behavior in flexible robotic assembly lines." Procedia manufacturing 28 (2019): 121-126.

[28] H. Naseer, S. B. Maynard, and K. C. Desouza. "Demystifying analytical information processing capability: The case of cybersecurity incident response." Decision Support Systems 143 (2021): 113476.

[29] B. Morel. "Artificial intelligence and the future of cybersecurity." In Proceedings of the 4th ACM workshop on Security and artificial intelligence, pp. 93-98. 2011.

[30] M. Eckhart, and A. Ekelhart. "Digital twins for cyber-physical systems security: State of the art and outlook." Security and Quality in Cyber-Physical Systems Engineering: With Forewords by Robert M. Lee and Tom Gilb (2019): 383-412.

[31] C. Alcaraz, and J. Lopez. "Digital twin: A comprehensive survey of security threats." IEEE Communications Surveys & Tutorials 24, no. 3 (2022): 1475-1503.

[32] D. Kansagra, M. Kumhar, and D. Jha. "Ransomware: a threat to cyber security." CS Journals 7, no. 1 (2016).

[33] A. Malin, and G. Van Heule. "Continuous monitoring and cyber security for high performance computing." In Proceedings of the first workshop on Changing landscapes in HPC security, pp. 9-14. 2013.

[34] Q. Xu, S. Ali, and T. Yue. "Digital twin-based anomaly detection in cyber-physical systems." In 2021 14th IEEE Conference on Software Testing, Verification and Validation (ICST), pp. 205-216. IEEE, 2021.

[35] M. Dodigovic and A. Tovmasyan. "Automated writing evaluation: The accuracy of Grammarly's feedback on form." International Journal of TESOL Studies 3, no. 2 (2021): 71-87.

[36] N. Chaisamran, T. Okuda, and S. Yamaguchi. "Using a trust model to reduce false positives of sip flooding attack detection in ims." In 2013 IEEE 37th Annual Computer Software and Applications Conference Workshops, pp. 254-259. IEEE, 2013.

[37] P. K. Jena, S. Ghosh, E. Koley, and M. Manohar. "An ensemble classifier based scheme for detection of false data attacks aiming at disruption of electricity market operation." Journal of Network and Systems Management 29, no. 4 (2021): 43.

[38] G. Jakobson. "Mission-centricity in cyber security: Architecting cyber attack resilient missions." In 2013 5th International Conference on Cyber Conflict (CYCON 2013), pp. 1-18. IEEE, 2013.

[39] K. M. Villalba, S. O. Tumbo, and S. A. Donado. "An adaptable Intelligence Algorithm to a Cybersecurity Framework for IIOT." Ingeniería y Competitividad 24, no. 02 (2022): 13-13.

[40] S. Zeadally, E. Adi, Z. Baig, and I. A. Khan. "Harnessing artificial intelligence capabilities to improve cybersecurity." Ieee Access 8 (2020): 23817-23837.