International Journal of Scientific Research and Modern Technology (IJSRMT) *ijsrmt.com*
Volume 4, Issue 10, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i10.894

Harnessing Machine Learning Algorithms for Proactive Cyber Threat Detection and Real-Time Incident Response in Enterprise Networks

Marcel Okoebor

Publishing Date: 2025/10/29

Abstract

The networks supporting business enterprises are becoming increasingly vulnerable to advanced cyber threats, including ransomware, insider threats, and advanced persistent attacks, which necessitate proactive countermeasures. With proactive threat detection and real-time incident response, ML has become a revolutionary way of optimising cybersecurity. The conceptual review synthesises existing frameworks, theoretical models, and algorithmic solutions to indicate how ML may be incorporated into enterprise security architectures. The paper analyzes ML paradigms of interest, including supervised, unsupervised, deep learning, and reinforcement learning, focusing on their conceptual strengths, limitations, and applicability in identifying known and unknown threats. It also explores the architectures of ML-enabled detection systems, including data gathering, feature extraction, model training, ongoing surveillance, and the incorporation of automated responses. Analysis is presented on conceptual models of real-time incident response, including response orchestration, intelligent decision support, mechanical playbooks, and Security Orchestration, Automation, and Response (SOAR) incorporation. Among the issues the review identifies, there are critical gaps and challenges, including data privacy restrictions, interpretability issues, scalability, adversarial threats, and a lack of integration of conceptual frameworks. It emphasizes the necessity that any proposed model should be empirically validated so that the model becomes practically applicable. The synthesis of these ideas has helped to build a theoretically enlightened vision of ML-enabled cybersecurity. It has highlighted a course of action to construct resilient, adaptive, and predictive enterprise security mechanisms.

Keywords: *Machine Learning, Cybersecurity, Proactive Threat Detection, Real-Time Incident Response, Enterprise Networks, Anomaly Detection, Deep Learning, Security Orchestration, Automation, and Response (SOAR)*.

I. INTRODUCTION

Enterprise networks now have to contend with the massive scale of cybersecurity-related issues due to the rise in sophistication, frequency, and diversity of malicious attacks (Alshamrani et al., 2021). Traditional defence measures, which are reactive, are usually ineffective in responding to advanced persistent threats, ransomware, insider threats, and zero-day exploits (Cavelty, 2022). As adversaries in the cyber domain have become more adaptive and resourceful, enterprises are demanding security measures that anticipate and prevent threats, thereby minimizing the occurrence of costly data breaches and network outages (Sarker et al., 2020). It is in this regard that machine learning (ML) has become a revolutionary technology in improving cybersecurity (Apruzzese et al., 2023). In contrast to traditional rule-based systems, ML models can build classifications based on significant amounts of network traffic, user behaviour, and system logs to recognise patterns and anomalies that can foretell possible threats (Li, 2022). This ability in adaptive learning makes ML a key enabler in proactive detection and real-time incident response since it was not only able to detect threats earlier but also auto/augmented their response methods (Anthi et al., 2021).

The purpose of this review is to explore the conceptual underpinnings of harnessing ML for proactive cyber threat detection and real-time incident response within enterprise environments. Rather than focusing on empirical performance outcomes, the review synthesises existing frameworks, theoretical models, and algorithmic approaches to highlight how ML can be integrated into enterprise security architectures. Guiding questions include: How are ML paradigms conceptualised in relation to proactive detection? What models exist for real-time response in enterprise networks? And what conceptual gaps remain in current discourse? Addressing these themes

Okoebor, M. (2025). Harnessing Machine Learning Algorithms for Proactive Cyber Threat Detection and Real-Time Incident Response in Enterprise Networks. *International Journal of Scientific Research and Modern Technology*, *4*(10), 64–68. https://doi.org/10.38124/ijsrmt.v4i10.894

provides a foundation for developing more resilient and adaptive cybersecurity frameworks.

II. CONCEPTUAL FOUNDATIONS

The nature of the threat that may be posed by the range of cyber threats in society has changed significantly in two decades in terms of technology and the increasing levels of sophistication of its adversaries (Zimba & Chishimba, 2019). Simple degradations like malware or phishing have now evolved into elaborate foes including the ransomware and insider threats as well as advanced persistent threats (APTs) (Bendovschi, 2015). Going a step further, ransomware has now evolved into well-coordinated attacks whereby it targets large businesses with sophisticated extortion tactics (Al-rimy et al., 2018). Insider threats also include increasing use of privileged access to commit intentional misuse, and APTs can gain undetected access to networks over extended periods of time (Krombholz et al., 2017). The mentioned trends underscore the drawbacks of reactive defence systems, in which measures are taken once a violation is detected (Sarker et al., 2020). This entails a theoretical separation of reactive defence and proactive defence. Reactive ones, such as incident logging and post-event analysis, tend to be ineffective in mitigating the damage, where proactive detection lies in the focus on pointing out unusual patterns before the breach occurs in full (Torkura et al., 2020). Effective anticipatory solutions are those that envision threat vectors, forecast the attack trajectories and adjust to adversarial actions in real-time, in a paradigm of resilience (Goldstein & Uchida, 2016).

Real-time incident response is a supplement to proactive detection that aims to automate, scale and intelligently compact the security workflow (Verma et al., 2021). It relates to real time containment, network isolation, control it is accessed by users, and prioitisation of alerts, which is essential in large enterprise-level networks where threats spread very quickly (Sharma et al., 2021). Machine learning connects proactive detection and real time response by using analytical and adaptation capabilities (Apruzzese et al., 2023). Supervised learning learns known threats, unsupervised learning learns new anomalies, reinforcement learning to take adaptive actions, and deep learning to process high-dimensional and complex data to support pattern recognition (Li, 2022). A combination of all these paradigms contributes to a cybersecurity ecosystem that can be predictive, responsive, and anticipatory as it continues to optimize its models against new forms of attacks (Sarker, 2021).

III. THEORETICAL UNDERPINNINGS

The deployment of machine learning in cybersecurity can be further discussed by putting it into one of the established theoretical frameworks that offer depth in explanations. A typical example of such a framework is anomaly detection theory, which holds that any deviation of a given established baseline is a possible indication of malicious activity (Chandola et al., 2009). This theory supports the implementation of unsupervised learning algorithms, including clustering and density-based models, which are good at identifying new or uncommon behaviours that do not fit normal patterns of operation (Goldstein & Uchida, 2016). The principles behind anomaly detection theory, when applied in enterprise domains, offer the rationale to implement models capable of changing in dynamic environments faced by the enterprises where the threats keep changing (Ahmed et al., 2016).

Security frameworks that are risk-based are also available as a line of theory (Stoneburner et al., 2002). These frameworks envisage cybersecurity as the process of prioritising risks associated with the threat based on the expected impact and probability rather than the effort to minimise all the risks. In this context, machine-learning can be treated as a dynamic risk assessment tool that assesses new streams of data in real-time (Fenz et al., 2014). An example of this is that supervised learning classifiers could be trained to provide probabilistic risk banding of the detected anomalies which will help the security teams in prioritising the response (Virvilis & Gritzalis, 2013). By using ML as part of the risk-based models, organisations can be able to have a more dynamic sense of risk management with mitigation strategies fed using data-driven information instead of a rigid risk management thinking (Smeraldi & Malacaria, 2018).

Adaptive security frameworks are another theoretical contribution that can be derived, which suggests that an effective defence demands a system that will change with the updates of the threat landscape (Torkura et al., 2020). This is similar to the reinforcement learning approaches, which allow models to optimise defence mechanisms through trial and error against simulated or real attacks (Servin & Crandall, 2021). Another theory in which the resilience and flexibility are emphasized is the theory of adaptive security which implies that security tools should be adaptive and able to develop themselves so that they can be effective (Goldstein & Uchida, 2016). Such a theoretical position fits the reinforcement learning models particularly well, not least because those reinforcement models show continuous improvement over time as they optimize their policies based on feedback loops (Liu & Lai, 2021). The mapping of these theories with respect to cybersecurity objectives once again points out the conceptual convergence between ML and enterprise security objectives. Detection, e.g. can be related to the anomaly detection models that identify abnormal behaviour (Ahmed et al., 2016). The prediction is similar to the risk-based models of estimating the possibility of future attacks, whereas the response is associated with an adaptive framework design that recommends or acts on countermeasures in real-time (Sarker, 2021). In combination, these theories provide a conceptual framework beyond establishing the legitimacy of applying ML in cybersecurity into informing how or why it should be applied to an enterprise setting (Apruzzese et al., 2023). They allow academics and practitioners to learn to learn to perceive ML, not as a technological adjunct, but as part of a multifaceted security philosophy. By so doing, these theoretical foundations raise their hopes as well as

potential obstacles to integrating ML into proactive detection and incident response strategies, raising the issue of conceptual clarity prior to large-scale empirical implementation (Buczak & Guven, 2016).

- *Machine Learning Algorithms in Threat Detection*

The paradigms of ML algorithms provide a flexible set of tools to be used in identifying threats in enterprise networks, with each of them having its benefits and drawbacks (Apruzzese et al., 2023). Supervised learning is fairly common in classification-based intrusion detection systems, where it is based on a list of labelled data identifying known types of attack (Khraisat et al., 2019). Examples of algorithms used include decision tree, support vector machine and random forest algorithms which assign network traffic or user behaviour to either benign or malicious (Buczak & Guven, 2016). Supervised learning can be very interpretable and highly accurate in cases of known threats; however, supervised learning is not suitable in cases of previously unknown threats because the correct answer needs to be identified in a piece of known training data (Sarker et al., 2020). Unsupervised learning tries to cover this shortcoming, by identifying threats that have never been seen before using anomaly and outlier detection (Chandola et al., 2009). Methods such as clustering, principal component analysis and autoencoders can detect outliers in behaviour without the use of labelled data and are therefore appropriate in the dynamic enterprise environment (Goldstein & Uchida, 2016). They have shown to really excel at finding patterns in those hidden and frequently require more fine-tuning to achieve low false-positive rates (Ahmed et al., 2016).

Deep learning goes a step further in the ML domain, allowing the multiple extraction of features in high dimensions and complex data (Goodfellow et al., 2016). CNNs, RNNs, and transformer models can be used to examine network traffic and logs, analogizing the temporal and spatial nature of dependency information that may be disregarded by more standard approaches (Vinayakumar et al., 2019). The benefits of using deep learning in processing unstructured data on a large scale are matched by the factors of intensive computing, the black box-esque characteristics of models, and the necessity of an extreme amount of data (Arp et al., 2022). The concept of reinforcement learning (RL) brings a degree of adaptability where agents are able to deduce the optimal policies of detecting and preventing attacks in real time (Servin & Crandall, 2021). What RL supports and dynamic response to changeable threats, it needs well-designed reward functions and stable training conditions, as well as the conversion of simulations to live networks may be tricky (Liu & Lai, 2021).

The combination of these paradigms create a conceptual spectrum between predictive classification and adaptive decision-making. Recognizing their capabilities and weaknesses can help create harmonized systems that can use overlapping capabilities in a more effective, preventive detection of threats.

- *Conceptual Models of Proactive Detection*

ML allows proactive prevention of security threats because it helps turn reactive security solutions into early warning fighters to stop the threat before it has effectively occurred (Torkura et al., 2020). Machine-learning-based models are constantly monitoring network traffic, system log, and user behaviour to find hints of emerging threats (Anthi et al., 2021). Such foreknowledge enables businesses to act swiftly, reducing any interference in business operations and any possible harm (Sharma et al., 2021). The early warning systems are based on predictive measure with early detection of the known malicious actors and a behaviour variation which has correlations to new unknown attacks (Sommer & Paxson, 2010). A conventional ML-based detection framework consists of a number of important elements. The method of data collection sums network packets and logs, as well as metrics that are used to measure user activity, all of which are of quality and representative inputs (Buczak & Guven, 2016). Features extraction then summarize the data, extracting meaning about objects as either handcrafted statistics or short summaries of data, or as complex neural networks automatically (Li, 2022). They use model training: based on existing patterns of malicious and normal behaviour, algorithms can learn said patterns, and continued monitoring ensures that models remain adaptive, changing parameters on-the-fly in response to new threats (Sarker et al., 2020). Combining big data and streaming analytics has the potential to augment these frameworks, making them more contextualized and capable of processing anomalies in real time such that they can trigger an automated warning in response to anomalies or adaptive responses on the fly (Verma et al., 2021). Conceptually, ML-based proactive detection is the combination of detection and action, moving enterprises one step closer to proactive security (Apruzzese et al., 2023). Nonetheless, issues like computational cost, data privacy, and model interpretability need to be resolved so that such systems are both in theory and practice guaranteeing they will work well on enterprise environments (Arp et al., 2022).

- *Conceptual Models of Real-Time Incident Response*

Real-time incident response is a logical addition to proactive threat detection since it shifts the process of recognizing threats into active and synchronized response in enterprise networks (Sharma et al., 2021). In conceptual terms, machine learning would allow orchestrating the responses by giving systems the ability to analyse the detected anomalies and decide on optimal mitigation measures on their own (Verma et al., 2021). This kind of orchestration implies the smooth combination of outputs produced by detection level, risk evaluation, and decision logics so that each of the identified potential threats is considered and acted upon in a timely fashion (Torkura et al., 2020). By relying on predictive outputs created using ML algorithms, enterprises are able to minimize the need to use manual intervention and thus, overcome manual efforts, which are inefficient and prone to making errors, especially when used in high-volume networks (Sarker et

al., 2020). Automated playbooks are a manageable tool in this conceptual framework (Barreto et al., 2021). They code predefined responses based on noticed threats in a way that enables ML models to choose and perform suitable action, basing on the incident severity and contexts (Lopez et al, 2022). Due to the ability of combining them with intelligent decision support, these systems can be used to generate more subtle steps based on a multi-facet consideration including collateral effects, the spread of the threat, and operational priorities (Servin & Crandall, 2021). This provides a balance in faster and more accurate response to achieve a more resilient security position (Verma et al., 2021).

Integration with the SOAR (Security Orchestration, Automation, and Response) platforms further compliments the abstract concept of incident response in near real-time (Lopez et al., 2022). The benefits of SOAR include centralisation, consolidating alerts of various tools that many security organisations utilise, and automation of repetitive processes, as well as collaborative decision-making (Barreto et al., 2021). This integration has conceptualised a way that ML models can work in a coordinated environment where the processes of detection, decision-making and responding are harmonised (Torkura et al., 2020). The scheme of detection, decision, response is how the active process of enterprise security runs constantly. The steps involved in the process consist of anomaly detection, the interpretation of the meaning by decision logic, and response mechanisms that implement containment, mitigation, or remediation (Sharma et al., 2021). Collectively, these elements shape a strong theoretical framework of real-time incident response, and they also demonstrated how ML can help shift enterprise cybersecurity beyond reactive management to anticipatory, automated, and adaptive defence (Apruzzese et al., 2023).

- *Challenges and Gaps in Current Conceptualisations*

Although the application of machine learning (ML) holds promise in censuring before the incident happens and in dynamic incident response, there are still some obstacles (Buczak & Guven, 2016). Data privacy and availability were highlighted as being essential since records of companies are usually sensitive, controlled, or partial, which restricts the performance of models (Sokol & Flach, 2020). There are even more challenges related to interpretability and explainability; deep learning, in particular, are highly opaque and can reduce trust and complicate compliance with regulation (Arp et al., 2022). Scalability is also an issue since memory-intensive enterprise networks must support models that must not lose accuracy and responsiveness with constant data flow (Li, 2022). Further, the exploration of adversarial machine learning even enables an attacker to escape notice or misinform systems, thus demanding effective defence plans (Apruzzese et al., 2022). Lastly, unified conceptual models are not conducive to integrated proactive detection and real-time response because existing models are often diverse and contextual in nature (Torkura et al., 2020). It is multifaceted to bridge these gaps in order to convert both theoretical research and methods into a practical, scalable, and reliable cybersecurity solution (Sarker, 2021).

IV. CONCLUSION

Machine learning (ML) is one of the most disruptive technologies to enter cybersecurity, enabling more advanced threat identification and live incident response. ML can be used to forecast potential threats, identify anomalous activities, and produce actions based on them, as well as learn and continuously and autonomously improve its performance. This paper has reviewed relevant theories, models, and algorithms that can inform ML adoption in enterprise networks with a particular emphasis on coherent orchestration of detection, decision-making, and response. Nonetheless, issues of data privacy, interpretation, scalability, and adversarial risks, as well as disintegrated frameworks, persist. Testing in real-world environments is scarce, and it is necessary to fill these gaps to establish credibility that ML-based solutions are effective in their operation and reliable.

RECOMMENDATIONS

To increase ML integration in enterprise cybersecurity, organisations should focus on high-quality and representative datasets and follow data privacy regulations to support successful model training. Enhancing interpretability and explainability, particularly of deep learning models, is crucial for achieving trust, ensuring human oversight, and complying with regulations. To achieve this, business enterprises must implement scalable architectures capable of handling high-throughput data in real-time. This can be achieved by combining ML with SOAR frameworks and playbooks, automating incident response coordination. The field should consider combining several ML paradigms in some hybrid form to improve the accuracy, adaptability, and robustness to adversarial attack processes. Lastly, empirical testing of the conceptual models in practical enterprise networks is essential to confirm, strengthen, and help bridge the gap between theory and practice.

REFERENCES

[1]. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. Journal of Network and Computer Applications, 60, 19-31.

[2]. Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. Computers & Security, 74, 144-166.

[3]. Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2021). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2), 1851–1877.

[4]. Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., & Burnap, P. (2021). A

supervised intrusion detection system for smart home IoT devices. IEEE Internet of Things Journal, 6(5), 9042–9053.

[5]. Apruzzese, G., Andreolini, M., Ferretti, L., Marchetti, M., & Colajanni, M. (2022). Modeling realistic adversarial attacks against network intrusion detection systems. Digital Threats: Research and Practice, 3(3), 1–19.

[6]. Apruzzese, G., Laskov, P., de Oca, E. M., Mallouli, W., Rapa, L. B., & Grammatopoulos, A. V. (2023). The role of machine learning in cybersecurity. Digital Threats: Research and Practice, 4(1), 1–38.

[7]. Arp, D., Quiring, E., Pendlebury, F., Warnecke, A., Pierazzi, F., Wressnegger, C., Cavallaro, L., & Rieck, K. (2022). Dos and don'ts of machine learning in computer security. In 31st USENIX Security Symposium (USENIX Security 22) (pp. 3971-3988). USENIX Association.

[8]. Bendovschi, A. (2015). Cyber-attacks – trends, patterns and security countermeasures. Procedia Economics and Finance, 28, 24-31.

[9]. Barreto, C., Briesemeister, L., & Rocha, F. (2021). A systematic mapping study on security orchestration. ACM Computing Surveys, 54(5), 1–35.

[10]. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[11]. Cavelty, M. D. (2022). The evolution of national cybersecurity. In Routledge Handbook of International Cybersecurity (pp. 25-36). Routledge.

[12]. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. ACM Computing Surveys, 41(3), 1–58.

[13]. Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. Information Management & Computer Security, 22(5), 410-430.

[14]. Goldstein, M., & Uchida, S. (2016). A comparative evaluation of unsupervised anomaly detection algorithms for multivariate data. PLOS ONE, 11(4), e0152173.

[15]. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.

[16]. Khraisat, A., Gondal, I., Vamplew, P., & Kamruzzaman, J. (2019). Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity, 2(1), 20.

[17]. Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2017). Advanced social engineering attacks. Journal of Information Security and Applications, 22, 113-122.

[18]. Li, J.-H. (2022). Cyber security meets artificial intelligence: A survey. Frontiers in Information Technology & Electronic Engineering, 23(1), 5–26.

[19]. Liu, Y., & Lai, Y. (2021). A review of reinforcement learning based intrusion detection systems. In 2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC) (Vol. 5, pp. 2445-2450). IEEE.

[20]. Sarker, I. H. (2021). Data science and analytics: An overview from data-driven smart computing, decision-making and applications perspective. SN Computer Science, 2(5), 377.

[21]. Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., & Ng, A. (2020). Cybersecurity data science: An overview from machine learning perspective. Journal of Big Data, 7(1), 41.

[22]. Servin, A., & Crandall, J. R. (2021). A review of reinforcement learning for autonomous cybersecurity. ACM Computing Surveys, 54(5), 1–37.

[23]. Sharma, P., Navdeti, C. P., & Jain, A. (2021). A systematic literature review on automated incident response. Computers & Security, 109, 102389.

[24]. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In 2010 IEEE Symposium on Security and Privacy (pp. 305-316). IEEE.

[25]. Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems (NIST Special Publication 800-30). National Institute of Standards and Technology.

[26]. Torkura, K. A., Sukmana, M. I., & Meinel, C. (2020). Integrating continuous security assessments in microservices and cloud native applications. Procedia Computer Science, 171, 1997-2006.

[27]. Verma, A., Kaushal, S., & Chaurasia, S. (2021). A systematic review on automated cyber incident response. Archives of Computational Methods in Engineering, 28(3), 1559-1574.

[28]. Virvilis, N., & Gritzalis, D. (2013). The big four - What we did wrong in advanced persistent threat detection? In 2013 International Conference on Availability, Reliability and Security (pp. 248-254). IEEE.

[29]. Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., Al-Nemrat, A., & Venkatraman, S. (2019). Deep learning approach for intelligent intrusion detection system. IEEE Access, 7, 41525-41550.

[30]. Zimba, A., & Chishimba, M. (2019). On the economic impact of crypto-ransomware attacks: The state of the art on enterprise systems. European Journal for Security Research, 4(1), 3-31.