Analysing Multidimensional Strategies for Cyber Threat Detection in Security Monitoring

Palvi Shelke[1] and Timo Hamalainen[2]
Faculty of Information Technology, University of Jyvaskyla, Finland

vidya.palvi0211@gmail.com
timo.t.hamalainen@jyu.fi

Abstract: The escalating risk of cyber threats requires continuous advances in security monitoring techniques. This survey paper provides a comprehensive overview of recent research into novel methods for cyber threat detection, encompassing diverse approaches such as machine learning, artificial intelligence, behavioral analysis and anomaly detection. Machine learning plays a central role in cyber threat detection, highlighting the effectiveness of deep neural networks in identifying evolving threats. Their adaptability to changing attack patterns is emphasized, underlining their importance for real-time security monitoring. In parallel, ensemble learning is explored, combining multiple models to improve overall detection accuracy and create a robust defense against a spectrum of cyber threats. The literature reviewed highlights the importance of behavioral analysis, with a novel approach that integrates user behaviour profiling with anomaly detection. This has proven effective in identifying suspicious activity within a network, particularly insider threats and stealthy attacks. Another behavioral framework using User and Entity Behavior Analytics (UEBA) is presented for enhanced anomaly detection, highlighting the importance of context-aware monitoring in improving threat detection accuracy. Collaborative defense mechanisms emerge as a major focus of the research papers reviewed, exploring the potential of sharing threat information between organisations to enhance collective security monitoring. Their findings underscore the importance of a collaborative approach to staying ahead of rapidly evolving cyber threats. Some types of cyber-attacks are also analysed in the context of a security operations centre (SOC) monitoring environment using a security information and event management (SIEM) tool - Splunk. In conclusion, this survey paper synthesizes recent advances in cyber threat detection methods in security monitoring that integrate machine learning, behavioral analysis, and collaborative defense strategies. As cyber threats continue to evolve, these novel methods provide valuable insights for researchers, practitioners, and organisations seeking to strengthen their cybersecurity defenses. This concise overview emphasises the multi-dimensional approach required to secure digital ecosystems, providing a concise yet comprehensive guide to modern cyber threat detection strategies.

Keyword(s): SIEM and Splunk Monitoring, Security Monitoring, Machine Learning, Behavioral Analysis, Anomaly Detection, Threat Intelligence

1. Introduction:

In the ever-evolving landscape of digital technology, the escalating risk of cyber threats poses a formidable challenge to the security and integrity of information systems. Protecting digital assets in this dynamic environment requires constant innovation in security monitoring techniques. This survey paper serves as a comprehensive guide to recent research efforts dedicated to advancing cyber threat detection methodologies.

Exploring a wide range of approaches, from machine learning and artificial intelligence to behavioral analysis and anomaly detection, this survey consolidates key findings from studies at the forefront of security monitoring. The role of machine learning is highlighted, emphasising the adaptability of deep neural networks in real-time security monitoring. At the same time, the paper explores ensemble learning techniques, advocating the integration of multiple models to improve overall detection accuracy and strengthen defenses against a wide range of cyber threats.

Behavioral analysis emerges as a focal point, with novel approaches combining user behaviour profiling and anomaly detection. This is proving to be a key method for identifying suspicious activity within networks, particularly in the case of insider threats and stealthy attacks. The importance of context-aware monitoring is highlighted, refining the accuracy of threat detection through a behavioural framework that leverages User and Entity Behavior Analytics (UEBA).

Collaborative defense mechanisms such as threat intelligence sharing between organisations are also explored, emphasising the importance of a community-driven approach to proactively countering rapidly evolving cyber threats.

In conclusion, this survey paper synthesizes recent advances in cyber threat detection methods in security monitoring, including machine learning, behavioral analysis, and collaborative defense strategies. As organisations and practitioners seek to strengthen their cybersecurity defenses, these innovative methods offer

valuable insights into the multidimensional approach required to secure digital ecosystems. This introduction provides the framework for a detailed exploration of contemporary cyber threat detection strategies.

2. Background and Literature Review

The primary objective of the Security Operations Centre (SOC) is to safeguard the organization against cyber breaches and attacks while ensuring the protection of valuable assets like data, applications, and infrastructure. Operating around the clock (Palo Alto Networks, 2020), the SOC aims to maintain the organization's normal operations. As defined by the SANS Institute (2018), the SOC represents a harmonious integration of individuals, processes, and technology, all dedicated to preserving the integrity of an organization's information systems. This involves proactive measures such as system setup and configuration, continuous monitoring for anomalies, early identification of unintended actions or unfavourable conditions, and timely mitigation of any undesirable effects.

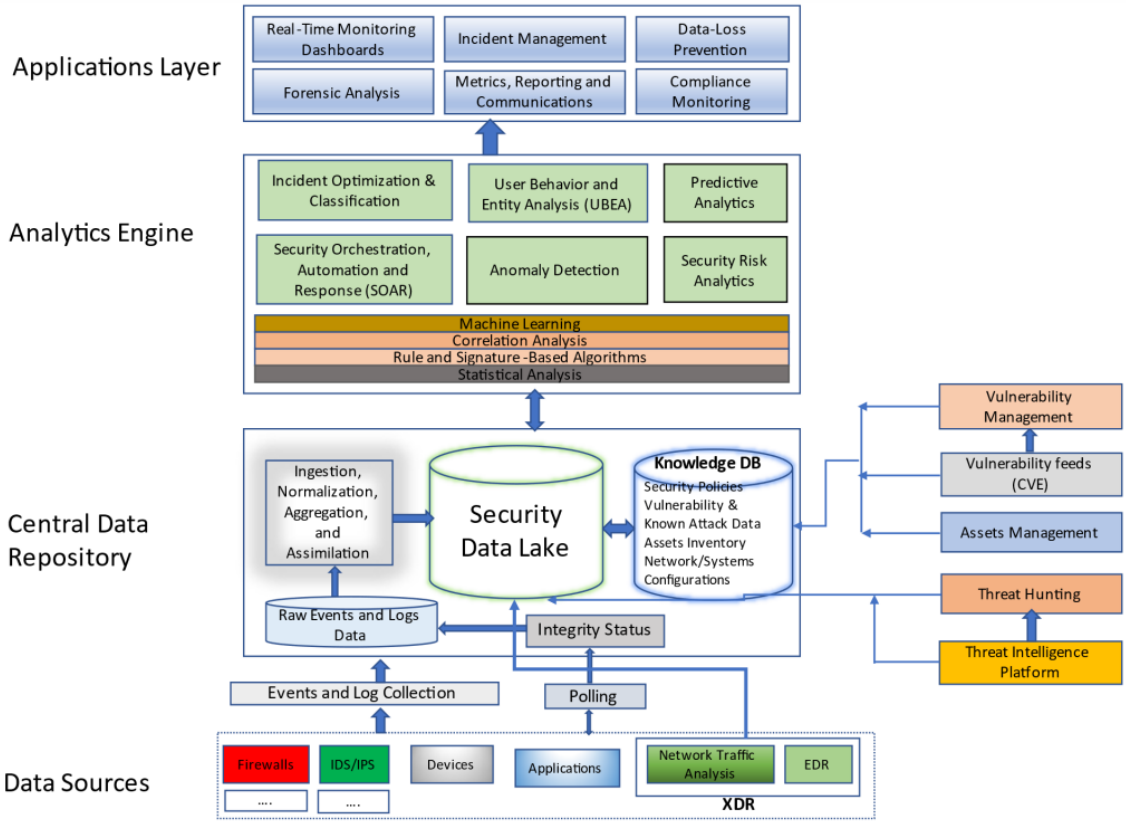

Figure 1: Security Architecture for the SOC (Mohammad A. Islam, 2023)

The Security Operations Centre (SOC) technology stack relies on the analytics engine as its core component for detecting, responding to, and recovering from cyber events and intrusions. This engine is based on machine learning, correlation analysis, rule-based algorithms and statistical analysis. It facilitates correlation analysis across the enterprise to detect intrusions or malicious activity. Anomaly detection, a machine learning algorithm within the analytics engine, identifies anomalous patterns in network traffic or user behaviour, using historical data to detect unknown threats and minimise false positives. In addition, user behaviour and entity analysis tools use advanced analytics and machine learning algorithms to detect anomalous user behaviour and potential insider threats. SOAR (Security Orchestration, Automation, and Response) automates incident response processes, including incident triage and response, threat hunting, and vulnerability scanning, streamlining workflows and eliminating false positives. In addition, predictive analytics, another machine learning model, can be trained to predict the likelihood of a security incident based on historical data (Mohammad A. Islam, 2023).

Alison Smith-Renner et al. (2019) provide an overview of anomaly detection using DAART (Detection of Anomalous Activity in Real Time) systems. Data enters the system from various sensor feeds and sensor features are extracted. These features feed the multimodal anomaly detection component along with user-defined ranges. A normalcy model is trained to represent normal behaviour against which new, potentially anomalous,

behaviour is compared. Identified anomalies are presented to the user by the active learning threat classification component, which assists the user in validating or rejecting anomalous alerts as threats, as well as specifying the threat class.

Md Faisal Ahmed et al (2023) explored the strategies, processes and mechanisms required to achieve cyber resilience in the face of emerging security risks in today's complex digital landscape. Within the domain of cyber resilience, they introduced an innovative conceptual cyber resilience model that encompasses both information security and cybersecurity considerations. The future scope of this research has been proposed to be extended to the areas of personal, network and organisational cyber security management. The foundational conceptual model of cyber resilience is of paramount importance, as it serves as a conduit for incorporating knowledge and subsequently improving the efficiency and effectiveness of cyber security and cyber defense processes. The aim is to reduce the prevalence of 'unknown unknowns' and gradually transform them into 'known unknowns' and 'known knowns'.

Junhong Kim et al. (2019) studied insider threats and applied anomaly detection algorithms and their combinations to detect malicious activities. They constructed three structured datasets to train the anomaly detection algorithms. Given the different nature of the three datasets - comprising a user's daily activity, an email's topic distribution and a user's weekly email communication - individual anomaly detection models are trained independently for each dataset. Effectively integrating the diverse results from these different anomaly detection models could potentially improve overall insider threat detection performance. Second, they built the insider threat detection model based on a specific unit of time, such as a day. In other words, this approach can detect malicious behaviour based on the batch process, but not in real time. Therefore, there may be value in developing a sequential insider threat detection model that can handle real-time streaming data. In addition, while the presented model relied solely on data-driven approaches, integrating domain expert expertise with a purely data-driven machine learning model has the potential to improve insider threat detection performance in the security domain.

Rasheed Yousef and Mahmoud Jazzar (2021) presented a real-time experiment to measure the effectiveness of user and entity behavior analytics for insider threat prevention, illustrating the impact of UEBA on false positives. The experiment demonstrated the effectiveness of UEBA in detecting insider threats and reducing false positives. However, the use of metadata, cloud and user privacy are still issues to be considered in future deployments.

Thomas D. Wagner et al. (2018) analysed 30 threat sharing platforms with respect to anonymity. Their work focused on implementing and evaluating the anonymity prototype as a proof of concept for automating the processes involved in real time. The study included the collection of Indicator of Compromise (IOC) activity data, advanced persistent threat (APT) analysis, and the development of a threat intelligence platform (TIP).

Yonghe Guo et al. (2015) mention cybersecurity as a challenging issue in smart grid implementation. They discuss the model of Distributed Denial of Service (DDoS) attack in Advanced Metering Infrastructure (AMI) system. In their study, they analysed the difference between the DDoS attack in AMI system and the Internet version. The future scope insists on focusing on developing effective defense approaches against DDoS attack in AMI system. The intrusion detection system has shown its potential in defending against various cyber-threats, but still needs to be improved to handle more advanced attacks.

3. Current and Evolving Challenges of SIEM and SOC:

The current and evolving challenges have been summarised based on literature reviews and published reports from several reputable security technology vendors, including Splunk, Microfocus, IBM, Veracode, Trend Micro, Rapid7, Exabeam, LogRhythm, CrowdStrike, Trellix, etc. SOC tools have been described as primarily defensive in nature, passively monitoring and reacting (InfosecMatter, 2020). Challenges such as manual investigation, alert prioritisation and the use of threshold-based correlation rules persist in many organisations (Kaliyaperumal, 2021).

Ongoing challenges in Security Operations Centres have been identified in four main areas: people (lack of skilled individuals, monotonous tasks, collaboration skills, integration of domain knowledge), processes (lack of standard procedures, adaptation of generic IT processes to the SOC), technologies (increased complexity, variety of tools, visualisation capabilities, insufficient level of automation), and governance and compliance (effective measurement of SOC performance, lack of best practices and standards, privacy regulations) (Microfocus, n.d.; Vielberth et al., 2020). While organisations lacked skilled individuals, determined and highly skilled attackers

were able to use the latest tools and technologies, including artificial intelligence and machine learning, to launch sophisticated attacks against organisations (Microfocus, n.d.). Even Tier 3 or Tier 4 SOC analysts found it difficult to investigate incidents when sophisticated attackers had removed their digital footprint (IIoT World, 2022).

Enormous amounts of data from network traffic and logs from devices, applications and networks need to be processed by the security operations centre. Parsing and ingesting data into the data lake and then identifying malicious activity in real time was identified as a challenge. Alert fatigue could result from numerous anomaly alerts without context or intelligence. A machine learning-based tool corroborates and correlates with contextual data across the enterprise, minimising false positives and generating a prioritised list of alerts and incidents. Zero-day attack vectors can be challenging due to lack of threat intelligence and undiscovered vulnerabilities. Behavioral analytics embedded in machine learning can detect unusual behaviour and unknown attacks (Microfocus, n.d.).

In some organisations, the CISO/CIO has chosen a best-of-breed set of security tools and software from multiple vendors. The use of too many security tools from multiple vendors without a unified framework, integration architecture, and sometimes disconnected work in silos could lead to duplicate, overlapping and conflicting alerts and recommendations (Microfocus, n.d.).

Many organisations lacked a complete inventory of their digital infrastructure, with different teams managing different components. Sometimes full configuration details, firewall rules and network diagrams were not available to the SOC. Naming conventions for infrastructure components may not be standardised across many organisations (InfosecMatter, 2020).

Some organisations may not subscribe to a threat intelligence platform and lack indicators of compromise (IOC) data. IOC data is essential to defend against advanced persistent threats (APTs) and determined malicious actors (InfosecMatter, 2020).

4. Security Attacks and Splunk Monitoring:

Live threat identification for cloud-based systems is performed using Splunk (Ananthapadmanabhan, 2022). Identification of cyber-attacks in the cloud involves the application of threat modelling and threat intelligence. Detection of malicious DNS behaviour, including spam, phishing, malware and botnet activity, is performed using the Splunk machine learning toolkit (Cersosimo, 2022). Cyber-attacks and suspicious user activity are identified using Splunk Enterprise 6.4.2 (Zhao, 2022). Network anomalies are detected in the Security Operation Centre (SOC) through a proactive threat hunting model and digital footprint analysis using Splunk (Prakash, 2022). Cyber-attacks on cyber-physical systems (CPS) will be detected using Splunk Enterprise Security software (Saraf, 2020), and predictive analysis of CPS cyber-attacks will be performed using Splunk (Saraf, 2022). Securing a contactless tachometer-based brushless DC motor involves a combination of lightweight cryptographic algorithms and Splunk (Saraf, 2021).

Monitoring for different types of cyber-attacks, including zero-day, eavesdropping, DDoS and brute force attacks, in Splunk involves configuring the platform to collect and analyse relevant log data (Saraf, 2023). Here is how to set up monitoring for each of these attack types in Splunk:

4.1 Zero-Day Attack Monitoring:

Steps:

- Behavioral Analytics: Use Splunk's Machine Learning Toolkit (MLTK) to build models that identify anomalous behaviour that could indicate a zero-day attack. Train the models on historical data to establish a baseline of normal activity.
- Threat Intelligence Integration: Integrate threat intelligence feeds into Splunk to stay on top of new vulnerabilities and threats. This can include indicators of compromise (IOCs) associated with zero-day attacks.
- Correlation searches: Implement correlation searches in Splunk to connect seemingly unrelated events that may indicate a zero-day attack. Correlation can help identify patterns that traditional signature-based detection may miss.
- Real-time alerting: Configure real-time alerts to notify security teams when suspicious activity or patterns indicative of a zero-day attack are detected.

- Threat hunting queries: Engage in threat hunting by creating specific queries and searches to proactively look for signs of zero-day attacks in Splunk.

4.2 Monitor for Eavesdropping Attacks:

Steps:

- Network traffic analysis: Monitor network traffic logs in Splunk to detect unusual patterns or unauthorised access that could indicate an eavesdropping attack.
- Encryption monitoring: Track the effectiveness of encryption protocols with Splunk. Ensure that communication channels are adequately encrypted to protect against eavesdropping.
- Alerts for unusual activity: Configure alerts in Splunk to notify administrators of any suspicious or unauthorised access to sensitive communication channels.

4.3 Monitoring DDoS Attacks:

Steps:

- Traffic Analysis: Analyse network traffic logs in Splunk to identify sudden spikes in traffic that could indicate a DDoS attack.
- Threshold Based Alerts: Configure alerts based on predefined network traffic thresholds. Any abnormal increase in traffic can trigger alerts.
- Anomaly detection: Leverage Splunk's machine learning capabilities to detect anomalies in traffic patterns that may indicate a DDoS attack.

4.4 Monitor for Brute Force Attacks:

Steps:

- Monitor login activity: Monitor authentication and login activity logs in Splunk to detect multiple failed login attempts that may indicate a brute force attack.
- Threshold Based Alerts: Set up alerts based on thresholds for failed login attempts. Unusual patterns or high numbers of failed attempts can trigger alerts.
- User behavior analytics: Implement user behavior analytics in Splunk to detect anomalous login patterns or suspicious user activity associated with brute force attacks.
- IP reputation analytics: Integrate threat intelligence feeds to assess the reputation of IP addresses attempting to log in. Identify and block IP addresses associated with malicious activity.

By implementing these monitoring strategies, organisations can improve their ability to detect and respond to different cyber threats and tailor their approach to the specific characteristics of each type of attack. Regularly review and update monitoring configurations to adapt to the evolving threat landscape.

5. Research Methodology and Implementation Guidelines:

The following is an in-depth analysis of the implementation of the SIEM solution, focusing on Splunk and its integral role in Security Operations Centre (SOC) monitoring:

1. The skills and training of SOC analysts play a critical role in influencing the effectiveness of threat detection and response supported by security information and event management (SIEM) systems. How does the expertise of SOC analysts impact the effectiveness of SIEM tools in identifying and responding to potential cybersecurity threats?
2. In time-critical scenarios, the design of user interfaces and visualisations in SIEM tools becomes critical in facilitating optimal decision making by Security Operations Centre (SOC) analysts. How can the layout and presentation of information in SIEM tools be customised to improve the decision-making process for SOC analysts, especially when rapid response is essential?

5.1 The Impact of SOC Analyst Training on SIEM-based Threat Detection:

The impact of SOC analyst training on the effectiveness of SIEM-based threat detection is significant and multi-faceted. Well-trained SOC analysts play a critical role in maximising the benefits of SIEM systems. Here are some key aspects of this impact:

- Detection accuracy: Trained analysts are better able to understand the nuances of security events and alerts generated by SIEM. Their expertise enables them to distinguish between false positives and real threats, reducing the likelihood of missing critical security incidents.
- Incident response efficiency: Trained SOC analysts have the skills to interpret SIEM output quickly and accurately, enabling them to respond quickly to security incidents. Their skills ensure a more efficient incident response process, minimising the time between threat detection and mitigation.
- Optimised rule tuning: Skilled analysts can fine-tune SIEM rules and correlation logic based on their deep understanding of organisational nuances. This optimisation improves the SIEM system's ability to adapt to the organisation's specific threat landscape.
- Contextual analysis: Training enables analysts to add context to SIEM alerts by integrating knowledge of organisational workflows, systems and user behaviour. This contextual analysis enables more informed decision making and reduces the risk of misinterpreting the severity of alerts.
- Continuous improvement: Ongoing training ensures that SOC analysts stay abreast of evolving cyber threats, attack techniques, and updates to SIEM technologies. This continuous learning is critical to maintaining the relevance and effectiveness of SIEM-based threat detection strategies.

5.2 Designing SIEM User Interfaces for Optimal Decision-Making:

The design of user interfaces (UIs) in SIEM tools is critical to supporting optimal decision making by SOC analysts, especially under time-sensitive conditions. Here are UI design considerations:

- Intuitive visualisation: Create visualisations that are intuitive and easy to interpret. Graphs, charts, and dashboards should present complex information in a clear and understandable manner, allowing analysts to quickly grasp security status.
- Prioritisation and alert clustering: Design the UI to prioritise alerts based on severity and relevance. Clustering related alerts and providing a hierarchy of threats can help analysts focus on the most critical issues first, facilitating efficient decision-making in high-pressure situations.
- Interactive and responsive features: Incorporate interactive features that allow analysts to drill down into details, pivot between data views, and dynamically adjust parameters. Responsive interfaces enable rapid exploration of data, enhancing the analyst's ability to make timely decisions.
- Display contextual information: Provide contextual information alongside alerts, such as historical data, threat intelligence, and user behaviour patterns. This additional context helps analysts make more informed decisions by understanding the broader security landscape.
- Customise to analyst preferences: Allows the user interface to be customised to suit different analyst preferences. Features such as customisable dashboards and alert views allow analysts to tailor the interface to their specific needs, improving the overall user experience.
- Real-time monitoring and notification: Implement real-time monitoring capabilities with instant notification of critical events. A responsive user interface that provides real-time updates ensures that analysts are promptly informed of unfolding security incidents, enabling rapid decision-making.

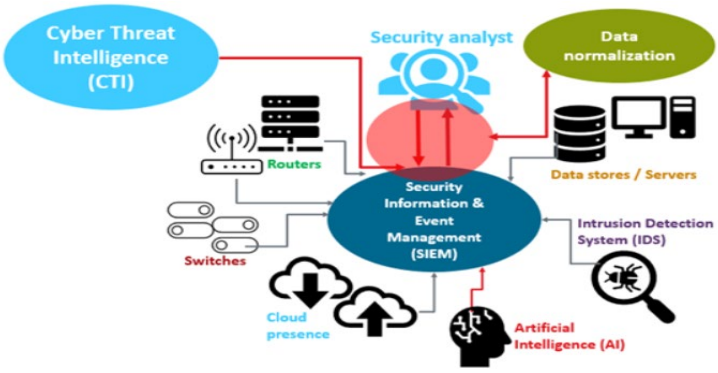

Figure 2: A high-level CompTIA suggested sample SIEM-SOC architecture.

CompTIA (n.d.) has delineated common responsibilities for the Security Operations Centre that include proactive monitoring, incident response and recovery, remediation, compliance monitoring, coordination and contextual understanding. Figure 2 illustrates the high-level overarching structure of a typical SOC (Mohammad A. Islam, 2023). By combining effective SOC analyst training with a well-designed SIEM user interface, organisations can

optimise their ability to efficiently detect, respond to and mitigate cybersecurity threats, even in time-sensitive situations.

6. Conclusions and Future Research:

This research has delved into the critical area of cybersecurity, focusing specifically on the monitoring and detection of various cyber threats, including zero-day attacks, eavesdropping attacks, DDoS attacks and brute force attacks. Leveraging the capabilities of Splunk, a robust security information and event management (SIEM) platform, the research highlighted the importance of proactive monitoring and advanced analytics in protecting digital assets.

The study of zero-day attacks highlighted the importance of behavioral analytics, threat intelligence integration and real-time alerting to effectively detect and respond to emerging threats. Eavesdropping attacks were addressed by examining network traffic and the effectiveness of encryption to ensure secure communication channels.

DDoS monitoring involved analysing network traffic patterns, setting up threshold-based alerts and using machine learning to detect anomalies. Monitoring for brute force attacks emphasised user behaviour analysis, IP reputation analysis and real-time alerts based on login activity.

In short, the cybersecurity landscape is dynamic, and ongoing research is critical to staying ahead of sophisticated cyber threats. The future of the field lies in the continuous evolution of strategies, technologies, and collaborative efforts to ensure the resilience and security of digital ecosystems. We have therefore analysed multi-dimensional strategies for cyber threat detection in security monitoring.

Looking ahead to future developments, a key focus is on a more comprehensive understanding of user behaviour. This includes extending analytics to provide nuanced insights for accurate identification of anomalous behaviour and potential insider threats, which will contribute significantly to cybersecurity measures. In addition, it is imperative to adapt security measures to the scale and complexity of extended environments, particularly those rooted in cloud infrastructure. The challenges associated with monitoring in such environments require the development and implementation of security strategies specifically tailored to the unique characteristics of cloud-based systems. In response to emerging threats, there is a need for dedicated platforms that systematically collect, analyse and share information. These platforms aim to remain proactive against evolving vulnerabilities and associated attack methods, improving overall cybersecurity resilience in the face of dynamic challenges.

References:

Alison Smith-Renner, Rob Rua, Mike Colony, (2019) “Towards an Explainable Treat Detection Tool”, In Joint Proceedings of ACM IUI 2019 Workshops. ACM, Los Angeles, USA, 20 March 2019

Ananthapadmanabhan A., and Krishnashree Achuthan (2022) “Threat Modelling and Threat Intelligence System for Cloud using Splunk”, In 2022 10th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-6. IEEE

Cobb, M. (n.d.), (2023) “SIEM vs. SOAR vs. XDR: Evaluate the differences”, TechTarget, Retrieved February 4, 2023, from https://www.techtarget.com/searchsecurity/tip/SIEM-vs-SOAR-vs-XDR-Evaluatethe-differences

Cersosimo, Michelle, and Adrian Lara (2022) “Detecting Malicious Domains using the Splunk Machine Learning Toolkit”, In NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium, pp. 1-6. IEEE

Crowley, C. and Pescatore, J. (2018) "The definition of SOC-cess? SANS 2018 Security Operations Center Survey", SANS Institute Reading Room, SANS Institute. Retrieved January 28, 2023, from https://assets.extrahop.com/whitepapers/Survey_SOC-2018_ExtraHop.pdf

Exabeam documentation "The SOC, SIEM and other essential SOC tools", Retrieved January 28, 2023, from https://www.exabeam.com/explainers/siem/the-soc-secops-and-siem/

Gustavo González-Granadillo, Susana González-Zarzosa, Rodrigo Diaz (2021) "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures", Sensors 2021, 21, 4759, https://doi.org/10.3390/s21144759

InfosecMatter (2020, 20 September) “Security Operations Centre: Challenges for SOC teams” Retrieved 3 February 2023, from https://www.infosecmatter.com/security-operations-center-challenges-ofsoc-teams/

IIoT World (2022, 28 January) “What is a SOC? Top security operations centre challenges” Retrieved 12 February 2023, from https://www.iiot-world.com/ics-security/cybersecurity/top-challengessoc-are-facing/

Kaliyaperumal, L.N. (2021, 21 October) “The evolution of security operations and strategies for building an effective SOC”. ISACA Journal, 5. Retrieved 3 February 2023, from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-securityoperations-and-strategies-for-building-an-effective-soc

Kundankumar Rameshwar Saraf, P. Malathi (2023) "Splunk-Based Threat Intelligence of Cyber-Physical System: A Case Study with Smart Healthcare", International Journal of Intelligent Systems and Applications in Engineering, IJISAE, 2023, 11(2), 537–549

Kim J, Park M, Kim H, Cho S, Kang P, (2019) "Insider Threat Detection Based on User Behavior Modeling and Anomaly Detection Algorithms", Applied Sciences, 2019; 9(19):4018, https://doi.org/10.3390/app9194018

Md Faisal Ahmed et al (2023) "Advancing Cyber Resilience: Bridging the Divide Between Cyber Security and Cyber Defense", International Journal for Multidisciplinary Research (IJFMR), Volume 5, Issue 6, November-December 2023

Mohammad Anwarul Islam (2023) "Application of artificial intelligence and machine learning in security operations center", Research paper from https://comp.mga.edu/static/media/doctoralpapers/2023_Islam_0516152253.pdf

Microfocus (n.d.) (2023) "What is a Security Operations Center (SOC)?" Retrieved February 3, 2023, from https://www.microfocus.com/en-us/what-is/security-operations-center

Prakash, G., M. Ganeshan, A. Shenbagavalli, M. Satheesh Kumar, K. Srujan Raju, and K. Suthendran (2022) "A Proactive Threat Hunting Model to Detect Concealed Anomaly in the Network" In Smart Intelligent Computing and Applications, Volume 2, pp. 553-565. Springer, Singapore

Rasheed Yousef, Mahmoud Jazzar (2021) "Measuring the Effectiveness of User and Entity Behavior Analytics for the Prevention of Insider Threats", Journal of Xi'an University of Architecture & Technology, Volume XIII, Issue 10, 2021

Saraf, K.R. and Malathi, P. (2020) "Cyber Physical System Security by Splunk" i-Manager's Journal on Communication Engineering and Systems, 9(2), p.41

Saraf Kundan Kumar Rameshwar, and P. Malathi. (2022) "Intelligent Learning Analytics in the Healthcare Sector Using Machine Learning and IoT", In Machine Learning, Deep Learning, Big Data, and Internet of Things for Healthcare, pp. 37-53. Chapman and Hall/CRC

Saraf Kundan Kumar Rameshwar, P. Malathi, and Kailash Shaw (2021) "Security Enhancement of Contactless Tachometer-Based Cyber-Physical System", In Machine Learning Approaches for Urban Computing, pp. 165-187. Springer, Singapore

Splunk documentation "Securing Splunk Enterprise", version 9.0.2, (2022) available: https://docs.splunk.com/Documentation/Splunk/9.0.2/Security/ConfigureS2Sonnewcipher

Splunk documentation "Securing Splunk Enterprise", version 9.0.2, (2022) available: https://docs.splunk.com/Documentation/Splunk/9.0.2/Security/Updates

Thomas D. Wagner et al (2018) "Towards an Anonymity Supported Platform for Shared Cyber Threat Intelligence", Springer International Publishing AG, part of Springer Nature 2018, https://doi.org/10.1007/978-3-319-76687-4_12

Vielberth, M., Böhm, F., Fichtinger, I., & Pernul, G. (2020) "Security Operations Center: A systematic study and open challenges" IEEE Access, 8, 227756-227779

Yonghe Guo, Chee-Wooi Ten, Shiyan Hu, and Wayne W. Weaver (2015) "Modeling Distributed Denial of Service Attack in Advanced Metering Infrastructure", DOI: 10.1109/ISGT.2015.7131828

Zhao, Liguo, Derong Zhu, Wasswa Shafik, S. Mojtaba Matinkhah, Zubair Ahmad, Lule Sharif, and Alisa Craig (2022) "Artificial intelligence analysis in cyber domain: A review", International Journal of Distributed Sensor Networks 18, no. 4: 15501329221084882