
| **RESEARCH ARTICLE**

Cyberattack Detection and Automated Response Using Microsoft Azure Sentinel

Shekar Rao Lakavath

Independent Researcher, Bonneylake, Washington, USA

Corresponding Author: Shekar Rao Lakavath, **E-mail:** Shekar.lakavath@gmail.com

| **ABSTRACT**

The growing sophistication and volume of cyberattacks have outpaced the capacity of manual security operations to detect and contain threats within an acceptable time window. Cloud-native Security Information and Event Management (SIEM) platforms combined with Security Orchestration, Automation, and Response (SOAR) capabilities have emerged as a response to this gap, enabling organizations to correlate telemetry across large, distributed environments and to trigger automated containment actions without waiting for manual analyst intervention. Microsoft Azure Sentinel (now marketed as Microsoft Sentinel) is one such platform, combining a cloud-scale data lake, machine-learning-based analytics, and low-code automation playbooks within a single service. This article examines how Azure Sentinel can be configured to detect a range of common cyberattack scenarios and to trigger automated response actions that contain threats before they escalate, spanning intrusion detection research, SIEM and SOAR architecture studies, threat intelligence frameworks including MITRE ATT&CK, and automated incident response systems, the article proposes an end-to-end detection-and-response pipeline architecture for Sentinel, compares its core components against their underlying detection and response functions, and maps common attack scenarios to specific Sentinel-based detection logic and automated mitigations. The findings indicate that Sentinel's integration of data aggregation, behavioral analytics, and orchestrated response substantially reduces mean time to detection and containment relative to manually operated security operations, provided that organizations invest in tuning analytics rules, mapping detection logic to a recognized threat taxonomy, and maintaining human oversight of automated response actions. The article concludes with practical recommendations for security operations teams adopting Azure Sentinel.

| **KEYWORDS**

Cyberattack detection, Microsoft Azure Sentinel, SIEM, SOAR, automated incident response, threat intelligence, MITRE ATT&CK, cloud security.

| **ARTICLE INFORMATION**

ACCEPTED: September 30, 2026 **PUBLISHED:** December 22, 2024 **DOI:** <https://doi.org/10.61424/ijans.v2i2.1074>

1. Introduction

Security operations centers (SOCs) have traditionally relied on Security Information and Event Management (SIEM) systems to aggregate log data from across an organization's infrastructure and to surface potentially malicious activity for analyst review. As attack surfaces have expanded to include cloud infrastructure, software-as-a-service applications, and remote endpoints, the volume of telemetry that SOCs must process has grown well beyond what manual triage can handle, a challenge documented extensively in the network anomaly detection literature (Bhuyan, Bhattacharyya, & Kalita, 2014).

Two developments have addressed this scaling problem. First, machine-learning-based detection techniques have been applied to distinguish genuinely anomalous activity from the enormous volume of benign log data that traditional signature-based systems struggle to filter efficiently (Ferrag, Maglaras, Moschogiannis, & Janicke, 2020). Second, Security Orchestration, Automation, and Response (SOAR) platforms have emerged to automate the containment actions that follow detection, reducing the time between an alert being raised and a threat being contained (Islam, Babar, & Nepal, 2020). Microsoft Azure Sentinel combines both developments within a single, cloud-native platform: a Log Analytics workspace ingests telemetry at cloud scale, analytics rules apply both rule-based and machine-learning detection logic, and Logic Apps-based playbooks automate response actions once an incident is confirmed.

This article addresses three questions. First, what categories of cyberattack does the intrusion detection and SIEM literature identify as most consequential, and how has detection methodology evolved to address them? Second, how do Azure Sentinel's core architectural components map onto these detection and response requirements? Third, what specific detection logic and automated response actions are appropriate for common attack scenarios, and what governance safeguards should accompany automated response? The remainder of the article reviews the relevant literature, proposes a detection-and-response pipeline architecture for Sentinel, compares its components against their underlying functions, maps attack scenarios to detection and response logic, and discusses practical implications for security operations teams.

2. Literature Review

2.1 The Evolution of Intrusion and Anomaly Detection

Network anomaly detection research has long distinguished between signature-based detection, which matches observed traffic against known attack patterns, and anomaly-based detection, which flags deviations from an established baseline of normal behavior. Bhuyan, Bhattacharyya, and Kalita (2014) provided a comprehensive survey of anomaly detection methods, systems, and tools, concluding that hybrid approaches combining both detection paradigms generally outperform either approach used in isolation. Tidjon, Frappier, and Mammar (2019) extended this analysis with a cross-domain overview of intrusion detection systems, noting that event stream processing methods have become increasingly important as organizations must process telemetry in near-real time rather than through periodic batch analysis, a requirement that directly shaped the design of cloud-native SIEM platforms such as Sentinel.

The application of machine learning and deep learning to intrusion detection has been a particularly active research area. Ferrag, Maglaras, Moschogiannis, and Janicke (2020) conducted a comparative study of deep learning approaches to intrusion detection across multiple benchmark datasets, finding that model performance varied substantially depending on the balance between detection accuracy and false-positive rate, a tradeoff with direct operational implications for any SOC relying on automated alerting. Salo, Nassif, and Essex (2019) proposed a dimensionality-reduction approach combining information-gain-based feature selection with principal component analysis, demonstrating that reducing feature space complexity before classification improved both detection accuracy and computational efficiency, a consideration relevant to tuning analytics rules that must operate across very large log volumes.

Othman, Ba-Alwi, Alsohybe, and Al-Hashida (2018) evaluated intrusion detection models in big-data environments, concluding that distributed processing frameworks were necessary to apply machine learning classifiers at the data volumes generated by modern enterprise networks, a finding directly applicable to Sentinel's Log Analytics workspace architecture. Yulianto, Sukarno, and Suwastika (2019) improved the performance of an AdaBoost-based intrusion detection system on a modern benchmark dataset, illustrating the ongoing refinement of ensemble-learning techniques for network intrusion classification. Hasan, Islam, Zarif, and Hashem (2019) applied similar machine-learning approaches to attack and anomaly detection in Internet of Things sensor networks, extending anomaly-detection methodology to the increasingly diverse set of connected devices that generate telemetry ingested by modern SIEM platforms.

2.2 SIEM Architecture and Critical Infrastructure Applications

As SIEM platforms matured from log aggregation tools into analytics-driven detection systems, researchers began systematically documenting their architecture and limitations. González-Granadillo, González-Zarzosa, and Díaz (2021) conducted what they describe as the first systematic academic analysis of the SIEM landscape, examining commercial and open-source solutions and identifying scalability, alert correlation accuracy, and integration with automated response as the primary axes along which SIEM platforms continue to evolve. Radoglou-Grammatikis et al. (2021) proposed SPEAR SIEM, a system information and event management platform purpose-built for smart grid environments, demonstrating how domain-specific detection logic can be layered onto a general SIEM architecture, an approach conceptually similar to how Sentinel's analytics rule templates are adapted to specific Azure workloads.

Majeed, ur Rasool, Ahmad, Alam, and Javaid (2019) addressed a persistent challenge in SIEM operations: the difficulty of visually distinguishing genuinely novel threats from near-miss variations of previously seen alerts, proposing a visual analysis technique to help analysts prioritize investigation effort, a concern directly relevant to alert fatigue in any Sentinel deployment generating a high incident volume. Moukafih, Orhanou, and Elhajji (2020) proposed a mobile agent-based architecture for SIEM event collection and normalization, addressing the practical challenge of ingesting heterogeneous log formats from diverse infrastructure components into a single normalized schema, a function performed within Sentinel by its data connector framework.

2.3 Threat Intelligence and the MITRE ATT&CK Framework

Effective threat detection increasingly depends on structured threat intelligence frameworks that describe adversary behavior in a standardized taxonomy. Al-Sada, Sadighian, and Oligeri (2023) reviewed the academic and industry literature applying the MITRE ATT&CK framework, finding that mapping detection rules to specific ATT&CK tactics and techniques improves both detection coverage assessment and cross-organizational threat-intelligence sharing, a practice directly reflected in Sentinel's built-in analytics rule templates, which are explicitly labeled with corresponding ATT&CK techniques. Kwon, Ashley, Castleberry, McKenzie, and Gupta Gouriseti (2020) proposed a cyber threat dictionary that maps MITRE ATT&CK techniques to the NIST Cybersecurity Framework, providing organizations with a bridge between technical detection logic and higher-level risk management and compliance reporting.

Mashima (2022) evaluated the use of the MITRE ATT&CK framework to assess in-network deception technology for electrical substation systems, illustrating how the framework extends beyond conventional information-technology environments into operational-technology and critical-infrastructure contexts increasingly monitored through cloud-based SIEM platforms. Homer et al. (2013) proposed a method for aggregating vulnerability metrics across an enterprise network using attack graphs, providing an earlier foundation for the kind of environment-wide risk correlation that modern threat-intelligence-informed analytics rules perform at cloud scale.

2.4 Security Orchestration, Automation, and Response

The automation of incident response has developed as a distinct research area addressing the operational bottleneck that occurs once a threat is detected but before it is contained. Islam, Babar, and Nepal (2020) proposed an architecture-centric approach for integrating heterogeneous security tools within a security orchestration platform, arguing that inconsistent application programming interfaces across security vendors represent a significant barrier to effective automation, a problem that cloud-native platforms such as Sentinel address by providing a large library of pre-built connectors and playbook templates. Schlette, Caselli, and Pernul (2021) conducted a comparative study of cyber threat intelligence from the specific perspective of security incident response, concluding that the value of threat intelligence depends heavily on how directly it can be operationalized into automated detection and response logic rather than remaining a passive reference resource.

Husák and Cegan (2014) proposed PhiGARo, an automated phishing detection and incident response framework that used honeypots to reduce reliance on user-reported phishing incidents, illustrating an early example of the automated detection-to-response pipeline that SOAR platforms have since generalized across a much broader

range of attack types. Ohmori (2019) examined the automation and orchestration of initial computer security incident response through a centralized incident tracking system, finding that standardizing the initial triage and escalation workflow substantially reduced the time to formal incident declaration. Kaiser et al. (2022) proposed a cyber threat intelligence-enabled automated attack incident response system, demonstrating that incorporating external threat intelligence feeds into automated response logic improved the precision of containment actions relative to response logic driven purely by internal telemetry.

Kraeva and Yakhyayeva (2021) applied metric learning techniques to the problem of security incident playbook recommendation, proposing a method for automatically suggesting the most appropriate response playbook based on the characteristics of a given incident, a capability with direct relevance to organizations managing large libraries of Sentinel playbooks across diverse attack scenarios.

2.5 Cloud-Specific Intrusion Detection and Behavioral Analytics

Intrusion detection research specific to cloud computing environments has addressed the unique visibility and multi-tenancy challenges that cloud platforms introduce. Modi, Patel, Borisaniya, Patel, Patel, and Rajarajan (2013) conducted an early comprehensive survey of intrusion detection techniques for cloud computing, examining how intrusion detection and prevention systems should be positioned within cloud architecture to achieve adequate visibility without introducing excessive performance overhead, considerations that remain directly relevant to configuring Sentinel data connectors across Azure subscriptions. Garcia, Bessani, Gashi, Neves, and Obelheiro (2014) examined operating system diversity as a mechanism for intrusion tolerance, proposing that architectural diversity within a computing environment can limit the blast radius of a successful compromise, a principle reflected in network segmentation recommendations that often accompany automated containment playbooks.

User and entity behavior analytics have emerged as a particularly important detection technique for identifying compromised credentials and insider threats that evade signature-based detection. Cui, Zhang, Chen, and Yu (2022) proposed a fuzzy particle swarm clustering algorithm for detecting abnormal behavior across multiple network domains within a user and entity behavior analytics framework, demonstrating improved detection accuracy relative to conventional clustering approaches, a technique conceptually aligned with the behavioral baselining that underlies Sentinel's built-in user and entity behavior analytics capability.

Taken together, this literature establishes a clear technical progression: from foundational signature- and anomaly-based intrusion detection, through machine-learning-enhanced detection methods, to structured threat-intelligence frameworks such as MITRE ATT&CK, and finally to the orchestration and automation systems that translate detection into contained, auditable response. The following sections apply these findings to the specific context of Microsoft Azure Sentinel.

3. A Detection and Automated Response Pipeline Architecture for Azure Sentinel

Building on the SIEM and SOAR research reviewed above (González-Granadillo, González-Zarzosa, & Diaz, 2021; Islam, Babar, & Nepal, 2020), this article proposes an end-to-end detection and response pipeline for Azure Sentinel. Figure 1 illustrates the pipeline, spanning data ingestion, analytics-driven detection, incident correlation, automated response, and analyst review.

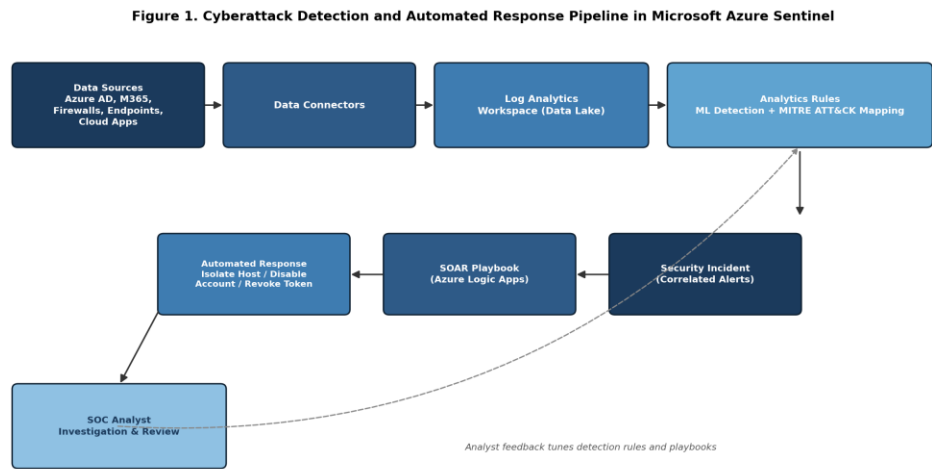


Figure 1. Cyberattack detection and automated response pipeline in Microsoft Azure Sentinel, showing the flow from data ingestion through analytics-driven detection, incident correlation, automated playbook response, and analyst review, with a feedback loop tuning future detection logic.

3.1 Data Ingestion and Normalization

Data connectors ingest telemetry from Azure Active Directory, Microsoft 365, network firewalls, endpoint detection tools, and third-party security products into a centralized Log Analytics workspace, addressing the log-format heterogeneity challenge documented by Moukafih, Orhanou, and Elhajji (2020). This centralized data lake enables the cross-source correlation that Homer et al. (2013) identify as essential for enterprise-wide risk assessment.

3.2 Analytics-Driven Detection

Analytics rules apply a combination of scheduled Kusto Query Language queries and built-in machine-learning models to detect anomalous patterns, following the hybrid signature-and-anomaly detection approach recommended by Bhuyan, Bhattacharyya, and Kalita (2014). Rules are explicitly mapped to MITRE ATT&CK tactics and techniques, operationalizing the threat-intelligence integration that Al-Sada, Sadighian, and Oligeri (2023) identify as improving detection coverage assessment.

3.3 Incident Correlation and Automated Response

Related alerts are aggregated into a single incident to reduce the alert-fatigue problem documented by Majeed, ur Rasool, Ahmad, Alam, and Javaid (2019). Once an incident is confirmed, a Logic Apps-based playbook executes automated containment actions, such as disabling a compromised account, isolating an affected host, or blocking a malicious IP address, applying the orchestration-centric architecture proposed by Islam, Babar, and Nepal (2020) within a cloud-native platform.

3.4 Analyst Review and Feedback

SOC analysts review automated actions and incident evidence, and their findings feed back into the tuning of analytics rules and playbook logic, consistent with the standardized triage and escalation workflow shown by Ohmori (2019) to reduce time to formal incident declaration. This feedback loop also supports the playbook-recommendation approach proposed by Kraeva and Yakhyeva (2021), allowing response logic to improve iteratively as new attack patterns are observed.

4. Mapping Sentinel Components to Detection and Response Functions

Table 1 details how each core Sentinel component maps onto the underlying detection or response function it performs, situating the platform's architecture within the broader SIEM and SOAR research reviewed above.

Table 1. Azure Sentinel Components Mapped to Detection and Response Functions

Sentinel Component	Underlying Function	Detection/Response Role
Data Connectors	Ingest logs from Azure AD, Microsoft 365, firewalls, endpoints, and third-party security tools	Provides the raw telemetry needed for correlation and anomaly detection across the environment
Log Analytics Workspace	Centralized, queryable data lake built on Kusto Query Language (KQL)	Stores and indexes security events for real-time and historical threat hunting
Analytics Rules	Scheduled and near-real-time queries, including machine-learning-based anomaly detection	Correlates raw events into meaningful alerts mapped to MITRE ATT&CK tactics and techniques
Incidents	Aggregation of related alerts into a single investigable case	Reduces alert fatigue by grouping evidence of a single attack campaign
Playbooks (Logic Apps)	Automated, no-code/low-code workflow engine triggered by incidents	Executes automated containment actions such as disabling accounts or isolating hosts
Workbooks and Hunting Queries	Customizable dashboards and proactive KQL-based hunting	Supports analyst-driven investigation and continuous refinement of detection logic

As Table 1 indicates, Sentinel's architecture directly operationalizes the SIEM maturity model described by González-Granadillo, González-Zarzosa, and Diaz (2021): raw log aggregation, analytics-driven correlation, and automated response are integrated within a single platform rather than requiring separate, loosely coupled tools, reducing the integration burden that Islam, Babar, and Nepal (2020) identify as a common barrier to effective security orchestration.

5. Mapping Attack Scenarios to Detection and Automated Response

Table 2 synthesizes common cyberattack scenarios documented in the literature reviewed above and maps each to specific Sentinel-based detection logic and automated response actions, along with representative supporting sources.

Table 2. Cyberattack Scenarios Mapped to Sentinel Detection and Automated Response

Attack Scenario	Sentinel Detection and Automated Response	Supporting Literature
Brute-force or credential-stuffing sign-in attempts	Analytics rules flag anomalous sign-in velocity and geolocation; playbook automatically disables the affected account and forces password reset	Bhuyan, Bhattacharyya, & Kalita (2014); Cui, Zhang, Chen, & Yu (2022)
Phishing-based initial access	Correlation of email security logs with sign-in and mailbox-rule anomalies triggers an incident; playbook quarantines the message and blocks the sender domain	Husák & Cegan (2014)
Malware or ransomware execution on an endpoint	Endpoint detection alerts correlated with process and network telemetry generate a high-severity incident; playbook isolates the host from the network	Ferrag, Maglaras, Moschoyiannis, & Janicke (2020); Garcia, Bessani, Gashi, Neves, & Obelheiro (2014)
Lateral movement across cloud resources	User and entity behavior analytics detect atypical resource access patterns relative to a baseline	Cui, Zhang, Chen, & Yu (2022); Kraeva & Yakhyayeva (2021)
Privilege escalation and persistence	Analytics rules mapped to MITRE ATT&CK tactics flag unusual role assignment or persistence-technique indicators; playbook revokes elevated tokens	Al-Sada, Sadighian, & Oligeri (2023); Kwon, Ashley, Castleberry, McKenzie, & Gupta Gourisetti (2020)
Distributed denial-of-service and network-layer anomalies	Network traffic analytics detect volumetric deviations from baseline; playbook engages upstream mitigation and alerts the network operations team	Homer et al. (2013); Modi, Patel, Borisaniya, Patel, Patel, & Rajarajan (2013)
Data exfiltration via unusual outbound transfer	Correlation of data-loss-prevention signals with outbound traffic volume triggers an incident; playbook blocks the destination and revokes active sessions	Salo, Nassif, & Essex (2019); Hasan, Islam, Zarif, & Hashem (2019)

The mapping in Table 2 illustrates that effective automated response depends on accurately distinguishing attack categories at the detection stage; a playbook that isolates a host in response to a brute-force sign-in attempt, for example, addresses the wrong stage of the attack relative to disabling the targeted account, underscoring the importance of aligning analytics rule logic precisely with the MITRE ATT&CK tactic each scenario represents (Kwon, Ashley, Castleberry, McKenzie, & Gupta Gourisetti, 2020).

6. Discussion

The analysis presented above supports several practical conclusions for security operations teams adopting Azure Sentinel. First, detection accuracy depends heavily on the quality of the underlying telemetry and the tuning of

analytics rules to the organization's specific environment; Ferrag, Maglaras, Moschoyiannis, and Janicke's (2020) finding that detection accuracy and false-positive rate trade off against one another means that analytics rules deployed without organization-specific tuning are likely to generate either missed detections or an unsustainable volume of false alerts.

Second, mapping detection logic to the MITRE ATT&CK framework, as Sentinel's built-in analytics rule templates do, provides a structured way to assess detection coverage across the full attack lifecycle rather than accumulating an unstructured collection of individually useful but uncoordinated rules. Al-Sada, Sadighian, and Oligeri's (2023) review of ATT&CK applications suggests that organizations should periodically audit which tactics and techniques their deployed analytics rules actually cover, since gaps in coverage often persist unnoticed until exploited.

Third, automated response introduces its own governance requirements. While Husák and Cegan (2014) and Kaiser et al. (2022) both demonstrate meaningful reductions in response time from automation, fully autonomous containment actions carry the risk of disrupting legitimate business activity if detection logic misfires, for instance automatically disabling an executive's account due to a false-positive anomalous sign-in alert. Organizations should therefore calibrate which response actions execute fully automatically, following the low-risk, high-confidence end of the detection spectrum, versus which require analyst confirmation before execution, particularly for actions with significant business disruption potential.

Fourth, alert correlation and incident aggregation are essential to making automated response scalable. Majeed, ur Rasool, Ahmad, Alam, and Javaid's (2019) work on distinguishing genuinely novel alerts from near-miss variations directly informs how Sentinel's incident correlation logic should be tuned; without effective correlation, automated playbooks risk triggering redundant or conflicting response actions across what is actually a single coordinated attack campaign.

Finally, the behavioral analytics techniques demonstrated by Cui, Zhang, Chen, and Yu (2022) for user and entity behavior analysis are particularly valuable for detecting the credential-based and insider-threat scenarios that signature-based detection consistently misses. Organizations should treat behavioral baselining as a complement to, rather than a replacement for, MITRE ATT&CK-mapped signature and anomaly rules, since each detection approach covers attack patterns that the other is likely to miss.

7. Recommendations

Organizations deploying Azure Sentinel for cyberattack detection and automated response should: (1) map every deployed analytics rule to its corresponding MITRE ATT&CK tactic and technique, and periodically audit the resulting coverage matrix for gaps, following the framework-based approach demonstrated by Al-Sada, Sadighian, and Oligeri (2023); (2) tune analytics rule thresholds against the organization's own baseline telemetry rather than relying solely on default thresholds, to manage the detection-accuracy and false-positive tradeoff documented by Ferrag, Maglaras, Moschoyiannis, and Janicke (2020); (3) classify automated response actions by risk and business-disruption potential, reserving fully automatic execution for low-risk, high-confidence scenarios and requiring analyst confirmation for high-impact actions; (4) deploy user and entity behavior analytics alongside signature- and anomaly-based analytics rules to cover credential-based and insider-threat scenarios, following Cui, Zhang, Chen, and Yu (2022); (5) establish a structured feedback loop in which analyst investigation findings are systematically used to refine analytics rules and playbook logic, as demonstrated by Ohmori (2019) and Kraeva and Yakhyayeva (2021); and (6) treat playbook design as an ongoing engineering discipline, with data-driven prioritization and phased implementation of new automation, drawing on the same disciplined project and cost-management principles that Agumalu (2021, 2022) applies to resource allocation and earned-value tracking in other large-scale operational programs, so that Sentinel adoption itself proceeds in a controlled, well-governed manner.

8. Conclusion

Cyberattack detection and response have evolved from manually operated, signature-based intrusion detection toward integrated, cloud-scale platforms that combine machine-learning analytics, structured threat intelligence,

and automated orchestration. Microsoft Azure Sentinel exemplifies this evolution, unifying data aggregation, MITRE ATT&CK-mapped analytics, incident correlation, and Logic Apps-based automated response within a single service. This article has proposed a detection and response pipeline architecture for Sentinel, mapped its core components to their underlying detection and response functions, and mapped common attack scenarios to specific detection logic and automated mitigations. The literature reviewed indicates that Sentinel's architecture directly operationalizes principles established across decades of intrusion detection, SIEM, and SOAR research, but that realizing its full benefit requires deliberate rule tuning, MITRE ATT&CK coverage auditing, and careful governance of which response actions are permitted to execute autonomously. As with the broader project and infrastructure governance challenges documented in other operational domains (Adenike, 2018, 2022; Agumalu, 2021, 2022), the technology itself is necessary but not sufficient; disciplined, well-governed implementation determines whether its detection and response capabilities are realized in practice. Future research should empirically evaluate mean time to detection and containment across production Sentinel deployments to quantify these benefits under real-world attack conditions.

Funding: This research received no external funding.

Conflicts of Interest: The authors declare no conflict of interest.

Publisher's Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers.

Artificial Intelligence (AI) Use Disclosure: The authors declare that no artificial intelligence tools were used in the preparation of this manuscript.

References

- [1] Adenike, A. (2018). Strengthening financial market infrastructure in emerging economies: Lessons from central banking operations. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, 10(02), 177–182. <https://doi.org/10.18090/samriddhi.v10i02.12>
- [2] Adenike, A. (2022). Central bank digital currency (CBDC) adoption challenges and remittance impacts: Empirical evidence from Nigeria's eNaira compared with global retail pilots and US Federal Reserve policy stance. *International Journal of Humanities and Information Technology*, 4(01-03), 214–233. <https://doi.org/10.21590/ijhit.04.01-3.16>
- [3] Agumalu, S. A. (2021). Project management strategies for improving NGO operational efficiency in Eastern Nigeria: A data-driven assessment of resource allocation, reporting, and project planning practices. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 4(1), 4351–4360. <https://doi.org/10.15662/IJRPETM.2021.0501005>
- [4] Agumalu, S. A. (2022). A predictive cost-management and benefits realization model for international projects using earned value management (EVM) to reduce cost overruns and improve project outcomes. *International Journal of Research Publications in Engineering, Technology and Management (IJRPETM)*, 5(2), 6517–6527.
- [5] Al-Sada, B., Sadighian, A., & Oligeri, G. (2023). MITRE ATT&CK: State of the art and way forward (arXiv:2308.14016). arXiv. <https://doi.org/10.48550/arXiv.2308.14016>
- [6] Bhuyan, M. H., Bhattacharyya, D. K., & Kalita, J. K. (2014). Network anomaly detection: Methods, systems and tools. *IEEE Communications Surveys & Tutorials*, 16(1), 303–336. <https://doi.org/10.1109/SURV.2013.052213.00046>
- [7] Cui, J., Zhang, G., Chen, Z., & Yu, N. (2022). Multi-homed abnormal behavior detection algorithm based on fuzzy particle swarm cluster in user and entity behavior analytics. *Scientific Reports*, 12, 22398. <https://doi.org/10.1038/s41598-022-26142-w>
- [8] Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, 50, 102419. <https://doi.org/10.1016/j.jisa.2019.102419>
- [9] Garcia, M., Bessani, A., Gashi, I., Neves, N., & Obelheiro, R. (2014). Analysis of operating system diversity for intrusion tolerance. *Software: Practice and Experience*, 44(6), 735–770. <https://doi.org/10.1002/spe.2180>
- [10] González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors*, 21(14), 4759. <https://doi.org/10.3390/s21144759>
- [11] Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. *Internet of Things*, 7, 100059. <https://doi.org/10.1016/j.iot.2019.100059>
- [12] Homer, J., Zhang, S., Ou, X., Schmidt, D., Du, Y., Rajagopalan, S. R., & Singhal, A. (2013). Aggregating vulnerability metrics in enterprise networks using attack graphs. *Journal of Computer Security*, 21(4), 561–597. <https://doi.org/10.3233/JCS-130475>

- [13] Husák, M., & Cegan, J. (2014). PhiGARo: Automatic phishing detection and incident response framework. In 2014 Ninth International Conference on Availability, Reliability and Security (pp. 295–302). IEEE. <https://doi.org/10.1109/ARES.2014.46>
- [14] Islam, C., Babar, M. A., & Nepal, S. (2020). Architecture-centric support for integrating security tools in a security orchestration platform. In Software Architecture: 14th European Conference, ECSA 2020 (pp. 165–181). Springer. https://doi.org/10.1007/978-3-030-58923-3_11
- [15] Kaiser, F. K., Andris, L. J., Tennig, T. F., Iser, J. M., Wiens, M., & Schultmann, F. (2022). Cyber threat intelligence enabled automated attack incident response. In 2022 3rd International Conference on Next Generation Computing Applications (NextComp) (1–6). IEEE. <https://doi.org/10.1109/NextComp55567.2022.9932254>
- [16] Kraeva, I., & Yakhyayeva, G. (2021). Application of metric learning for security incident playbook recommendation. In 2021 IEEE 22nd International Conference of Young Professionals in Electron Devices and Materials (EDM) (1194–1200). IEEE. <https://doi.org/10.1109/EDM52169.2021.9507632>
- [17] Kwon, R., Ashley, T., Castleberry, J., McKenzie, P., & Gupta Gouriseti, S. N. (2020). Cyber threat dictionary using MITRE ATT&CK Matrix and NIST Cybersecurity Framework mapping. In 2020 Resilience Week (RWS) (106–112). IEEE. <https://doi.org/10.1109/RWS50334.2020.9241271>
- [18] Majeed, A., ur Rasool, R., Ahmad, F., Alam, M., & Javaid, N. (2019). Near-miss situation based visual analysis of SIEM rules for real time network security monitoring. *Journal of Ambient Intelligence and Humanized Computing*, 10(4), 1509–1526. <https://doi.org/10.1007/s12652-018-0936-7>
- [19] Mashima, D. (2022). MITRE ATT&CK based evaluation on in-network deception technology for modernized electrical substation systems. *Sustainability*, 14(3), 1256. <https://doi.org/10.3390/su14031256>
- [20] Modi, C., Patel, D., Borisaniya, B., Patel, H., Patel, A., & Rajarajan, M. (2013). A survey of intrusion detection techniques in cloud. *Journal of Network and Computer Applications*, 36(1), 42–57. <https://doi.org/10.1016/j.jnca.2012.05.003>
- [21] Moukafih, N., Orhanou, G., & Elhajji, S. (2020). Mobile agent-based SIEM for event collection and normalization externalization. *Information & Computer Security*, 28(1), 15–34. <https://doi.org/10.1108/ICS-01-2019-0008>
- [22] Ohmori, M. (2019). On automation and orchestration of an initial computer security incident response by introducing a centralized incident tracking system. *Journal of Information Processing*, 27, 564–572. <https://doi.org/10.2197/ipsjip.27.564>
- [23] Othman, S. M., Ba-Alwi, F. M., Alsohybe, N. T., & Al-Hashida, A. Y. (2018). Intrusion detection model using machine learning algorithm on Big Data environment. *Journal of Big Data*, 5, 34. <https://doi.org/10.1186/s40537-018-0145-4>
- [24] Radoglou-Grammatikis, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., Eftathopoulos, G., Spyridis, Y., Sesis, A., & Vakakis, N. (2021). SPEAR SIEM: A Security Information and Event Management system for the Smart Grid. *Computer Networks*, 193, 108008. <https://doi.org/10.1016/j.comnet.2021.108008>
- [25] Salo, F., Nassif, A. B., & Essex, A. (2019). Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection. *Computer Networks*, 148, 164–175. <https://doi.org/10.1016/j.comnet.2018.11.010>
- [26] Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Communications Surveys & Tutorials*, 23(4), 2525–2556. <https://doi.org/10.1109/COMST.2021.3117338>
- [27] Tidjon, L. N., Frappier, M., & Mammar, A. (2019). Intrusion detection systems: A cross-domain overview. *IEEE Communications Surveys & Tutorials*, 21(4), 3639–3681. <https://doi.org/10.1109/COMST.2019.2922584>
- [28] Yulianto, A., Sukarno, P., & Suwastika, N. A. (2019). Improving AdaBoost-based intrusion detection system (IDS) performance on CIC IDS 2017 dataset. *Journal of Physics: Conference Series*, 1192, 012018. <https://doi.org/10.1088/1742-6596/1192/1/012018>