Risk-Based Alerting in Siem Enterprise Security: Enhancing Attack Scenario Monitoring Through Adaptive Risk Scoring

Article *in* INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY · April 2020

DOI: 10.34218/IJCET_11_02_009

International Journal of Computer Engineering and Technology (IJCET)
Volume 11, Issue 2, March-April, 2020, pp. 75-85, Article ID: IJCET_11_02_009
Available online at https://iaeme.com/Home/issue/IJCET?Volume=11&Issue=2
ISSN Print: 0976-6367; ISSN Online: 0976-6375
DOI: https://doi.org/10.34218/IJCET_11_02_009

RISK-BASED ALERTING IN SIEM ENTERPRISE SECURITY: ENHANCING ATTACK SCENARIO MONITORING THROUGH ADAPTIVE RISK SCORING

Karthik Chandrashekar
Senior Software Engineer,
Intuit Inc, United States.

Vinay Dutt Jangampet
Staff Systems Engineer,
Intuit Inc, United States.

ABSTRACT

Traditional sequenced search-based alerting mechanisms in SIEM Enterprise Security are effective for detecting predefined attack scenarios but exhibit significant limitations in handling the complexity and variability of modern threats. These mechanisms rely on rigid sequences of conditions to trigger alerts, which often results in missed detections when attackers use alternative techniques to achieve their objectives. This creates critical gaps in security monitoring and leaves enterprise environments vulnerable to sophisticated attack strategies.

To address these challenges, this paper introduces a Risk-Based Alerting (RBA) framework that leverages the advanced capabilities of SIEM's Risk Analysis Framework. Unlike sequenced search-based systems, the RBA framework dynamically evaluates and scores events based on multiple factors, including the fidelity of the security event, the risk profile of the asset involved, and the criticality of the associated attack scenario. This approach ensures comprehensive coverage by capturing both high-fidelity and low-fidelity alerts. However, only high-priority alerts that exceed a predefined risk threshold are classified as "notable," significantly reducing the noise generated by low-impact alerts.

The RBA framework employs adaptive risk scoring mechanisms that account for evolving attack patterns and operational contexts. By incorporating non-overlapping scheduling, throttling mechanisms, and real-time dashboard enhancements, the framework streamlines alert prioritization and improves the overall efficiency of security operations. Furthermore, the integration of industry-standard frameworks, such as MITRE ATT&CK, ensures a robust and comprehensive mapping of attack techniques, enabling precise detection and actionable insights.

Our findings demonstrate that the RBA framework significantly enhances the prioritization and detection of critical events while mitigating operational inefficiencies. Key outcomes include a substantial reduction in false positives, improved usability of risk analysis dashboards, and better alignment with real-world threat landscapes. This paper concludes by highlighting the potential of RBA to transform SIEM Enterprise Security into a more dynamic, responsive, and effective defense mechanism against modern cyber threats.

Keywords: SIEM, Risk-Based Alerting (RBA), Risk Analysis Framework, Alert prioritization, High/low-fidelity alerts, Adaptive risk scoring, MITRE ATT&CK, Operational efficiency, Threat detection, False positives reduction.

Cite this Article: Karthik Chandrashekar, Vinay Dutt Jangampet. Risk-Based Alerting in Siem Enterprise Security: Enhancing Attack Scenario Monitoring Through Adaptive Risk Scoring. *International Journal of Computer Engineering and Technology (IJCET)*, 11(2), 2020, 75-85.

https://iaeme.com/Home/issue/IJCET?Volume=11&Issue=2

Introduction

In the rapidly evolving landscape of cybersecurity, the complexity and sophistication of attack techniques have increased significantly. The emergence of advanced persistent threats (APTs), ransomware-as-a-service models, and zero-day vulnerabilities has underscored the need for robust, flexible, and adaptive security systems. Enterprise Security Information and Event Management (SIEM) systems have become the backbone of modern cybersecurity operations, providing centralized logging, analysis, and response capabilities. By aggregating data from multiple sources, SIEM systems enable organizations to detect anomalies, correlate events, and respond to potential threats in real time. However, the increasing diversity of attack techniques has exposed significant gaps in traditional SIEM functionalities.

Challenges of Traditional Sequenced Search-Based Alerting

One of the foundational methods in SIEM systems is sequenced search-based alerting, which relies on predefined event sequences to identify notable security incidents. For example, a sequence of login attempts from multiple IP addresses followed by administrative account creation might indicate a brute force attack. While effective in detecting specific patterns, this approach has inherent limitations. It lacks the flexibility to account for deviations in attacker methodologies.

Attackers often employ diverse techniques to achieve the same objective. For instance, in the case of a compromised EC2 instance, one attacker may install a crypto miner by leveraging weak credentials, while another may exploit unpatched vulnerabilities in an application running on the instance. The sequenced search model is rigid and unable to detect these variations, as it focuses on predefined conditions. Consequently, such limitations lead to missed alerts and reduce the overall security coverage.

Impact of Modern Threat Landscape

The modern threat landscape is characterized by increasing automation and scalability of attacks. Attackers can now execute complex campaigns across multiple environments, including cloud, on-premises, and hybrid infrastructures. These campaigns often involve lateral movement, privilege escalation, and data exfiltration—none of which may follow a predictable sequence. Moreover, with the growing adoption of containerization and serverless

architectures, traditional monitoring techniques struggle to provide the granularity required to detect sophisticated threats.

In addition to technical challenges, the sheer volume of alerts generated by SIEM systems further complicates security operations. Low-fidelity alerts, while not critical on their own, can overwhelm security analysts when combined with high-priority alerts. The result is alert fatigue, where critical events may be overlooked due to the noise created by irrelevant or redundant alerts.

The Need for a Risk-Based Approach

To address these challenges, there is a pressing need for an adaptive and dynamic approach to alerting. A risk-based framework shifts the focus from static, rule-based detection to dynamic evaluation of events based on their context, fidelity, and associated risk. Such a framework not only captures a wider range of attack scenarios but also prioritizes alerts based on their potential impact. This ensures that security analysts can focus on high-priority events, improving both detection accuracy and operational efficiency.

The Risk-Based Alerting (RBA) framework is designed to address these gaps by leveraging SIEM's advanced Risk Analysis capabilities. Unlike sequenced searches, RBA dynamically scores and prioritizes events, enabling comprehensive monitoring of diverse attack techniques. It integrates industry-standard frameworks like MITRE ATT&CK to map detected events to known adversarial tactics, techniques, and procedures (TTPs), providing actionable insights to security teams.

Advancing Security Monitoring with RBA

RBA represents a paradigm shift in SIEM-based monitoring, emphasizing flexibility and adaptability. By continuously evaluating the risk associated with each event, RBA minimizes false positives, reduces noise, and aligns monitoring strategies with real-world attack techniques. This approach not only addresses the limitations of traditional sequenced search mechanisms but also enhances the overall resilience of enterprise security systems against evolving threats.

In the following sections, this paper explores the design, implementation, and evaluation of the RBA framework, demonstrating its effectiveness in addressing the challenges of traditional alerting mechanisms while paving the way for next-generation SIEM capabilities.

Methods

Sequenced Search-Based Alerting

Sequenced search-based alerting has been a cornerstone of traditional SIEM systems, relying on a defined series of conditions or events to trigger alerts. For example, a sequenced search may be configured to detect potential unauthorized access by requiring the following conditions to occur in order: multiple failed login attempts, successful login from a different geographic location, and privilege escalation activities. If any step in this sequence is skipped or occurs out of order, no alert is generated.

While this approach ensures precision in detecting specific patterns, it inherently lacks flexibility. Modern attack scenarios are often dynamic, with attackers employing varying techniques to achieve their objectives. For instance, an attacker compromising an EC2 instance might exploit a vulnerability, use stolen credentials, or escalate privileges using social engineering tactics. Such variability in attacker behavior renders sequenced searches ineffective, as they are unable to detect deviations from predefined patterns.

Furthermore, sequenced searches fail to account for emerging threats that do not align with established sequences. As a result, critical attack scenarios may go undetected, reducing the overall efficacy of security monitoring. This limitation underscores the need for a more adaptive and comprehensive approach to alerting, as addressed by the Risk-Based Alerting (RBA) framework.

Risk-Based Alerting Framework

The RBA framework builds upon the limitations of sequenced search-based alerting by introducing a dynamic and flexible risk scoring system. Unlike traditional methods, RBA evaluates the risk associated with each event in real-time, considering factors such as event fidelity, asset criticality, and attack context.

Key Components of the RBA Framework

1. RISK SCORE CALCULATION

Risk scoring forms the backbone of the RBA framework. Each event is assigned a risk score based on the formula:

Calculated Risk Score=(Base Risk Score×Fidelity)×Risk Factor\text{Calculated Risk Score} = (\text{Base Risk Score} \times \text{Fidelity}) \times \text{Risk Factor}Calculated Risk Score=(Base Risk Score×Fidelity)×Risk Factor

Here, the Base Risk Score represents the inherent risk associated with the event, Fidelity indicates the reliability of the detection mechanism, and Risk Factor accounts for additional contextual factors such as asset criticality or environmental conditions.

The total risk score for an attack scenario is then aggregated by summing the calculated risk scores of all associated risk rules. This aggregated score provides a comprehensive view of the potential impact of the scenario.

Risk,Fidelity	**>75%**	**50% - 75%**	**25% - 50%**	**<25%**
Critical	Critical	Critical	High	Medium
High	Critical	High	High	Medium
Medium	High	Medium	Medium	Low
Low	Medium	Medium	Low	Low

2. ALERT PRIORITIZATION

Once risk scores are calculated, alerts are categorized into critical, high, medium, and low priorities based on predefined thresholds. This categorization is guided by the Risk Matrix and IVSS Matrix, which align risk scores with severity levels. For example:

- Critical alerts are those with risk scores exceeding 75.
- High alerts range from 50 to 75.
- Medium alerts fall between 25 and 50.
- Low alerts are below 25.

Priority	**IVSS Score**
Critical - P0	20 - 25
High - P1	15 - 19.9
Medium - P2	10 - 14.9
Low - P3	< 10

3. By prioritizing alerts, the RBA framework ensures that security teams focus their efforts on addressing the most significant threats first, improving response times and resource allocation.

Severity	**Risk Score (Base Value)**
Critical - P0	> 75
High - P1	> 50 & < 75
Medium - P2	> 25 & <50
Low - P3	<25

Implementation Details

The implementation of the RBA framework is designed to maximize efficiency and accuracy. Key strategies include:

1. **Non-Overlapping Cron Schedules**
   To optimize resource utilization and ensure timely detection, different cron schedules are defined for attack scenarios based on their severity:
   - **Critical and High-Severity Scenarios:** Monitored every 5 minutes.
   - **Medium-Severity Scenarios:** Checked hourly.
   - **Low-Severity Scenarios:** Monitored every 4 hours.
2. Non-overlapping schedules prevent conflicts and ensure that critical searches are not delayed by lower-priority tasks. This approach enhances the overall detection capability of the SIEM system.
3. **Throttling Mechanisms**

Throttling is employed to reduce noise and prevent alert fatigue, particularly for low-severity events. By grouping similar alerts and applying deduplication, throttling ensures that only meaningful and actionable alerts are presented to security analysts. For example:
    - Critical alerts may have a throttling window of 4 hours, grouped by fields such as AWS account ID or domain.
    - Low-severity alerts may have a longer throttling window, such as one week, to minimize unnecessary noise.
4. This mechanism allows the RBA framework to maintain a balance between alert volume and actionable intelligence.
5. **Risk Analysis Dashboard Enhancements**
   The Risk Analysis Dashboard serves as the primary interface for security teams to monitor and respond to alerts. Enhancements to the dashboard include:
    - Improved visualizations for risk scores and alert trends.
    - Filters to focus on high-priority alerts.
    - Integration with the MITRE ATT&CK framework to provide contextual information about detected events.
6. These updates enhance the usability of the dashboard, enabling security teams to quickly identify and address critical threats.

Adaptive Response Actions

The RBA framework includes dynamic adjustments to risk scores based on real-time data and feedback. Key factors influencing these adjustments are:

- **Fidelity of Security Events:** High-fidelity events, such as logs from trusted sources, receive higher weight in risk calculations.
- **Criticality of Affected Assets:** Events impacting critical assets, such as production servers or sensitive databases, are assigned higher risk scores.
- **Mapping to the MITRE ATT&CK Framework:** By aligning detected events with known adversarial tactics, techniques, and procedures (TTPs), the RBA framework ensures comprehensive threat coverage.

These adaptive actions ensure that the RBA framework remains responsive to the evolving threat landscape, providing a robust defense mechanism for enterprise environments.

By integrating these components, the RBA framework addresses the limitations of traditional sequenced search-based alerting, providing a more flexible and effective approach to security monitoring. The next sections will demonstrate the results and effectiveness of this framework in real-world scenarios.

Results

The implementation of the Risk-Based Alerting (RBA) framework introduced significant improvements across several dimensions of security monitoring in SIEM systems. This section details the observed enhancements in alert prioritization, detection capabilities, operational efficiency, and the integration of industry-standard frameworks.

Improved Alert Prioritization

The primary goal of the RBA framework is to ensure that high-fidelity alerts receive the attention they deserve while reducing the noise from low-impact events. By dynamically calculating risk scores and categorizing alerts based on their severity, the framework achieves a robust prioritization mechanism.

In traditional sequenced search-based systems, critical events could often be overshadowed by the sheer volume of low-priority alerts, leading to alert fatigue among security analysts. The RBA framework addresses this issue by aligning notable alerts with real-world attack scenarios. For example, alerts related to crypto miner processes running on compromised EC2 instances are elevated based on their criticality and risk score. This ensures that such events are marked as "notable" and are promptly brought to the attention of security teams.

Furthermore, the prioritization process takes into account the fidelity of the event source. High-fidelity sources, such as logs from cloud service providers or application firewalls, are weighted more heavily, reducing the likelihood of false positives. This approach significantly improves the reliability of alerts, ensuring that critical events are not missed due to misclassification or insufficient scoring.

Enhanced Detection Capabilities

One of the major limitations of traditional sequenced search-based alerting is its inability to detect variations in attacker methodologies. The RBA framework addresses this by employing non-overlapping cron schedules and adaptive risk scoring mechanisms, which enhance the system's detection capabilities.

Non-Overlapping Cron Schedules

The RBA framework's use of tailored cron schedules ensures that critical and high-priority scenarios are monitored at shorter intervals, typically every 5 minutes. This rapid monitoring cycle allows for near-real-time detection of high-risk events, such as privilege escalation attempts or lateral movement within a network.

Medium-severity scenarios are scheduled for hourly monitoring, while low-severity scenarios are checked every 4 hours. This staggered approach ensures that system resources are utilized efficiently without compromising the detection of less critical events. By avoiding overlapping cron schedules, the RBA framework minimizes the risk of missed detections due to resource contention or search delays.

Adaptive Risk Scoring

The adaptive risk scoring mechanism dynamically evaluates events based on their context, fidelity, and associated risk factors. This ensures comprehensive coverage across all severity levels, from low to critical. For instance, a low-severity event, such as repeated failed login attempts on a non-critical asset, may not trigger immediate action but is still tracked for trend analysis. In contrast, a critical event, such as unauthorized access to a production database, is flagged for immediate investigation.

The combination of adaptive scoring and optimized scheduling has resulted in a significant improvement in the system's ability to detect and respond to attack scenarios across the enterprise.

Operational Efficiency

The introduction of the RBA framework has had a profound impact on the operational efficiency of the SIEM system. Key improvements include the reduction of noise from low-

severity alerts, enhanced usability of the Risk Analysis Dashboard, and streamlined incident management processes.

Noise Reduction and Throttling

Low-severity alerts, which often contribute to alert fatigue, are now effectively managed through throttling mechanisms. By grouping similar alerts and applying deduplication, the framework minimizes the volume of repetitive notifications. For example, low-severity events, such as minor policy violations or non-critical configuration changes, are aggregated and presented as a single alert with contextual details. This allows security analysts to focus on actionable intelligence rather than sifting through redundant notifications.

Dashboard Usability

The Risk Analysis Dashboard has been enhanced to provide clearer visualizations and more intuitive navigation. Filters for severity, risk score, and event type allow analysts to quickly identify high-priority threats. Additionally, the dashboard now includes detailed mappings to the MITRE ATT&CK framework, providing contextual information about detected events. These updates have made the dashboard a central tool for effective threat monitoring and incident response.

Streamlined Incident Management

The improved prioritization and noise reduction mechanisms have streamlined the incident management process. Notable events are automatically escalated based on their urgency, ensuring timely resolution. The alignment of urgency levels with asset criticality further reduces confusion and enhances the efficiency of response teams.

MITRE ATT&CK Framework Integration

The integration of the MITRE ATT&CK framework into the RBA system represents a significant enhancement in the comprehensiveness of threat monitoring. By mapping risk rules and notable events to known adversarial tactics, techniques, and procedures (TTPs), the framework provides a structured and actionable view of potential attack vectors.

Comprehensive Threat Mapping

Each notable event is now associated with one or more techniques from the MITRE ATT&CK matrix. For example, a detected instance of unauthorized script execution on a server might be mapped to "Command and Scripting Interpreter" (T1059), providing immediate context about the adversarial behavior.

Actionable Insights

The integration also enables the identification of gaps in the current security posture. For instance, if a specific TTP frequently appears in alerts but lacks a corresponding mitigation strategy, it highlights an area for improvement. Security teams can use this information to prioritize updates to their defense mechanisms, ensuring alignment with industry best practices.

Enhanced Reporting and Compliance

Finally, the use of MITRE ATT&CK mappings enhances the system's reporting capabilities. By presenting alerts in the context of a globally recognized framework, organizations can demonstrate compliance with security standards and frameworks, such as NIST or ISO 27001.

The RBA framework has transformed the SIEM system into a more dynamic, responsive, and effective tool for enterprise security monitoring. By improving alert prioritization, detection

capabilities, operational efficiency, and threat mapping, the framework addresses the limitations of traditional sequenced search-based systems while aligning with modern cybersecurity challenges. The next section will explore the broader implications of these findings and potential areas for future enhancement.

Discussion

The Risk-Based Alerting (RBA) framework represents a significant advancement in the field of enterprise security monitoring, offering solutions to several limitations of traditional sequenced search-based alerting mechanisms. By introducing flexibility and adaptability, the RBA framework aligns better with the dynamic nature of modern cybersecurity threats. This section discusses the benefits, challenges, and potential future directions for enhancing the framework.

Benefits of Risk-Based Alerting

The RBA framework is designed to overcome the rigid structure of sequenced search-based alerting, providing a more comprehensive and dynamic approach to monitoring attack scenarios.

1. **Comprehensive Monitoring of Diverse Attack Scenarios**
   Traditional sequenced searches are limited to predefined patterns, making them ineffective against attackers who use alternative techniques to achieve the same goal. The RBA framework, with its dynamic risk scoring and aggregation of multiple risk rules, enables the detection of a broader range of attack techniques. For instance, whether an attacker exploits a software vulnerability or uses stolen credentials, the RBA framework ensures that such events are evaluated holistically, minimizing the risk of oversight.
2. **Improved Alignment with Real-World Attack Techniques**
   By integrating the MITRE ATT&CK framework, RBA provides contextual mapping of alerts to known adversarial tactics, techniques, and procedures (TTPs). This alignment offers security teams actionable insights, allowing them to prioritize responses based on established attack patterns. For example, detecting a lateral movement attempt (T1021) or unauthorized script execution (T1059) becomes more precise when associated risk rules are mapped to MITRE ATT&CK techniques.
3. **Enhanced Resource Allocation Through Prioritized Scheduling**

   The RBA framework optimizes the allocation of system resources and analyst efforts by categorizing alerts based on risk scores and prioritizing them accordingly. Critical and high-priority scenarios are monitored at frequent intervals, ensuring timely detection and response. Meanwhile, low-severity events are tracked less frequently, conserving resources without compromising long-term trend analysis.

Overall, these benefits make the RBA framework a more efficient and effective solution for enterprise security monitoring, reducing alert fatigue and improving threat coverage.

Challenges and Limitations

Despite its many advantages, the implementation and operation of the RBA framework come with certain challenges:

1. **Calibration of Risk Scores and Thresholds**

The effectiveness of RBA heavily depends on accurately calibrating risk scores and thresholds. Overly aggressive scoring can lead to a high volume of false positives, burdening security teams with unnecessary alerts. Conversely, overly conservative thresholds may result in missed detections of critical events, leaving the organization vulnerable to potential breaches. Achieving the right balance requires continuous refinement based on real-world feedback and operational data.

2. **Complexity of Implementation**
   The integration of dynamic risk scoring mechanisms and advanced features, such as non-overlapping cron schedules and throttling, requires careful planning and execution. Organizations need to invest time and resources to ensure smooth deployment and ongoing maintenance of the framework.
3. **Dependence on Accurate Data**
   The accuracy of the RBA framework relies on high-quality data from various sources. Inconsistent or incomplete data can impact the calculation of risk scores, leading to inaccuracies in alert prioritization. Ensuring data fidelity is critical for the success of the framework.

While these challenges are significant, they are not insurmountable. With proper planning, validation, and refinement, organizations can mitigate these limitations and fully realize the benefits of the RBA framework.

Future Work

The RBA framework has demonstrated significant potential in addressing the limitations of traditional alerting mechanisms, but there is room for further enhancement. Future efforts should focus on the following areas:

1. **Integration of Machine Learning Algorithms**

   Machine learning can play a pivotal role in refining risk scoring mechanisms. By analyzing historical data and identifying patterns in attack scenarios, machine learning models can enhance the accuracy of risk scores and thresholds. For example, anomaly detection algorithms could identify unusual behaviors that warrant higher risk scores, improving the detection of emerging threats.
2. **Development of Feedback Loops for Continuous Improvement**
   Establishing feedback loops between security analysts and the RBA framework can help validate and improve risk rules. Analysts can provide input on false positives or missed detections, enabling the system to adapt and evolve over time. This iterative approach ensures that the framework remains effective in the face of evolving threats.
3. **Expansion of Attack Scenario Libraries**
   Incorporating insights from open-source intelligence and threat research can expand the library of attack scenarios monitored by the RBA framework. By integrating new TTPs and aligning them with existing risk rules, organizations can stay ahead of adversaries and maintain comprehensive threat coverage.

Conclusion

The Risk-Based Alerting (RBA) framework signifies a major leap forward in the field of SIEM Enterprise Security by addressing the inherent limitations of traditional sequenced search-based alerting mechanisms. In an era where attackers continuously adapt their techniques, the static nature of sequenced searches has proven insufficient. The RBA framework overcomes these

challenges through the use of adaptive risk scoring, which dynamically evaluates and prioritizes alerts based on event fidelity, asset criticality, and contextual risk factors.

By integrating key features such as non-overlapping cron schedules, throttling mechanisms, and dynamic prioritization, the RBA framework ensures that security analysts focus on the most critical threats. High-fidelity alerts are brought to the forefront, while low-priority alerts are effectively managed, reducing alert fatigue and optimizing resource allocation. Moreover, the seamless integration with the MITRE ATT&CK framework further enhances the system's ability to map alerts to real-world adversarial tactics, techniques, and procedures (TTPs), providing actionable insights and improving the accuracy of threat detection.

Operationally, the RBA framework streamlines workflows by improving the usability of dashboards and automating the escalation of critical events. This alignment with the evolving threat landscape ensures that enterprise environments are equipped to handle both known and emerging attack scenarios.

In conclusion, the RBA framework not only addresses the shortcomings of traditional alerting systems but also sets the stage for more dynamic, intelligent, and effective security monitoring. Its adaptive nature and emphasis on risk-based prioritization make it an essential tool in modern cybersecurity, ensuring robust protection and resilience in enterprise environments. As the framework continues to evolve, it has the potential to redefine industry standards for SIEM systems, making it a cornerstone of proactive and responsive security strategies.

References

[1] K. Scarfone, M. Souppaya, and A. Cody, "Guide to Computer Security Log Management," NIST Special Publication 800-92, 2006.

[2] MITRE Corporation, "MITRE ATT&CK Framework," 2015. [Online]. Available: https://attack.mitre.org.

[3] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Computing Surveys (CSUR)*, vol. 41, no. 3, pp. 1–58, 2009.

[4] R. Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*. San Francisco, CA, USA: No Starch Press, 2013.

[5] Splunk Inc., "Risk-Based Alerting Framework Documentation," Splunk Official Guide, 2017.

[6] Symantec Corporation, "Advanced Threat Protection: Concepts and Case Studies," Symantec White Paper, 2019.

[7] K. Stouffer, J. Falco, and K. Scarfone, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800-82 Revision 2, 2015.

[8] S. Rajasekharan and T. Thomas, "Next-Generation SIEM Systems: A Survey," *Journal of Cybersecurity*, 2018.

[9] Cisco Systems, "Best Practices for SIEM Implementations," Cisco White Paper, 2018.

[10] Red Canary, "The Atomic Red Team Framework: Threat Simulation Made Simple," Red Canary Technical Guide, 2018.