2581-4575
International Journal For Recent Developments in Science & Technology
Crossref
A Peer Reviewed Research Journal

Enhancing SIEM Usability and Accessibility for Security Analysts

Avinash Gupta Desetty
Splunk Engineer
Sony Corporation Of America
Dallas,USA
gupta.splunker@gmail.com

Abstract:

Security Information and Event Management (SIEM) solutions are essential for organizations to effectively monitor, detect, and address evolving cyber threats. However, SIEM systems' inefficiency is limited by their complexity and lack of user-friendliness. To address these problems, organizations need to take steps to make SIEM more user-friendly and accessible to security analysts.

Effective strategies include streamlining user interactions, enhancing data visualization, promoting seamless integration with other security systems, and providing extensive documentation and training. It is imperative that SIEM systems undergo constant enhancements and modifications to meet the evolving needs of security teams. To identify and address usability concerns, collaboration, honest feedback, and open communication are necessary.

Increasing the system's usability and accessibility can help organizations battle cyber threats, strengthen their cybersecurity posture, and get the most out of their SIEM investments.

Keywords — SIEM, Cybersecurity, Usability, Accessibility, Security analysts, Data visualization, Integration, Threat detection, Incident response, Cybersecurity posture

Introduction

Security Information and Event Management (SIEM) solutions are becoming essential tools in the ever-expanding field of cybersecurity for businesses of all kinds, defending their digital borders against the constant barrage of cyberattacks. SIEMs are essential tools for security analysts because they carefully gather, examine, and correlate log data from a wide range of sources, giving them a clear and informative picture of the security posture of their company. Nevertheless, SIEMs' intrinsic complexity frequently poses difficult problems, impeding their ability to quickly detect and address security breaches. In order to turn SIEMs into effective and user-friendly tools that optimize the value of these vital instruments, this article explores various approaches for improving SIEM usability and accessibility for security analysts. Organizations can enable their security analysts to fully utilize SIEMs and ensure a proactive and strong cybersecurity posture, protecting their valuable assets and sustaining a strong presence in the constantly changing digital landscape, by

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

tackling the issues of complexity, alert fatigue, contextualization, and customization.

I. Literature Survey on SIEM Usability and Accessibility

SIEM (Security Information and Event Management) systems have become indispensable instruments for enterprises of all kinds to keep monitor on, utilize, and respond to security events. Security analysts are given a thorough understanding of their organization's security posture via SIEMs, which gather, examine, and correlate log data from several sources. Nevertheless, SIEMs' intrinsic complexity may make it more difficult for them to recognize and respond to security threats.

A. Key Challenges and Real-time Scenarios or Challenges

1) Complexity:

a) Challenges:

- Overwhelming User Interface (UI): Security analysts may find it challenging to navigate SIEMs' cluttered UIs with erratic terminology and complex data structures.
- Inconsistent Terminology: Analysts may become confused and find it more difficult to find pertinent information if jargon and inconsistent terminology are used across various SIEM components.
- Complex Data Structures: Analysts without specialized training may find it difficult to understand the intricate data structures and formats used in SIEMs.

b) Real-time Scenario:

A possible data breach is alerted to a security analyst. Nevertheless, the analyst finds it difficult to locate the pertinent log data and assess the scope of the breach because of the confusing user interface and inconsistent terminology. The attacker might be able to take advantage of more vulnerabilities as a result of the delay in determining the extent of the incident.

*2) Alert Fatigue:***

a) Challenges:

- High Alert Volume: SIEMs continuously produce a large number of false positives or irrelevant alerts. This may overwhelm analysts and cause them to become insensitive to important events.

- Ineffective Alert Prioritization: SIEMs might not do a good job of prioritizing alerts, which leaves analysts missing important events and wasting time on unimportant notifications.
- Difficulty Determining Alert Severity: Insufficient context may make it difficult for analysts to determine the seriousness of alerts, which could cause them to react improperly or too slowly.

b) Real-time Scenario:

A security analyst finds it challenging to concentrate on the most important events due to the constant barrage of alerts from multiple sources. Because of the excessive number of alerts and the hazy prioritization,

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

the analyst might overlook a real security risk.

3) *Contextualization:**

a) *Challenges:*

- Ineffective Correlation of Relevant Log Data: SIEMs may fail to efficiently correlate log data from various sources, which keeps analysts from getting a complete picture of the context surrounding the event.
- Limited Network Traffic Visibility: Analysts may be unable to identify the origin, character, and scope of suspicious activity if they do not have visibility into network traffic.
- Lack of Integration with Threat Intelligence: Information about known vulnerabilities, threat actor profiles, and malware signatures can all be used to add important context to alerts.

b) *Real-time Scenario:*

An alert about a possible data breach reaches a security analyst. However, the analyst is unable to ascertain the scope of the breach or pinpoint the attacker's techniques if they do not have access to pertinent log data, network traffic data, or threat intelligence. This lack of context may cause reaction strategies to be ineffective or incorrect.

4) *Customization:**

a) *Challenges:*

- Inability to Customize Dashboards for Particular Roles: SIEMs may prevent analysts from customizing dashboards to meet their unique set of duties and responsibilities, which makes it more difficult for them to keep an eye on pertinent metrics and alerts.
- Strict Alert Configurations for Various Environments: Pre-established alert thresholds and rules might not be compatible with the particular security stance of various user groups or network segments.
- Lack of Flexibility in Event Correlation Rules: Fixed correlation rules might not be able to account for the unique security needs of various industries or standards of regulatory compliance.

b) *Real-time Scenario:*

The SIEM dashboard cannot be customized by a security analyst working on a highly sensitive network segment to show pertinent metrics and alerts for that segment, possibly leaving important threats unnoticed. Inadequate customization may result in ineffective reaction strategies for the particular network environment or the missing of important threats.

5) *Unique Approaches to SIEM Usability and Accessibility*

a) *User-Centered Design (UCD):*

Strategies:

- Involve Security Analysts in Design Workshops: To get their feedback on the user interface, alert prioritization, and contextualization features, hold workshops with security analysts.
- Perform Usability Testing with Diverse User Groups: To find usability issues across a range of skill levels and experiences, test the SIEM on a regular basis with a diverse group of security analysts.
- Design for Cross-Platform Accessibility: Meeting the demands of remote or mobile workers by making sure the SIEM is compatible with a range of devices, including desktops, laptops, and mobile platforms.

International Journal For Recent Developments in Science & Technology
2581-4575
Crossref
A Peer Reviewed Research Journal

Real-time Scenario:

Security analysts from various departments participate in a design workshop led by a software development team to provide input on the usefulness and efficacy of the SIEM for their respective roles.

b) Machine Learning and Artificial Intelligence (ML/AI):

Techniques:

Implementing Machine Learning Algorithms to Sort Alerts: Train machine learning algorithms to find patterns in past data and apply filters.

CONCLUSION

Organizations now depend heavily on SIEMs as vital tools for managing, tracking, and reacting to security events. Nevertheless, SIEMs' intrinsic complexity may make it more difficult for them to recognize and respond to security threats. The main issues and current situations pertaining to SIEM accessibility and usability were noted in this literature review, along with original solutions to these issues. Businesses can greatly increase the efficacy of their SIEMs by putting techniques like machine learning, visualization, and user-centered design into practice.

References

[1] Adams, A., & Sasse, A. (2009). User-centered design for security informatics. In Security and Privacy in Information Systems (pp. 101-117). Springer, Berlin, Heidelberg.

[2] Carr, J., & Hu, W. (2014). An evaluation of correlation rule analysis techniques for security information and event management. Journal of Network and Computer Applications, 40, 1-15.

[3] Goodman, C., & Scaffidi, C. (2014). Context-sensitive help for security information and event management (SIEM) systems. In Advances in Human-Computer Interaction (pp. 57-62). Springer, Cham.

[4] He, Q., Li, Z., & Jin, S. (2015). An efficient alert correlation and prioritization method for security information and event management (SIEM) in cloud computing environment.

[5] Kaisler, P., Tuecke, S., & Rundel, C. (2017). Customizable dashboards in security information and event management (SIEM) systems: Benefits and challenges. Computer Fraud & Security, 2017(11), 16-21.

[6] Liao, Y., Sun, Z., & Jin, H. (2016). Anomaly detection and alert correlation for security information and event management (SIEM). In Security and Privacy in Information Systems (pp. 272-286). Springer, Berlin, Heidelberg.

[7] Yurcik, W., & Alexander, S. (2016). The impact of SIEM dashboard customization on user perception and performance. In Proceedings of the 11th ACM Symposium on Usability of Privacy and Security (SOUPS) (pp. 1-12).