Impact of SIEM on Compliance: Achieving Security and Adherence Simultaneously

ShivaDutt Jangampeta
Vice President
JPMorgan Chase
Plano, USA
shivadutt87@gmail.com

Sai Krishna Reddy Khambam
Software Developer
Amdocs
Krishna.reddy0852@gmail.com

ABSTRACT

Security Information and Event Management (SIEM) solutions are broadly used as important tools to identify, prevent, and respond to cyber security incidents. Recently, SIEM systems have immensely advanced to become extensive solutions that provide a broad view of IT infrastructures, help IT teams spot cyber risks, and devise proactive mitigation strategies aimed at minimizing time and expenditure for incident response. Besides, SIEM addresses a vast range of regulatory requirements, like state and international regulations with which organizations must comply together with industry-specific policies and standards. As such, this review paper explains how SIEM helps businesses meet regulatory requirements and achieve compliance with industry best practices.

Keywords - Security Information and Event Management (SIEM), compliance, Regulations, policies, standards.

Introduction

Owing to the soaring trends and changes in policies, businesses are resorting to solutions that offer enterprising measures of information security. Today, organizations have to adhere to stricter guidelines for collecting, storing, and protecting customer data. As such, they are looking for contemporary solutions that can execute this accurately and cost-effectively. Security Information and Event Management (SIEM) solutions enable threat management together with a complete and centralized visibility of enterprise data security. Above all, businesses require SIEM solutions to achieve compliance with industry-specific rules and minimize security risks.

A. What's Security Information and Event Management (SIEM)?

SIEM is a technology/tool that enables businesses to obtain a synchronal analysis of security notifications. These solutions help businesses collect, match up, and examine log information from a vast range of computer systems linked to the IT architecture. Depending on the outcome, the SIEM system helps detect security threats and malicious activities.

SIEM solutions bolster the security posture of enterprises' IT systems with real-time automation, surveillance, logging, and security incident alerts. Using the SIEM software, IT teams can track incidents concerning organizations' information security, including potential security breaches, phishing attacks, or ransomware; enabling swift response.

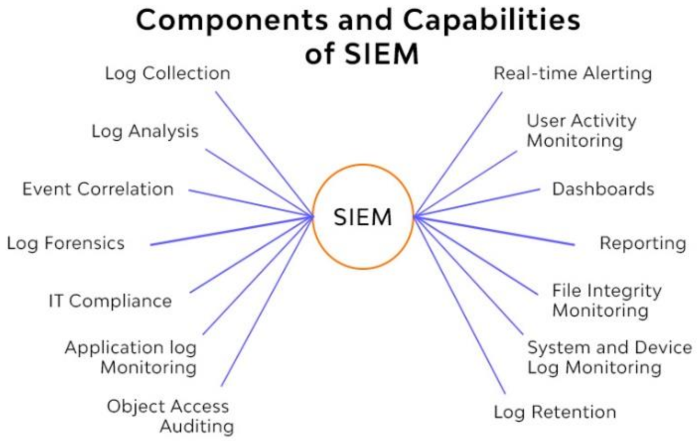

Fig. 1. Functions/capabilities of SIEM solution

B. SIEM Application in Minimizing Security Risk

Recently, security threats have become a major challenge to business continuity. As technology evolves, cybercrime has also advanced making it hard to mitigate security risks using legacy security technologies. Verizon's 2019 DBIR found that 34 percent of data breaches were caused by internal actors [1]. Besides, the detection of insider threats can take several months. Thus, using manual threat identification and response methods is no longer effective. Businesses need advanced solutions to proactively spot suspicious activities and anomalies, analyze behaviors, and respond swiftly and effectively.

Implementing SIEM solutions in a company's IT system helps significantly prevent insider threats and minimize security risks. SIEM software leverages behavioral analysis to detect abnormal user behaviors and habits and alerts security teams to respond promptly.

As technology advances and cyber threats become more complex, engineers are developing more sophisticated SIEM systems using AI, ML, and statistical analysis. These modern solutions can seamlessly reduce security risks while ensuring business organizations comply with security standards and policies. Let's see why SIEM is critical for regulatory compliance:

Importance of SIEM in Regulatory Compliance

Lately, compliance with industry-specific standards has immensely become a priority for organizations that collect, store, and handle data. Essentially, there are different compliance regulation schemes, and these requirements vary based on the field/industry in which an organization operates. Generally, compliance governs: (1) how data is collected, stored, and handled; (2) how data is transmitted/shared; and (3) how information is secured.

Businesses must invest in on security resources and practices that sometimes tend to be costly owing to the complexity and arduousness of compliance. Preventing failed compliance audits requires real-time monitoring and analysis of all data logs and reports. Whereas the main goal of SIEM solutions is to enhance threat identification and swift incident response, these technologies assist in compliance. Prerequisite actions, including threat identification, security incident tracking, and logging can easily be automated with the use of SIEM software. Additionally, SIEM generates reports issuing information on every measure that has been taken for compliance required for security audits. Let's see two examples of regulation compliance provided by SIEM solutions.

A. General Data Protection Regulation (GDPR) Compliance with SIEM solutions

The European Union's General Data Protection Regulation (GDPR) governs the processing by a person or an establishment of personal information within the EU region. GDPR's new activation started in May 2018 and has been in operation up to date [2]. Its activation sparked the significance of protecting data privacy by businesses, irrespective of the size: from small ventures to giant companies.

All companies dealing with the data of EU citizens are required to comply with the GDPR standard. Noncompliance attracts huge penalties and bad reputations. To guarantee effective GDPR controls, organizations within the EU jurisdiction should adopt contemporary solutions that enable/support monitoring, detection, response, and notification of security incidents. Configuring SIEM to detect security events proves that the business has appropriate security controls to manage EU-related data. Therefore, SIEM solutions help businesses to comply with staunch GDPR regulatory requirements through effective threat detection, file integrity monitoring, detecting and tracking unauthorized system/network access, holistic IT system analysis, monitoring international data transfers, and compliance reporting [3].

B. Payment Card Industry Data Security Standard (PCI DSS) Compliance with SIEM solutions

The PCI DSS standard constitutes security policies designed to safeguard credit and payment card information as well as related transactions. The standard provides consistent information security controls to be broadly adopted globally. Essentially, PCI DSS sets out twelve security dimensions that organizations must focus on to guarantee data security [4]. The requirements are compulsory for organizations that handle credit card data, such as banks, retailers, service providers, processors, etc.

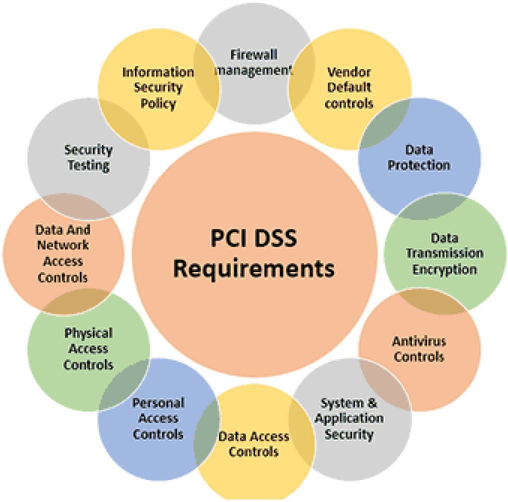

Fig. 2. The twelve PCI DSS Requirements.

SIEM solutions help monitor user activities, identify unusual traffic and suspicious activities, and issue alerts in case of any security event to guarantee PCI DSS compliance. It collects, stores, and manages information about security incidents and logs often needed for compliance regulations. Overall, SIEM helps PCI DSS compliance in five primary ways: real-time threat identification, user credentials, auditing, and reporting, generation and information systems, as well as perimeter security.

Conclusion

Businesses looking forward to investing in cybersecurity solutions that help in detecting, preventing, and responding to security threats as well as compliance with regulatory requirements should consider SIEM solutions. SIEM systems are all-inclusive, cost-effective, and fast methods of automating cybersecurity processes to guarantee users swift and accurate outcomes.

References

[1] Verizon, 2019 Data Breach Investigations Report., 2019.

[2] Paul Voigt, Axel von dem Bussche, The EU General Data Protection Regulation (GDPR) A Practical Guide, Springer International Publishing, 2017.

[3] LogPoint , SIEM: A holistic approach to compliance, 2019.

[4] Pinsent Masons, New payment card data security standards finalized:, Available at: https://www.pinsentmasons.com/out-law/news/new-payment-card-data-security-standards-finalised,2013.