The Role of Data Security in SIEM Compliance: Meeting Regulatory Requirements and Data Protection Standards

ShivaDutt Jangampeta
Global CyberSecurity Engineer
PepsiCo
Plano, USA
shivadutt87@gmail.com

Sai Krishna Reddy Khambam
Junior Software Developer
Sage IT Inc
krishna.reddy0852@gmail.com

ABSTRACT

Owing to the soaring trends and changes in policies, businesses are adopting security solutions that guarantee a proactive degree of cybersecurity. Rising concerns over information security have resulted in a corresponding rise in the number of compliance mandates across different industries. So, businesses are required to meet numerous regulatory requirements and conform to several compliance mandates. Thus considering different regulatory requirements, businesses are embracing security solutions like Security Information and Event Management (SIEM) to meet and adhere to state and industry-specific standards. This review explains in detail how SIEM solutions help organizations meet compliance and regulatory requirements.

Keywords – Security Information and Event Management (SIEM), regulatory compliance, industry-specific standards.

Introduction

Security Information and Event Management (SIEM) systems enhance the cybersecurity of an organization's computer system/network with real-time automation, analysis, surveillance, logging, correlation, threat detection, and security incident alerts [1]. SIEM solutions enable tracking of security incidents related to a business' information security, like security breaches, and help security teams respond on time to events.

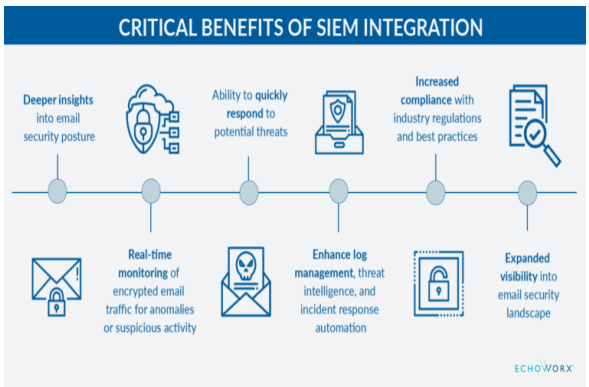

Fig. 1. Benefits of SIEM integration

Minimum Security Requirements Associated with Compliance

Cybersecurity compliance is not centralized for every single standard or industry-specific regulation since there is "no silver bullet" to accommodate all. However, there are notable minimum security requirements regarded as security best practices. So, to comply with most regulatory requirements applicable to the cybersecurity world, an enterprise should at least:

- Monitor security events critical to their business,
- Analyze data to spot data breaches,
- Based on the level of risk, single out what events are regarded as the severest threats,
- Have a well-established plan, outlining how to handle security incidents,
- Keep a register of security events, what transpired, the exact time and date, and how the event was mitigated, etc.

Most regulatory requirements and industry-specific standards mandate organizations to log security incidents and review them on time, to take appropriate measures if needed. Often, monitoring security events can be tedious, especially if it is to be done manually, due to the vast amount of data and processes. However, with SIEM solutions in place, most of the regulatory requirements can be automated to enable more accurate and faster handling. While some regulations would not need to explicitly adopt SIEM systems to achieve compliance, SIEM solutions have been established to be cost-effective and capable of covering security mandates of several regulations at the same time.

How SIEM Systems are used for Compliance and Regulatory Requirements

A. **Comprehensive view and real-time visibility into organization IT infrastructure**

One way to use SIEM systems to meet regulatory and compliance mandates is to leverage its comprehensive view and real-time visibility into an organization's IT environment. SIEM systems collect and analyze data from across the business's IT infrastructure to detect any anomaly, or potential security threats, provide an all-inclusive view of the organization's cybersecurity posture, and notify security teams of any potential security incidents. This enables swift and effective mitigation of cyber threats, patching up of existing security flaws presenting security vulnerabilities to the company's IT system, and prevention of security threats before they executed into successful attacks

B. **Compliance Reporting**

Another way to use SIEM systems to meet regulatory and compliance mandates is to leverage their capability to generate compliance logs and security event reports. The generated reports and compliance logs are used to exhibit compliance with different standards and regulations. That way, businesses can provide them as evidence that they are adhering to different standards and regulations and avoid being fined or penalized.

C. **Security monitoring and Operations**

While data privacy and security are essential requirements for any business, most industry policies and standards require organizations to ensure that they are maintained. As more businesses migrate their workflows and workloads to cloud-based data environments, the regulatory and compliance demands for their information are becoming even more critical, day by day. Businesses are required to put in place sturdier security measures to monitor network activities to ascertain their corporate and customer data is secure. SIEM tools help businesses address these security requirements to monitor and secure their data

[2]. Organizations can integrate SIEM with cloud-powered security solutions to gain a real-time and comprehensive view of their cloud data and guarantee compliance with industry standards and regulations.

D. Compliance and regulatory strategy

Another way to use SIEM systems to meet regulatory and compliance mandates is to facilitate the execution of an all-inclusive regulatory and compliance strategy. The strategy includes technical controls like access controls and data encryption; as well as procedural controls like incident response strategies and employee training. By executing these important plans, businesses will have met several regulatory mandates. Also, it will help them avoid hefty fines and penalties associated with non-compliance.

SIEM Regulatory Compliance Use Cases

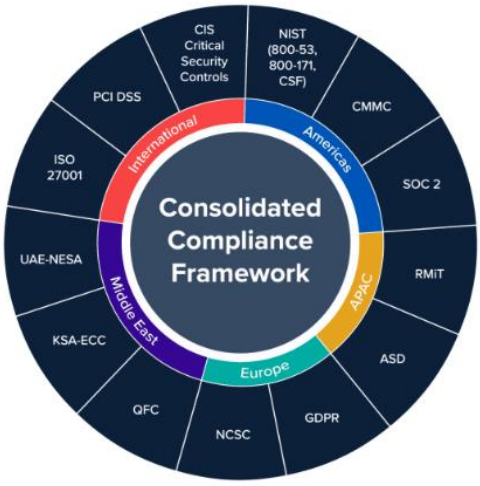

Fig. 2. SIEM compliance use cases

A. GDPR compliance:

SIEM solutions, especially Next-Gen SIEM enable businesses to achieve regulatory compliance with minimal effort.

B. Financial Compliance:

Since the financial industry is a lucrative target for cybercriminals, it is highly regulated. Thus all companies in this sector, from fintech startups to giant multinational banks must comply with several regulations/policies regarding data security, Anti-money laundering (AML), Know Your Customer (KYC), etc. SIEM systems cover all these security requirements.

C. NIS Compliance:

The Network and Information Systems Directive (NIS Directive) defines cybersecurity mandates for essential service operators. Leveraging SIEM capabilities in an organization's IT environment helps comply with most NIS Directive demands.

D. SOX Compliance:

Oftentimes, financial institutions extend audit procedures to financial data stored within their corporate databases to validate the authenticity of the financial information. To measure the level of regulatory compliance, auditors check multiple aspects like access control, user management, allocation of responsibilities, authentication, audit trails, etc. Most companies use SIEM solutions to cover all these requirements.

E. PSD2 Compliance:

Payment Services Directive Two (PSD2) is a regulation designed to compel payment service providers to enhance customer authentication procedures. To cover the demands of the PSD2 regulation, organizations should consider adopting SIEM systems.

F. EU Data Protection Regulation:

While some EU regulations offer EU citizens more privileges over private information, they also require businesses to use strong data security and privacy measures when handling people's data. Hence SIEM solutions play a critical role in complying with set regulations and policies like ISO 27001, GDPR, etc.

Conclusion

SIEM systems play an essential role in helping businesses comply with industry standards and regulations. Therefore, by leveraging SIEMs, businesses can align their security strategies with regulatory requirements.

References

[1] M. Gupta, Handbook of Research on Emerging Developments in Data Privacy, IGI Global, 2014.
[2] Adam Gordon, Steven Hernandez, The Official (ISC)2 Guide to the SSCP CBK, Wiley, 2015.