Security Information and Event Management

Loic Niragire

School of Technology, Northcentral University

TIM 7030: Managing Risk, Security, & Privacy in Information Systems

Dr. Gabe Goldstein

September 3rd, 2023

Security Information and Event Management (SIEM) systems facilitate real-time analysis of alerts generated from various hardware and software infrastructures within an organization. It provides a centralized view for monitoring, analysis, and reporting of security events by collecting and aggregating log data generated throughout an organization's technology infrastructure (Bhatt, Manadhata, & Zomlot, 2014). Therefore increasing the organization’s ability to detect and respond to threats, ensure compliance with various regulations, and improve the efficiency of security operations.

By normalizing aggregated data, SIEM systems can identify patterns and anomalies that may suggest a security threat using rule-based detection (Cinque, Cotroneo, & Pecchia, 2018). Moreover, SIEM systems can automate the collection and reporting of compliance data required by many regulatory frameworks such as PCI DSS, HIPAA, and GDPR for organizations with specific industry compliance requirements. Additionally, advanced SIEM systems, such as IBM Security QRadar, can incorporate machine learning algorithms to establish a baseline of normal behavior for users and entities within an organization (IBM, 2023). Deviation from this baseline can trigger alerts, thus providing an additional layer of security against insider threats (Mitchell & Chen, 2015).

Traditional approaches

Compared to SIEM systems, traditional solutions often lack the ability to correlate data from multiple sources and require manual interventions. Therefore, SIEM systems are often used in conjunction with traditional methods as part of a layered security strategy (Ghorbani, Lu, & Tavallaee, 2009). Table 1 lists prominent network security monitoring approaches and their limitations.

The effectiveness of a layered security strategy depends not just on the individual components but also on how well they are integrated. SIEM systems can serve as the glue that binds these layers together, offering a centralized platform for monitoring, analysis, and response (Wheeler, 2011)

Table 1. Traditional network security monitoring and incident response methods

Method	Description	Limitations
Log file monitoring	Monitoring of log files generated by servers, firewalls, and other network devices. Manual or automated	Lacks real-time alerting and correlation capabilities.
Intrusion Detection Systems (IDS)	Monitors network traffic for suspicious activity and known threats, generating alerts when such activity is detected.	Detects known signatures and patterns, may generate false positives and negatives.
Intrusion prevention Systems (IPS)	An extension of IDS that not only detects but also prevents known malicious activities.	Limited to known signatures and can be bypassed by zero-day attacks.
Firewalls	Filters incoming and outgoing network traffic based on an organization's previously established security policies.	Cannot detect or prevent attacks that do not violate predefined rules.
Antivirus Software	Scans files and system memory for known malicious patterns.	Primarily effective against known malware and often ineffective against new or modified malware variants.
Security Policy and Procedures	Written guidelines and procedures aimed at governing how organizational IT resources should be used and protected.	Human error, lack of compliance, and outdated policies can render them ineffective.
Vulnerability Scanners	Automated tools that scan systems for known vulnerabilities.	Cannot detect zero-day vulnerabilities or complex attack vectors that require a multi-step exploitation process.

Pocket Sniffers	Tools that capture and analyze network packets.	Useful for analysis but do not offer real-time protection or alerting capabilities.
Honey Pots	Decoy systems designed to lure attackers, allowing organizations to study their methods.	Does not offer protection for actual network and can be identified and avoided by sophisticated attackers.

Splunk and SIEM primarily serve different purposes and offer distinct capabilities. Splunk was initially designed for searching, monitoring, and analyzing machine-generated big data. It provides a highly scalable and performant solution, capable of efficiently handling large volumes of data. Moreover, it offers data ingestion flexibility and allows custom-defined alerting rules using machine learning (Diakum, Johnson, & Derek, 2018). However, it requires additional customization and configuration for security use cases. On the other hand, SIEM systems are purpose-built for security monitoring but may lack Splunk's scalability and broader analytics capabilities. Hence, organizations often use Splunk in conjunction with a SIEM system.

Data acquisition

Continuous network security monitoring involves collecting data from various sources such as mail logs, mobile device records, web traffic, and operating system logs. Devices running protocols designed specifically for network monitoring, such as the Simple Network Management Protocol (SNMP), provide another source of logs. Data collected from SNMP include intrusion detection/prevention system alerts, firewall alerts and logs, and real-time network monitoring (Detken, Rix, & Hellman, 2015). Operating systems also store log files containing specific event information, often called audit logs. Table 2 lists a sample of typical logs encountered in a networked environment and their content.

Table 2. Sample of logs encountered in a networked environment.

Log types	Description	Data captured
Network logs	Records generated by networking hardware devices of software applications.	Traffic data, connection details, security events, system events, error messages, and performance metrics.
System logs	Records that capture events and activities occurring within an operating system or software application chronologically.	Boot and shutdown events, system errors and warnings, security events, resource utilization, configuration changes, service and process events, timestamps.
Application logs	A subset of system logs dedicated to software application events.	Error messages, debug information, performance metrics, and security events.
Security logs	A subset of system logs dedicated to system components and software application for security related events.	Authorization events, network security events, data access and transfer, configuration changes, and security incidents.
Kernel logs	Records that capture events and activities related to the operating system kernel.	System boot and shutdown, hardware events, system errors, resource allocation, security events, and driver activities.
Audit logs	Records that capture sequence of activities or changes that affect a system, application, or data. They provide an auditable trail of events for the purpose of accountability, compliance, and security monitoring.	User activities, system events, data access and modifications, security events, transaction logs, and timestamps.
DNS log	Records that capture queries, responses, and other activities related to DNS operations.	Query information, response information, server details, timestamps, and protocol details.
Authentication log	A subset of security logs that capture events related to the authentication process in a system, application, or network.	User identification, source information, timestamps, authentication method, authentication status, session details.

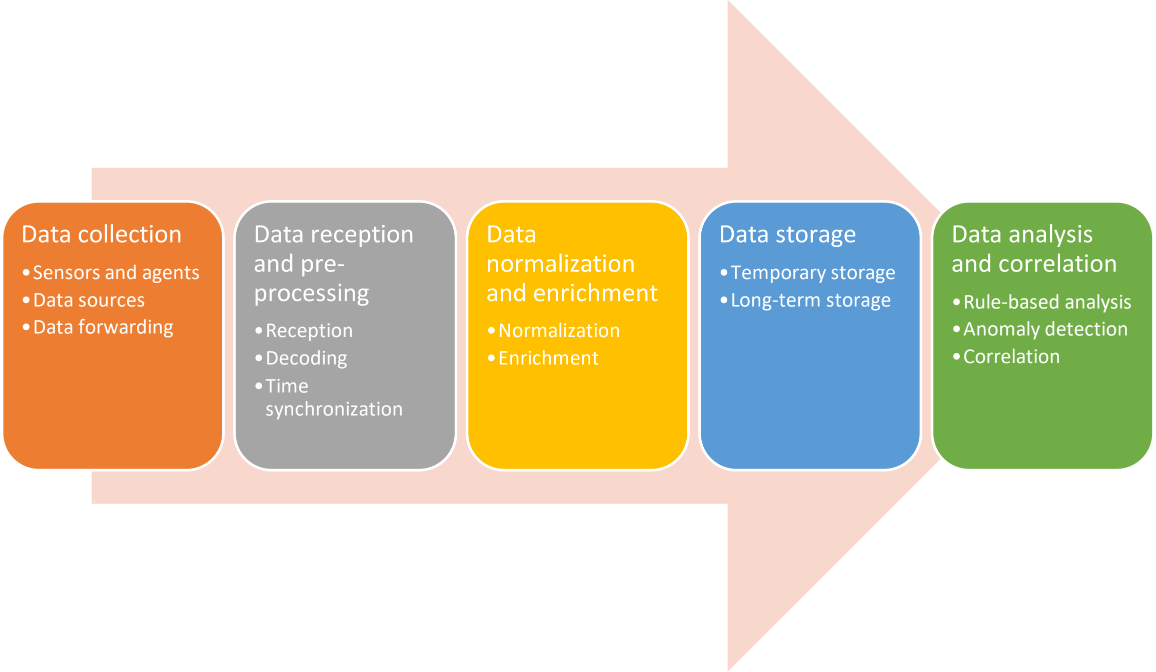
Dump files	Records that store the captured state of a program, system, or specific data structures at a particular point in time. They are often generated automatically when a software application or operating system encounters an error condition such as a crash.	Core dumps, heap dumps, thread dumps, system dumps, mini dumps.
Session Initial Protocol (SIP) traffic logs	Records that capture events and transactions related to SIP-based communications. SIP is a signaling protocol used for initiating, maintaining, and terminating real-time multimedia sessions, such as voice, video, and messaging applications.	Request and response messages, transaction details, timestamps, endpoint information, media attributes, error messages.
Event Viewer logs	Log files that store events displayed in the Event Viewer interface on Windows.	Application logs, security logs, system logs, setup logs, forwarded events, application, and services logs.
Syslog logs	Log files that store the messages collected via Syslog protocol on Unix-like systems.	Timestamps, hostname or IP address, facility, severity level, message content
Device logs	Records that capture events, transactions, and operational data generated by hardware devices such as routers, switches, and IoT devices.	Operational events, network activities, security events, error messages, resource utilization, timestamps.

Integration of knowledge bases and automation

SIEM is an integrated approach to monitoring networks based on log data. A typical SIEM system comprises five components: sensors/collectors, servers, analyzers, and a dashboard. Sensor devices facilitate data input by acquiring raw data about the network. Data from sensors is then aggregated and stored on an SIEM server for further processing. Using a myriad of tools, analyzers sift through the data on the server, trying to locate signatures of something that an organization would consider an incident (Arass & Souissi). Then, the results are presented in an SIEM dashboard.

Sensors forward collected data to the SIEM server using protocols like Syslog, SNMP, or custom APIs. This data may be encoded and/or encrypted. Upon receipt, the SIEM server decodes and encrypts sensor data and aligns log entries based on timestamps to ensure chronological accuracy. The normalization step attempts to convert disparate log formats into a common, standardized format. Then metadata or additional context is added to the log entries to make them more informative. The normalized and enriched data is stored depending on the analysis being performed. For real-time analysis, data is temporarily stored in high-speed storage. Whereas for compliance and historical analysis, data is archived in long-term storage solutions, often with data retention policies in place (Meyers & Jernigan, 2021). Lastly, the data analysis step applies pre-defined rules to incoming data to identify known malicious or suspicious activity patterns using statistical models or machine learning algorithms. Figure 1 illustrates how data flows from sensors to the SIEM server and the steps involved in this process.

Figure 1. Data flow from sensors to SIEM server



Automation is crucial in the abovementioned process to increase efficiency, reduce manual overhead, and improve response times. For instance, automation scripts and configuration management tools are used to set up log forwarding from multiple devices to the SIEM system to ensure that new sensors are automatically integrated into the process. Likewise, custom parsers can be automatically applied to incoming data streams to transform them into a standardized format. Other areas dominated by automation include reporting, trend analysis, configuration drift monitoring, and real-time dashboard updates.

Routine tasks can be automated for more effective incident response without human assistance, using a Security Orchestration, Automation, and Response (SOAR) framework. SOAR compliments SIEM systems by automating follow-up actions. For instance, given a security event identified by an SIEM system, a SOAR platform focuses on automating the actions that should be taken in response. SIEM provides the data and analytics capabilities, and SOAR provides the action and automation capabilities, therefore reducing the time required to detect and respond to security incidents. Hence, Security Operations Centers (SOCs) can handle large volumes of alerts and incidents without proportionally increasing staff size.

Specification of Appropriate Provision of Information

A critical aspect of SIEM configuration and operation involves defining the types of data that should be collected, how they should be processed, and what kinds of insights or interpretations should be delivered from that data. This section specifies appropriate information provision in the context of the "ABC Financials" organization described in prior work. As a recap, ABC Financials is a software organization that handles recurrent customer payments through various payment methods such as credit cards, ACH, digital currency, and more. Moreover, the organization maintains a hybrid infrastructure with resources running on-prem and AWS.

Data Sources and Formats.

On-Prem infrastructure.

- *Firewall logs*: Capture all inbound and outbound traffic logs.
- *Server logs*: Include logs from all servers involved in payment processing.
- *Database logs*: Transaction, access, and change logs from databases storing payment information.
- *Application logs*: Logs for custom-built payment processing software.
- *Format*: Syslog for network devices, JSON, or XML for application logs

AWS infrastructure.

- *CloudTrail logs*: For monitoring API calls and other activities.
- *VPC flow logs*: For network traffic monitoring.

- *S3 access logs*: For any S3 buckets used in payment processing.
- *Lambda logs*: For lambda executed during the payment processing.
- *Format*: AWS-specific formats, converted to a JSON.

Payment Processing Systems.

- *Transaction logs*: Detailed logs of all payment transactions, including timestamps, amounts, and anonymized customer identifiers.
- *Error logs*: Logs of failed transactions or system errors.
- *Format***:** JSON

Data Granularity and Retention.

Granularity.

- *High-Granularity*: For payment transaction logs, database access logs, and application error logs.
- *Medium-Granularity*: For server and network logs.

Retention.

- *Short-Term*: High-granularity logs are retained for 30 to 90 days of operational use.
- *Long-Term*: Medium-granularity logs are retained for up to a year or more for compliance (e.g., PCI DSS) and auditing.

Interpretations.

Alerts and Correlation Rules.

- *Unauthorized access*: Multiple failed login attempts and unusual access patterns.
- *Data exfiltration***:** Unusual data transfer sizes or destinations.
- *Transaction anomalies*: Unusual large transactions or rapid sequence of transactions.

Contextual Enrichment.

- *Geolocation*: Add geolocation data to IP addresses.
- *User mapping*: Map user IDs to actual names or roles for internal users.

Threat Intelligence Integration.

- Integrate with threat intelligence feeds to identify known malicious IPs or URLs.

Reporting and Dashboards.

- *Compliance reports*: Regular PCI DSS compliance reports.
- *Incident reports*: Details reports for each security incident, including root cause analysis and remediation steps.

SIEM-SOAR Integration Points.

Alert enrichment and escalation.

- Define rules for which SIEM alerts should automatically escalate to the SOAR platform for further action.
- Specify the additional context or threat intelligence the SOAR platform should add to these alerts.

Automated workflows.

- Detail the automated workflows (or playbooks) that the SOAR platform should execute in response to specific types of SIEM alerts.
- For example, if the SIEM detects a potential data breach, the SOAR platform could automatically isolate the affected system and initiate a predefined incident response workflow.

Data synchronization.

- Specify how and when the SOAR platform should update the SIEM system with information about actions taken, incident statuses, and other relevant data.
- This could include updating the SIEM with new indicators of compromise (IoCs) discovered during the incident response process.

A comprehensive real-time network security monitoring strategy shortens the cycle from threat detection to threat response, allowing the organization to remain compliant with industry regulations. SIEM systems play a major role in achieving such a monitoring strategy (González-Granadillo, González-Zarzora, & Diaz, 2021). They are exceptionally great at collecting and aggregating log data from various sources within an organization's infrastructure. More importantly, SIEM systems integrate seamlessly with other industry-established tools and systems like Splunk, providing a complete solution. Automation capability is another major factor in network security as it allows an organization to handle a high volume of log data and respond rapidly to security incidents. To this end, organizations can leverage a Security Orchestration, Automation, and Response (SOAR) framework to automate responses based on SIEM's analysis outcome. However, SIEM systems are not without limitations. They require extensive configuration to tailor them to an organization's specific needs. Thus, their complexity and associated operational overhead necessitate specialized personnel to manage the SIEM, which can be a significant cost factor.

References

Arass, M. E., & Souissi, N. (n.d.). Smart SIEM: From Big Data logs and events to Smart Data alerts. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* (pp. 3186-3191). Blue Eyes Intelligence Engineering & Sciences.

Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy, vol. 12, no. 5*, 35-41, doi: 10.1109/MSP.2014.103.

Cinque, M., Cotroneo, D., & Pecchia, A. (2018). Challenges and Directions in Security Information and Event Management. *IEEE International Symposium on Software Reliability Engineering Workshops*, 95-99, doi: 10.1109/ISSREW.2018.00-24.

Detken, K.-O., Rix, T., & Hellman, B. (2015). SIEM approach for a higher level of IT security in enterprise networks. *IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)* (pp. 322-327, doi: 10.1109/IDAACS.2015.7340752.). Warsaw, Poland: IEEE.

Diakum, J., Johnson, P. R., & Derek, M. (2018). *Splunk Operational Intelligence.* Packt Publishing; 3rd Revised edition.

Ghorbani, A. A., Lu, W., & Tavallaee, M. (2009). Network Intrusion Detection and Prevention - Concepts and Techniques. In *Advances in Information Security.*

González-Granadillo, G., González-Zarzora, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. *Sensors (ISSN 1424-8220)*, https://doi.org/10.3390/s21144759.

IBM. (2023, August 25). *IBM Security QRadar Suite.* Retrieved from ibm.com: https://www.ibm.com/qradar?utm_content=SRCWW&p1=Search&p4=43700074604556106&p5=e&gclsrc=aw.ds&gclid=EAIaIQobChMI76rF6t7FgQMVkt_ICh0h5AY-EAAYASAAEgJpu_D_BwE

Meyers, M., & Jernigan, S. (2021). *Mike Meyers' CompTIA Security+ Certification Guide.* McGraw Hill.

Mitchell, R., & Chen, I.-R. (2015). Behavior Rule Specification-Based Intrusion Detection for Safety Critical Medical Cyber Physical Systems. *IEEE Transactions on Dependable and Secure Computing Vol. 12*, 16-30.

Wheeler, E. (2011). *Security Risk Management: Building an Information Security Risk Management Program from the Ground Up.* Elsevier.