A Framework for SIEM Implementation

In 1996, a group set out to climb Mount Everest. They had all the right equipment, and they were well trained and fit, but on Everest there is a rule: If climbers do not reach the summit by a certain time of the day, they must abandon the attempt. This day, there was a traffic jam of sorts as four different expeditions all attempted to reach the summit, and these climbers did not reach the summit by the specified time. At this point, they should have turned around, but they did not. They reached the summit too late and had to climb down in the darkness and were caught unprepared by an unexpected storm. Sadly, they all died during the attempt.[1]

> The true value of SIEM is often not realized due to poor implementation and lack of a purpose-driven event-logging approach.

This tragedy offers a valuable lesson for security teams. They commit to a three-year plan or an 18-month road map, and then, as time passes, the business context changes, the threat landscape evolves and evidence starts to emerge that the current strategy is a bad idea. At that point, the team should stop, reevaluate and readjust the strategy. But it is often difficult to admit that mistakes have been made, so security leaders may continue heading in the wrong direction. However, if it becomes apparent that a security information and event management (SIEM) solution has been implemented incorrectly, for example, it is the security team's responsibility to rectify it.

In its simplest form, a SIEM solution consumes information in the format of event logs from many different source systems and provides a consolidated view of security activities within an enterprise. Depending on the vendor, SIEM may incorporate a level of machine learning (ML), artificial intelligence (AI) or both. In addition, industry regulations often mandate the implementation of log correlation solutions to achieve and maintain compliance.

In theory, SIEM should provide valuable insights for security teams and enable more efficient and effective incident response activities. However, the true value of SIEM is often not realized due to poor implementation and lack of a purpose-driven event-logging approach.

The proposed framework provides guidance on implementing SIEM technologies in a structured and pragmatic manner to ensure maximum value from investments in SIEM. Event logging is emphasized, as it is a prerequisite for SIEM.

Approaches to Security Event Logging

There are three types of approaches to event logging:

1. **Leave it on default and hope for the best**—This approach is dangerous and will certainly result in blind spots that SIEM cannot address.
2. **Log it all and let the analyst sort it out**—This approach is costly and results in storage

GRANT HUGHES | CISA, CISM, CDPSE, CCSP, CEH, CISSP

Is principal security architect at Engen Oil in South Africa. He has more than 12 years of IT experience and a background in security strategy, architecture, cybersecurity risk and security operations. He can be contacted on LinkedIn at *https://www.linkedin.com/in/grant-hughes-52196569/.*

challenges, frustrated security operations center (SOC) analysts or excessive costs for cloud-based solutions.

3. **Purpose-driven logging**—Although it is not the easiest, this is the ideal approach. It requires planning; defining use cases and playbooks up front; and supporting event logs to be identified, enabled on log sources and incorporated into the SIEM solution. This is the only approach that realizes the full value of SIEM.

Despite the value of security event logging and monitoring, it is one of the most overlooked areas of security.

Regulations and Industry Standards

Despite the value of security event logging and monitoring, it is one of the most overlooked areas of security. As a result, an increasing number of regulations address event-logging requirements. The most common recommendations related to event logging include:

- The US National Institute of Standards and Technology (NIST) released Special Publication (SP) 800-92 *Guide to Computer Security Log Management*, which asserts that past incidents highlight the importance of generating, safeguarding and retaining logs of system and network events, both to improve incident detection and to aid in incident response and recovery activities.[2]
- The Center for Internet Security (CIS) Critical Security Control Version 8 recommends that enterprises establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, the strategy should address collecting, alerting, reviewing and retaining audit logs and events that can help detect, investigate, respond to and recover from a cyberattack.[3]
- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) standard ISO/ IEC 27001 covers logging and monitoring. The standard is for event logs to be produced, retained and regularly reviewed to record user activities, exceptions, defects and other anomalies. The objective is to record events and generate evidence for future investigations.[4]
- The Payment Card Industry Data Security Standard (PCI DSS) 4.0 provides extensive requirements and guidelines for system logging and monitoring, which are critical aspects of security that can provide incident responders with the information required to detect and investigate events.[5]
- The Open Web Application Security Project (OWASP) Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security threats to web applications. In 2021, security logging and monitoring failures was listed as number nine on the OWASP Top 10.[6]

The number of regulations illustrates the importance of event logging and monitoring. These are pivotal security functions that warrant the right level of attention and investment, as SIEM and other capabilities are dependent on them.

Analysis of Requirements

Before implementing SIEM, both current and future requirements must be identified. Is the enterprise looking for new security insights? Is it seeking compliance only? These requirements will ultimately drive the SIEM deployment strategy. Approaches can vary significantly in terms of cost. The enterprise should answer these questions:

- What risk factors might go undetected if there is no SIEM?
- What regulatory implications might the enterprise face if there is no SIEM?

Common Challenges

Some of the most mentioned SIEM challenges include:

- Excessive number of security alerts
- High number of false positives
- Shortage of skills to maintain and use the technology
- Event-logging gaps (e.g., no logging, insufficient verbosity level, insufficient retention)

There are many more challenges, but the main problem is that SIEM is not delivering on its promise to provide a consolidated view of meaningful security

LOOKING FOR MORE?

- Read *Defending Data Smartly. www.isaca.org/defending-data-smartly*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

events and incidents within an enterprise. When evaluating the root causes of these challenges, it is clear that most of them can be attributed to a lack of planning, limited or no involvement of skilled resources, and failure to identify use cases and supporting event logs up front.

Definition of Terms

The meaning of the phrase "implementing SIEM" must be clearly defined in terms of activities and outcomes, and this definition needs to be supported by a detailed responsible, accountable, consulted and informed (RACI) matrix. If left undefined, unmet expectations and poor implementation are likely. For example, consider the phrase "defining use cases." This could mean providing a list of use cases, or it could mean implementing logic rules with email alerts. SIEM deployment is riddled with phrases that can have different meanings; thus, establishing a common language is essential.

Technologies such as SOAR are considered a force multiplier when used in combination with SIEM.

SIEM Governance

Mature organizations often adopt an IT service management (ITSM) framework that governs various processes. The IT Infrastructure Library (ITIL), which covers processes such as change and incident management, is an example of a widely adopted ITSM framework.[7] It is important to align SIEM with the organization's incident and change procedures. For example, if the organization needs to implement a new SIEM dashboard, either a service request or a minor change may need to be logged, as defined in the organization's ITSM framework. There are many activities associated with managing a SIEM, and failing to manage these activities can inadvertently introduce risk to the organization, impact the performance of log sources or impact the effectiveness of the SIEM as a security control. Therefore, it is also important to consider the existing governance structure of the organization. Common types of SIEM activities and how they might be recorded in the ITSM system are shown in **figure 1**.

FIGURE 1

Recording SIEM Activities

Activity	Record
Upgrading the version	Significant or planned change
Adding a new dashboard	Service request
Adding a new email alert	Standard change
Adding a new threat intelligence source	Standard change
Integrating SIEM with a SOAR solution	Significant or planned change
Allow listing host or users from triggering specific use cases	Standard change

When defining a support model for a SIEM solution, it is vital to consider factors such as:

- Size of the team
- Skill level of the team
- On-premises vs. cloud deployment model
- In-house vs. outsourced

Expecting cyberincident responders to manage and maintain a SIEM platform is a recipe for disaster. It is the equivalent of expecting a bus driver to also be a bus mechanic. Individuals are generally one or the other; they are rarely both. Similarly, cyberincident responders should focus on cybersecurity anomalies and response activities, while infrastructure engineers should be concerned with the operation, maintenance and upgrade of the tools. A detailed responsible, accountable, consulted and informed (RACI) matrix must be documented and shared with all key stakeholders. Support agreements must be considered and aligned with internal service-level agreements (SLAs).

Training is another key to success, and it is guided by the support model. Training consists of two core considerations:

1. Operation, maintenance and upgrading of the SIEM solution in terms of hardware, software and operating system
2. Use of the SIEM application

SIEM and SOAR

Whether enterprises want to admit it or not, they are in a race with bad actors. Within 15 minutes of the disclosure of common vulnerabilities and exposures (CVE), attackers are scanning for them. Common

challenges encountered by SOCs include complexity, an overload of alerts and events and duplication of tools. Automation promises to solve some of these challenges, and security orchestration, automation and response (SOAR) is viewed as the means to accomplish this.

Technologies such as SOAR are considered a force multiplier when used in combination with SIEM. SOAR technologies are adopted to improve detection and response by adding context and enrichment; this improves downstream prioritization and efficiency in a SOC. SOAR is used primarily for incident response, and vendors are increasingly building SOAR capabilities into other security tools such as SIEM solutions.

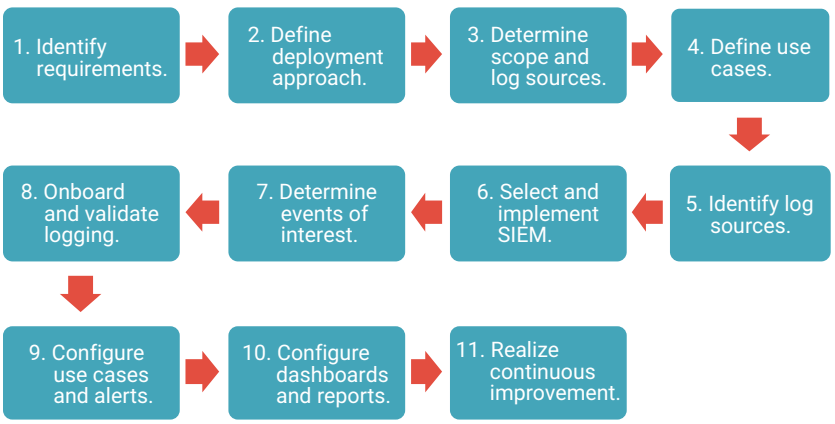
SIEM Implementation Framework

The proposed framework (**figure 2**) illustrates how to implement SIEM in a manner that guarantees value for the enterprise.

1. **Identify regulatory and business requirements**—Depending on where an enterprise is located or conducts business, there may be certain limitations that impact its selection of SIEM providers. Likewise, an enterprise may be prohibited from conducting business with certain other enterprises for political reasons.
2. **Define the deployment approach**—An enterprise may choose to include all systems in SIEM or follow a risk-based approach and target only critical business systems or IT infrastructure. It is important to complete a proper risk analysis and a cost-benefit analysis at this stage to drive the final decision. It rarely makes economic sense to onboard all logs without applying a risk-based methodology.

FIGURE 2

SIEM Implementation Framework



3. **Determine the scope of assets and log sources**—Once the regulatory requirements and the approach have been confirmed, it is possible to identify the scope of systems to be incorporated into SIEM. It is important to note that one system may have multiple components, such as a front end and a database. Furthermore, the database may be hosted on a cluster. The system must be identified in its entirety.
4. **Define use cases**—Use case definition is essentially where the value of SIEM is either obtained or lost. This requires time, research and expertise. Certain industry standards or regulations may be prescriptive in terms of which use cases must be covered. Most SIEM technologies come with a library of built-in use cases. Some systems, such as Microsoft Active Directory, document multiple use cases that are freely available on the Internet for consideration.[8] SIEM technologies may have limitations in this regard, so this step is critical.
5. **Identify log sources**—In this step, the actual source devices are identified to support the defined use cases. To address a use case related to phishing emails, for example, email gateways, network firewalls and exchange servers would be identified as possible source systems. In addition, identifying the source systems provides input into the SIEM selection process; some log sources may require an agent, while others might involve a configuration update or a third-party utility at additional cost. This step builds on step three, but it is more detailed and focuses on device, model and version levels. Having a list of source systems before making a purchasing decision is vital.
6. **Select and implement SIEM**—The scope of systems and the use cases are critical parts of the request for information (RFI), request for proposal (RFP) and, ultimately, selection of the SIEM technology or service provider. If a solution is chosen before the requirements are understood and the scope is known, the enterprise may have to purchase third-party utilities. The biggest risk is purchasing a SIEM solution that does not meet the enterprise's needs. This step includes both the purchase and the installation of SIEM technology.
7. **Determine events of interest**—In this step, it is important to validate that the appropriate level of event logging is enabled in source systems to support the defined use cases. For example,

consider a use-case monitoring logon failure: To support this, event logging for Event-ID 4325 must be enabled. Similarly, devices such as firewalls provide a granular level of specific event selection. This is often a balancing act, as too much logging can affect the performance of the source device and fill disk space, while too little logging can result in key information not being logged. A risk analysis of missing vs. required events of interest must be undertaken and understood by all stakeholders as this may severely affect the ultimate value of the SIEM investment, regardless of SIEM capabilities. This step is internal to the enterprise and can occur after SIEM is implemented. It may be initialized after step five but cannot be delayed beyond this point in the process.

8. **Onboard and validate logging**—This step includes performing the technical onboarding procedure and confirming that all events are received and parsed correctly. Most SIEM vendors assist with parsing and validation; it is most important to ensure that the required events are being sent to and received by the SIEM system.
9. **Configure use cases and alerts**—At this point, alerts are configured based on identified use cases. This step is completed only after all required use cases are triggered on a test endpoint and result in a SIEM alert. Ideally, a dedicated email account should receive SIEM alerts, with a defined process for dealing with them.
10. **Configure dashboards and reports**—Depending on the enterprise's requirements, visualizations or dashboards and reports may be required. If so, they should be identified during the requirements analysis phase and provided as input into the SIEM selection decision.
11. **Realize continuous improvement**—Alerts should always provide valuable and actionable information. If alerts do not add value, they should be reviewed and improved or disabled. The number of false positives must be closely tracked and addressed until the SIEM system is providing a high percentage of true positives.

Health Monitoring

Health monitoring is critical because even a perfectly implemented SIEM system is of no value if it stops working. To assess SIEM health, the enterprise must ensure the SIEM system is functional and that all documented log sources are sending logs as expected.

Whichever platform is ultimately used to centralize log data, it should incorporate a threat intelligence feed for enrichment and context.

Key considerations include health alerts, thresholds and the extent of manual health checks compared with automated health checks. Health monitoring is an important part of the SIEM implementation process, and it should be given the time and attention it deserves; otherwise, the consequences could be costly in the long run.

Documentation

SIEM implementation needs to be well documented. The RACI matrix should clearly state who is responsible for which documents. Documentation of SIEM deployment should include:

- Implementation guide
- Configuration document
- Disaster recovery plan
- Support model
- Incident response procedures (playbook)
- Reference architecture
- Operational guidelines
- Reporting catalog
- List of log sources (including enabled events)
- Use cases (configured and planned)

Integrating SIEM With Threat Intelligence

Previously, security teams missed threats because the technology and telemetry were not available to support detection efforts. Now, security teams miss threats because too many events and alerts are being triggered by security devices. Threat intelligence helps security analysts focus on what is important. Automating the use of threat intelligence in a SIEM system or any other security solution used by the SOC provides a significant benefit as it enables security solutions to automatically prioritize events associated with actively exploited vulnerabilities that may impact the enterprise. Whichever platform is ultimately used to centralize log data, it should incorporate a threat intelligence feed for enrichment and context.

Normalizing and Parsing Logs

When logged correctly, high-fidelity prioritized incidents can be presented to security analysts with supporting attributes such as indicators of compromise, signatures, an event timeline, other impacted systems and users, and attack stage progression based on the MITRE ATT&CK framework. One critical component is normalizing and parsing events. Consider the example of the user field. Different systems log this field differently, and if it is not being parsed and normalized correctly, context will be missed, detection rules will fail to alert and the timelines will be incomplete. Some common examples of the user field include User, Usr, Uname, Src_usr, Dst_user, User_name, Sys_created_by, and Sys_updated_by.

Conclusion

According to the IBM *Cost of a Data Breach 2022* report, organizations with fully deployed security AI and automation solutions took an average of 181 days to identify a data breach.[9] This is unacceptable. Mandiant, a subsidiary of Google, published a report called *The Defender's Advantage*,[10] which is based on the notion that organizations defending against attacks in their own environment should provide a fundamental advantage because they have full control over the entire landscape where they meet their adversaries. Sadly, organizations are not capitalizing on this advantage.

One of the fundamental reasons organizations are struggling to capitalize on this advantage and, as a result, are failing to adequately protect themselves is faulty SIEM implementation. Deploying the right tools is only half the battle. Implementing the tools correctly, testing control effectiveness and ensuring support processes and skilled resources are available to use the tools is the other half.

Author's Note

None of the content herein represents the view of the author's current employer or any former employers. It is based on his personal experience and independent research.

Endnotes

1 History, "Eight Climbers Die on Mt. Everest," *https://www.history.com/this-day-in-history/death-on-mount-everest*

2 Kent, K.; M. Souppaya; National Institute of Standards and Technology (NIST) Special Publication (SP) 800-92 *Guide to Computer Security Log Management*, USA, September 2006, *https://csrc.nist.gov/publications/detail/sp/800-92/final*

3 Center for Internet Security (CIS) Critical Security Controls Version 8, USA, *https://www.cisecurity.org/controls/v8*

4 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27001, Switzerland, *https://www.iso.org/isoiec-27001-information-security.html*

5 Payment Card Industry (PCI) Security Standards Council, *PCI Data Security Standard (DSS) Quick Reference Guide*, USA, July 2018, *https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf*

6 Open Web Application Security Project (OWASP), "OWASP Top 10," USA, 2021, *https://owasp.org/www-project-top-ten/*

7 BMC Software, "ITIL Change Management Basics," 22 December 2016, *https://www.bmc.com/blogs/itil-change-management/*

8 Microsoft, "Visualize Collected Data," 24 November 2022, *https://learn.microsoft.com/en-us/azure/sentinel/get-visibility*

9 IBM, *Cost of a Data Breach 2022*, USA, 2022, *https://www.ibm.com/reports/data-breach*

10 Mandiant, *The Defender's Advantage: Executive Summary*, USA, *https://experience.mandiant.com/defenders-advantage-landing-page/p/1*