

Detailed report on Security tool - Security Information and Event Management (SIEM)

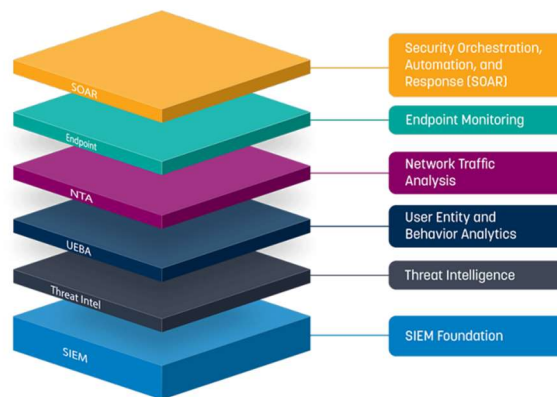
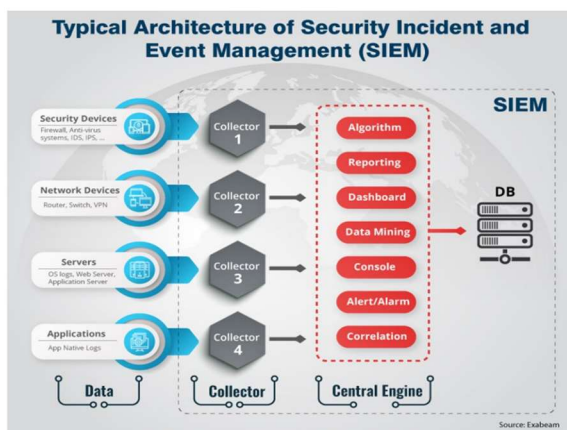
Security Information and Event Management (SIEM)

Abstract -

Security Information and Event Management (SIEM) systems have been widely deployed as a powerful tool to prevent, detect, and react against cyber-attacks. SIEM solutions have evolved to become comprehensive systems that provide a wide visibility to identify areas of high risks and proactively focus on mitigation strategies aiming at reducing costs and time for incident response. Currently, SIEM systems and related solutions are slowly converging with big data analytics tools.

Introduction-

Security analysts rely on the help of a SIEM that will correlate logs and reliably identify any suspicious activities within their infrastructure, so that they may respond against any threats or attacks immediately. A SIEM is the combination of Security Information Management (SIM) - the collection of log data, events; and Security Event Management (SEM) - real-time monitoring and alerts. SIEMs have become a core component of any Security Operations Center (SOC), but traditional SIEMs that were primarily designed as log collectors and central alert repositories that do not take any action on events are being left behind. With an increasing number of cyberattacks happening, companies created “advanced SIEM systems that have evolved to include user and entity behaviour analytics (UEBA) and security orchestration, automation and response (SOAR).



Why SIEM-

Without the help of a SIEM, the amount of time that security analysts will need to reliably identify suspicious activities by correlating logs between different types of devices would be astronomical given the complexity of most networks. It is rare to detect and respond to any threat or attack against their infrastructures in time to prevent any damage. Furthermore, the SIEM solution can expand the ability to use the information that has been collected. For instance, the help desk staff can generate a “failed authentication” report for a user whose account is being locked out. Without a SIEM, the help desk would have had to make a request to a system administrator who would have to manually search through logs for failed authentication events. This type of query-based report generation can be used to improve security, monitor capacity, and resolve technical problems.

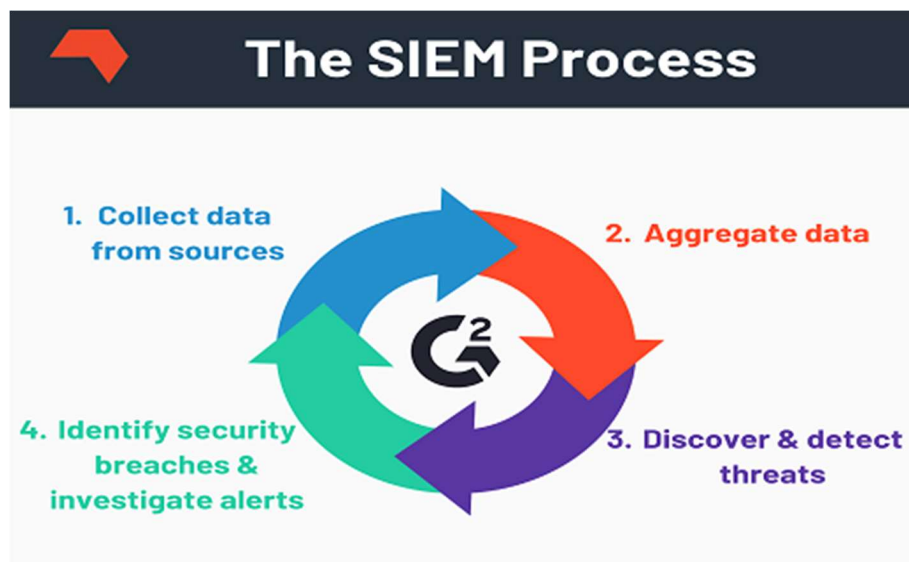
Benefits of SIEM solutions include:

- Increased efficiency of a security team and better utilization of man-hours.
- Preventing potential security threats from becoming large-scale security incident.
- Reducing overall security expenditures for an organization.
- Providing a better system for reporting, log analysis, and data retention.
- Minimizing the impact of security breaches.

How does a SIEM work?










A SIEM solution collects logs and events data from various components of an enterprise network. After normalizing the data, it uses threat intelligence, inbuilt rules, and advanced analytical functions to detect security incidents real-time. Depending on its architecture, it arranges alerts into various categories such as malware, failed logins, successful logins, other potentially harmful activity, etc. It combines two technologies: Security Information Management (SIM) and Security Event Management (SEM). In modern SIEM solutions, it is difficult to separate the two components. SIM primarily looks after data collection from log sources and generates the desired reports. On the other hand, SEM performs real-time monitoring of enterprise systems for threat detection and event correlation.

When a SIEM solution identifies a potential threat, it generates alerts to notify the security team. Based on pre-defined rules, the priority of an alert can be low, medium, or high. For example, if the user account of user X generates ten login attempts in five minutes, that can be considered as suspicious activity. Most likely, however, user X has forgotten their password and is unable to login. Suppose the same user account experiences 200 login attempts in the same duration. In that case, the SIEM solution will tag this activity as a high severity incident since it can be a brute-force attack.



10 Best Free and Open-Source SIEM Tools

What You Need to Know

| | | |
|---------------|---|---|
| OSSIM |  | Offers both server-agent and serverless modes, with log analysis for mail servers, databases, and more. |
| Sagan |  | Real-time log analysis and correlation tool that's compatible with graphic consoles like Snorby and EveBox. |
| Splunk Free |  | Free version of Splunk tool that lets you index up to 500 MB daily for real-time data indexing and alerts. |
| Snort |  | Analyzes network traffic in real time, but features make it best-suited for experienced IT professionals. |
| Elasticsearch |  | Combine log search types and easily scan through large volumes of logs with this basic tool. |
| MozDef |  | A microservices-based tool that can integrate with third-party platforms for straightforward security insights. |
| ELK Stack |  | Combines Elasticsearch with tools like Kibana, Beats, and Logstash, for a fuller SIEM solution. |
| Wazuh |  | An on-premises tool that offers threat detection, incident response, and compliance support. |
| Apache Metron |  | Combines security operations center functions into one centralized, dynamic tool for catching threats. |

Tools and features involved in a SIEM solution

1. Log Data Management

Collection of log data is the foundation of Security Information and Event Management. Real-time data collection, analysis and correlation maximizes productivity and efficiency.

2. Network visibility

By inspecting packet captures between for visibility into network flows, the SIEM analytics engine can get additional insights into assets, IP addresses and protocols to reveal malicious files or the data exfiltration of personally identifiable information (PII) moving across the network.

3. Threat Intelligence

Being able to incorporate either proprietary or open-source intelligence feeds into your SIEM solution is essential in order to recognize and combat modern-day vulnerabilities and attack signatures.

4. Analytics

Not all SIEM solutions offer the same level of data analysis. Solutions that incorporate next-gen technology such as machine learning and artificial intelligence help to investigate more sophisticated and complex attacks as they arise.

5. Real-time Alerting

SIEM solutions can be customized to business needs, making use of pre-defined, tiered alerts and notifications across multiple teams.

6. Dashboards and reporting

In some organizations, hundreds or even thousands of network events can happen on a daily basis. Understanding and reporting incidents in a customizable view, with no lag time is essential.

7. IT Compliance

Regulatory compliance requirements vary considerably from one organization to the next. While not all SIEM tools offer the full range of compliance coverage, organizations in heavily regulated industries prioritize auditing and on-demand reporting over other features.

8. Security & IT Integrations

Organizational visibility begins with integrating the SIEM with a variety of security and non-security log sources; established organizations will benefit from a SIEM that integrates with existing investments in security and IT tooling.

Many companies have created commercial SIEM solutions.

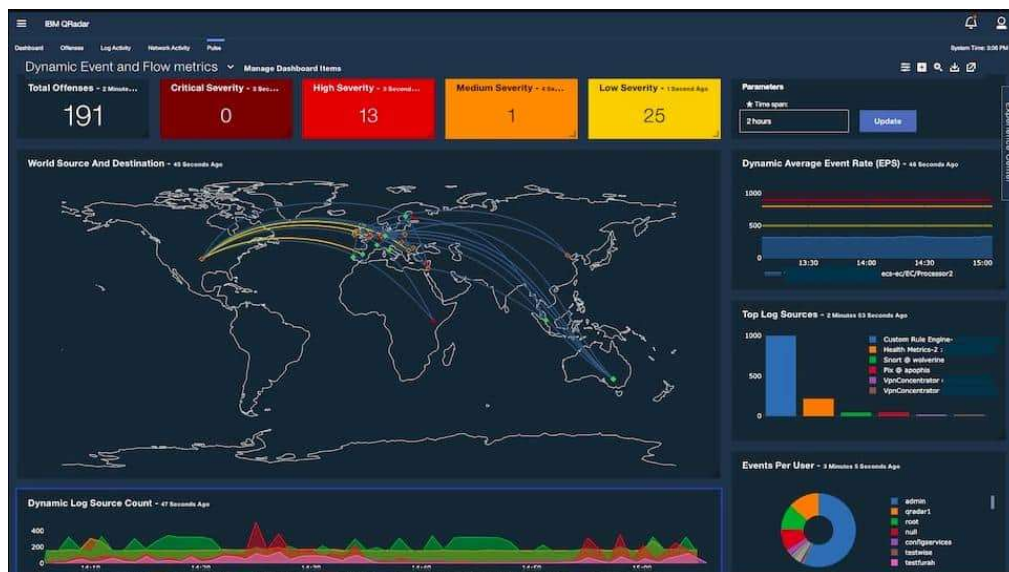
Splunk, LogRhythm, ArcSight, and QRadar are among the most common names you will hear, as they are commercial solutions that have proved their worth in the space. However, these solutions can be quite costly because it is priced based on how much data you are generating. There are open-source Billy Leung, May 2021 SIEM Evaluation Report 3 solutions that are available for everyone to use for free. **ELK Stack and Snort are most popular.** Commercial solutions are often costly monetarily but offers the full features of their product with support while open-source solutions may require significant personnel resources to maintain and does not come with any product support. The challenge for companies is to decide which solution will fit them best, which often depends on their needs and resources available.

IBM QRadar –

QRadar offers a 14-day demo license to allow potential customers to explore and test their product. The demo itself has sample data already embedded for user experience and use case scenarios. During the research, it appears that the product is being overhauled on the User Interfaces (UI). The old interface looked to be development in the early 2000s where the new one is more modern, sleek looking.

The solution includes more than 450 pre-built Device Support Modules (DSMs), which provide default setting integrations with commercial off-the-shelf technologies. Customers can simply point logs to QRadar, and it will automatically detect the log source type and apply the correct DSM to parse and normalize the log data. Once this data is centralized, it can be automatically analyzed to identify known threats, anomalies that may indicate unknown threats and critical risks that may leave sensitive data exposed. IBM QRadar SIEM sits at the core of the IBM QRadar Security Intelligence Platform, which applies automated, intelligent analytics to a vast amount of security data to provide security analysts with actionable insight into the most critical threats, enabling them to make better, faster triage and response decisions. This comprehensive platform brings together log management SIEM, network analysis, vulnerability management, user behavior analytics, threat intelligence and AI-powered investigations into one single platform managed from a single interface.

Overall, the solution fits the need for El Dorado county, because it is easy to navigate, easy to pivot from function to function, and mostly compatible with other third-party products for integration.



The screenshot shows the 'All Offenses' view in IBM QRadar. It lists various offenses with columns for Magnitude, Status, Relevance, and Severity. The details for 'Offense 1' are expanded, showing a description of a configuration change, source and destination IP addresses, and a summary of the offense source.

| Magnitude | Status | Relevance | Severity |
|-----------|------------|-----------|----------|
| unknown | Unassigned | 2 | 5 |

Description: unknown preceded by SIM Configuration Change preceded by SIM User Authentication preceded by SIM User Action preceded by Certificate validation passed preceded by Unknown log event.

Source IP(s): 192.76.175.118

Destination IP(s): 172.31.41.8, 192.76.175.118

Network(s): Multiple (2)

Offense Source Summary:

| IP | Location |
|----------------|----------|
| 192.76.175.118 | India |

Offense Details:

| Offense Type | EventFlow count | Start | Duration | Assigned to |
|--------------|--|---------------------------|----------------|-------------|
| Source IP | 730 947 events and 0 flows in 6 categories | Jan 27, 2021, 12:16:09 PM | 8d 18h 59m 50s | Unassigned |

Offense Source Summary:

| Username | Host Name | Asset Name | Offenses |
|----------|-----------|------------|----------|
| Unknown | Unknown | Unknown | 1 |

Offense Source Summary:

| Magnitude | Vulnerabilities | MAC Address | Weight | Events/Flows |
|-----------|-----------------|-------------|--------|--------------|
| Unknown | 0 | Unknown NIC | 0 | 730 947 |