**What is SIEM:**

SIEM stands for security information and event management, a SIEM solution enables an organization to centrally collect data across its entire network environment to gain real-time visibility into activity that may potentially introduce risk to the organization. SIEM software combines security information management (SIM) and security event management (SEM) to provide real-time analysis of security alerts generated by applications and network hardware. SIEM software matches events against rules and analytics engines and indexes them for sub-second search to detect and analyze advanced threats using globally gathered intelligence. This gives organization a track record of all the activities that being performed in their IT environment.

**Features of SEIM:**

**Real-Time Log & Data Collection**

A SIEM collects logs from many it devices and external sources like servers, security devices applications, OS etc, The logs that are collected by a siem are mapped to the information of the IT infrastructure of the organization so that any activity performed in the system can be analyzed against the set of rules that are defined by performing this mapping.

Its important to define from which devices and or applications, the logs will be collected, its also crucial to collect logs in real time so that any security threat is dealt with in the shortest time possible. The security team gets deep knowledge about the activities in the whole network.

**Log Correlation & Threat Intelligence**

Since logs from different applications and systems are collected, they vary greatly with each other, and can be in a format that cannot be understood easily by people.

A SIEM solution parses through all the logs, converts them in readable format so that they can be understood by security analysts. It also corelates logs from different applications and systems so that insights into the whole system can be provided.

The SIEM ingests logs from various sources and correlates it to threat intelligence feeds and malicious activity found within the environment.

**Prioritization, Analytics & AI**

SIEM solution can generate hundreds or thousands of events per second, security analysts need to be able to swift through these events and gain proper insights, for this purpose it is important to prioritize the events and alerts based on some pre-defined security rules.

In this regard, machine learning and AI can be of big help, ML algorithms look through large volume of log data and help analysts quickly detect indicators for possible malicious activity.

Artificial intelligence helps improve the accuracy of SIEM solution.

**Reporting & Dashboards**

A SIEM solution distributes information in a meaningful way by creating reports from the information it collects, it lets the organization choose the kinds or templates of reports for various purposes.

After collecting log data from different systems and application, a SIEM solution normalizes data for proper analysis and converts it into actionable information through dashboards so the meaningful insights are provided to the bussiness or organization.

**Security Workflows**

Finally, security workflows are another important SIEM feature you’ll need. A security workflow allows your security team to visualize the security monitoring stages, the incident response process, and the events that occur across each of these stages. A security workflow allows your team to identify reactive responses or prevention-centric responses and shift to a more response-centric mindset.

**How is SEIM Implemented?**

There are a few steps involved in implementing a SEIM solution, which are as follows:

**1. Define project and requirements**

The first step to launching a SIEM implementation process is planning the project’s timeline. This involves outlining the scope of the project along with its necessary informational, budgetary, and physical resources. Here, companies should define their goals and identify all necessary resources.

These are some basic components that most companies include while scoping their SIEM requirements and log sources:

Defining project timeline is the first step in implementing a SIEM solution, this includes highlighting the scope of the project, the budget, and physical resources that we are going to need. The company should also define the goals at this stage.

**2. Research products**

There are three main factors to consider while deciding on a SIEM solution for your company.

**Vendor analysis:** This can be done in three ways, the first is gathering information from the vendor himself, online resources and from search engines, this could identify the major SIEM vendor in the market quickly. Software analyst firms and empirical testing can also be used as resources for evaluation. Research and testing services providers produce insights on markets and tools. Just be cautious, as some of these providers may lack transparency in their evaluation and rating criteria.

**Product analysis:** Review sites like G2 are great places to read firsthand accounts of SIEM tools being used in the real world. Companies can easily visit G2's SIEM category and see the products ranging in popularity and satisfaction. We also provide ratings for individual features and information related to the user’s role, company size, and industry.

**Use case assessment:** Assessing the use case as it pertains to your business will likely require communication with the vendors on your shortlist of potential products. Many of them will provide industry-specific scenarios, case studies, and product demos at your request. Teams fulfilling all three requirements will come away with a list of potential products. This list will make it easier to choose a solution based on how each tool would or would not fulfill the requirements they’ve already outlined and the resources they have available.

**3. Implementation planning**

Once a product has been selected, outline a number of implementation procedures to ensure a smooth and effective transition. These are a few components to include in your plan.

**Design architecture:** Diagram all data sources related to log sources and data inputs. Deploy information collectors to ensure all log sources are connected. In addition to data aggregation from all your connected devices, SIEM systems integrate both internal and third-party threat and vulnerability data. Storage and alerting systems also ensure proper functionality after deployment.

**Create rules:** Ensure your correlation engines are functioning with basic policies and determine the more customized rules and policies to implement in the long term. These rules are intended to optimize documentation and alerting without damaging network performance. They should also be customized to meet any necessary compliance requirements previously outlined.

**Define process** — Before deployment, put a handoff plan in place to transfer control from the implementation team to security operations or IT management team. Adjust in accordance with your company’s staffing capabilities to ensure teams can effectively manage the SIEM going forward. Any other long-term management processes should be outlined as well. Companies must train staff on general SIEM management as well as their team’s logging processes and data management plans. You may need to adjust to avoid understaffing, unmanageable logging rates, and storage capacity issues.

**4. Deployment and review**

As deployment becomes a reality, a few immediate actions need to take place. Here is what to focus on once a new SIEM is operationalized.

Collection: Examine recently implemented SIEM systems to ensure data is collected and encrypted properly. Depending on your solution, agent-based systems should be examined and monitored during preliminary deployment to ensure they’re collecting data properly. Those implementing agentless solutions should simply ensure all points of monitoring are communicating back to the SIEM properly.

Storage: Once information is being properly collected, teams must ensure all activities, logs, and events are stored correctly. Companies using external storage systems must make sure transfers and integrations are secured and functional, that databases are properly formatted, and that information can be queried once stored.

Testing: Test the system to visualize connected devices and display to those planned. Users can test a new SIEM solution by simulating events. Threat modeling and simulated tests should be conducted. These mimic real-world security threats to verify that all operations are functional. Teams should also compare data on correlated and severe events to their pre-implementation figures. Once the testing and review processes are completed, implementation teams should hand off to security teams for full-time management.

**DATABASE Connectivity and programming languages used to implement SEIM:**

Based on the requirements of the organization, various mix of databases and programming languages can be used to implement a SIEM solution.