SIEM(Security Information and Event Management)

SIEM's basic function is to centralize all the notification from various security technologies like firewall IDS/IPS and more. SIEM can be referred to as a log aggregation solution . There is automated cross correlation and analysis of all raw events and logs there SIEM looks for hidden cyber issues.
The main focus is on security-related incidents and events, such as succeeded or failed logins, malware activities or escalation of privileges. These insights can be sent as notifications or alerts, or discovered by security analysts using the SIEM platform's visualization and dashboarding tools.

Like from IDS alert we have received an alert for SQL injection against one of our servers

Why is SIEM needed?

1. It can normalize activity to readable format
2. Run analysis on data breach
3. Set Rules and other parameters to block cyber attacks
4. Security Monitoring
5. Can detect insider threats also
6.

How can SIEM Help ?

1. Data aggregation: It can aggregate data coming from various security devices like IDS/IPS firewalls and other security devices
2. Correlation : This basically means it links events and data into a meaningful bundle which reflects meaningful security issues.
3. Alerting : It can send out alert if any malicious activity is found
4. Dashboard and Visualization : It can represent output into visual/patterns that do not conform to standard patterns
5. Compliance : Automates the gathering of compliance data, producing reports that adapt to security, governance and auditing processes for standards like HIPAA, PCI/DSS

How SIEM Works?

1. Data collection : We can setup collecting agents on the devices to collect the data. There can be pre processing done at that end point also and only some of the events and event data passed to centralized storage.
2. Data storage : SIEMs are built on top of modern data lake technology such as Amazon S3 or Hadoop, allowing nearly unlimited scalability of storage at low cost

3. Policies and rules: We can set up rules and define how devices/system should work under normal condition
4. Correlation : The central purpose of a SIEM is to pull together all the data and allow correlation of logs and events across all organizational systems.

Components and Capabilities in SIEM architecture

- **Data aggregation** Collects and aggregates data from security systems and network devices
- **Threat intelligence feeds:** Combines internal data with third-party data on threats and vulnerabilities
- **Correlation and security monitoring:** Links events and related data into security incidents, threats or forensic findings
- **Analytics:** uses statistical models and machine learning to identify deeper relationships between data elements
- **Alerting:** Analyses events and sends alerts to notify security staff of immediate issues
- **Dashboards:**Creates visualizations to let staff review event data, identify patterns and anomalies
- **Compliance:** Gathers log data for standards like HIPAA, PCI/DSS and generates reports
- **Retention:** Stores long-term historical data, useful for compliance and forensic investigations
- **Incident response** Helps security teams identify and respond to security incidents, bringing in all relevant data

Data Management : **Stored->Optimized and indexed->Tiered**
Hot data necessary for live security monitoring should be on high-performance storage,
Cold data, which you may one day want to investigate

Log Retention Techniques used by SIEM for Security Standards :

1. Syslog servers: syslog is a standard which normalizes logs, retaining only essential information in a standardized format
2. Deleting Schedule:SIEM automatically deletes logs which are no longer needed for compliance
3.Log Filtering : Logs can be filtered by the source system, times, or by other rules defined by the SIEM administrator.
4.Summarization: log data can be summarized to maintain only important data elements such as the count of events, unique IPs, etc.

Log FLow:

Capture -> Filter -> Index -> Analyze ->Correlate ->Threshold

1. Filter out and keep relevant data
2. To enable Analysis Indexing and optimization is performed
3. The result of above step is correlated and analyzed in depth
4. The one which exceeds the threshold becomes a security threat.

SIEM Reporting and Dashboards

- Alerts and notifications--prompt security staff to investigate an anomaly or apparent security issue
- Data exploration--enable security staff to freely explore data to actively hunt for threats, or investigate a known security incident
- Dashboards--display status of security-related systems and metrics and highlight potential security issues

A **SOC** uses **SIEM** software as a foundational component. It's a collection of tools that provides a combination of SIM (security information management) also known as log management, and SEM (security event management), also known as the correlation engine. With a SIM and SEM, a **SIEM** offers actionable intelligence.