Security Information and Event Management:

In any network (with endpoints, servers, and websites), **every device generates logs** — records of what's happening.
Without visibility, **attacks can go unnoticed for days**

Types of Log Sources:

Host-Centric Logs

These come from **inside the devices** (computers, servers).within or related to the host. Some log sources that **generate host-centric logs** are Windows Event logs, Sysmon, Osquery, etc

A user accessing a file

1. A user attempting to authenticate.
2. A process Execution Activity
3. A process adding/editing/deleting a registry key or value.
4. Powershell execution

Examples:

- **Windows Event Logs, Sysmon, Osquery**

2**. Network-Centric Logs**

These come from communication **between devices or with the internet.**
Examples:

- SSH, VPN, HTTP/S, FTP

Since each device **generates hundreds of logs per second,** checking them **manually is impossible.**
A SIEM tool solves this problem by collecting, analyzing, and alerting on logs in one place.

1. **Real-time log ingestion :** collects logs instantly **from all devices**
2. **Alerts on suspicious activity** — detects abnormal behavior early
3. **24/7 monitoring** — ensures constant visibility
4. **Threat protection** — helps stop attacks before damage occurs
5. **Data visualization & insights** — shows trends and patterns clearly
6. **Incident investigation** — allows reviewing past events to find the root cause

---

✅ In short:
SIEM = Central brain of the SOC — it **collects logs**, **detects threats early,** and helps security **teams investigate incidents efficiently.**

That is one of the advantages of having **a SIEM solution in place. I**t not only takes logs from various sources in real-time b**ut also provides the ability to correlate between events, search through the logs, investigate incidents and respond promptly**

Windows Machine:
Windows records every event that can be viewed through the **Event Viewer utility.**
Linux OS

stores all the related logs, such as events, errors, warnings, etc. Which are then ingested into SIEM for continuous monitoring. Some of the common locations where Linux store logs are:

- /var/log/httpd : Contains **HTTP Request / Response** and error logs.
- /var/log/cron : **Events related to cron jobs** are stored in this location.A **cron job** is a scheduled task in Linux that runs automatically at specified times or intervals.
- /var/log/auth.log and /var/log/secure : Stores **authentication related logs.**
- /var/log/kern : This file stores kernel related events.

WEB SERVER:

In Linux, common locations to write all apache related logs are /var/log/apache or /var/log/httpd.

Log Ingestion

Log ingestion means **collecting logs from different devices** (like computers, servers, routers) and **sending them to the SIEM.**
These logs help detect suspicious activity and security issues.

Agent / Forwarder: These SIEM solutions provide a **lightweight too**l called an **agent (forwarder by Splunk)** that gets installed in the **Endpoint.**

syslog: Syslog is a widely used **protocol to collect data from various systems** like web servers, databases, etc., **are sent real-time data to the centralized destination**.Manual Upload

1. Used for **offline or old log files.**
2. Analysts can **manually upload logs into the SIEM (like Splunk or ELK) for quick analysis.**
3. Once uploaded, **logs are normalized (formatted properly) for easy searching.**

port-Forwarding: SIEM solutions can also be **configured to listen on a certain port**, and then the endpoints forward the data to t**he SIEM instance on the listening port**.

Devices (like routers/firewalls) cannot **install a forwarder — they can only send logs using Syslog.**

Syslog is lightweight and built-in to most network devices — no extra setup or software needed.

Main capabilities:

1. Correlation: Connects **related events** from different sources to detect real attacks.
2. Visibility: Shows **both host activity (like user login) and network activity (like data transfer).**

Monitoring & Investigating: Watching alerts and investigating suspicious activities.

Identifying False Positives: Finding alerts that are not real threats.

Tuning Rules: Adjusting **SIEM rules** to reduce **unnecessary alerts (noise).**

Reporting & Compliance: Creating reports for **management and meeting security standards.**

Improving Visibility: Finding **areas (blind spots) not covered by monitoring** and fixing them.

Analysing Logs and Alerts:
sinnce the logs are ingested, SIEM looks for **unwanted behavior or suspicious pattern** within the logs with the help of the conditions set in the rules by the analysts.

Dashboard

Dashboards are the **most important components** of any SIEM. SIEM presents the data for analysis after being **normalized and ingested.**Each SIEM solution comes with **some default dashboards** and provides an option for custom Dashboard creation.

Alert Highlights

1. System Notification
2. Health Alert
3. List of Failed Login Attempts
4. Events Ingested Count
5. Rules triggered
6. Top Domains Visited

Correlation rules : are logical conditions in SIEM that detect suspicious activity.

Correlation logs: Individual logs are not very useful. SIEM correlates the logs of different sources and finds any relationship between them. This helps to identify malicious activity by analyzing its pattern

Examples: 5 failed logins in 10 seconds → alert for multiple failed logins; successful login after failed ones → alert for suspicious login.

When triggered, SIEM checks events to confirm rule conditions, and analysts decide if it's a true or false positive.
Event ID 104 appears when someone tries to clear Windows event logs.

Normalization of Logs

Raw logs are of different formats and sizes. A Windows log does not look the same as a Linux log.