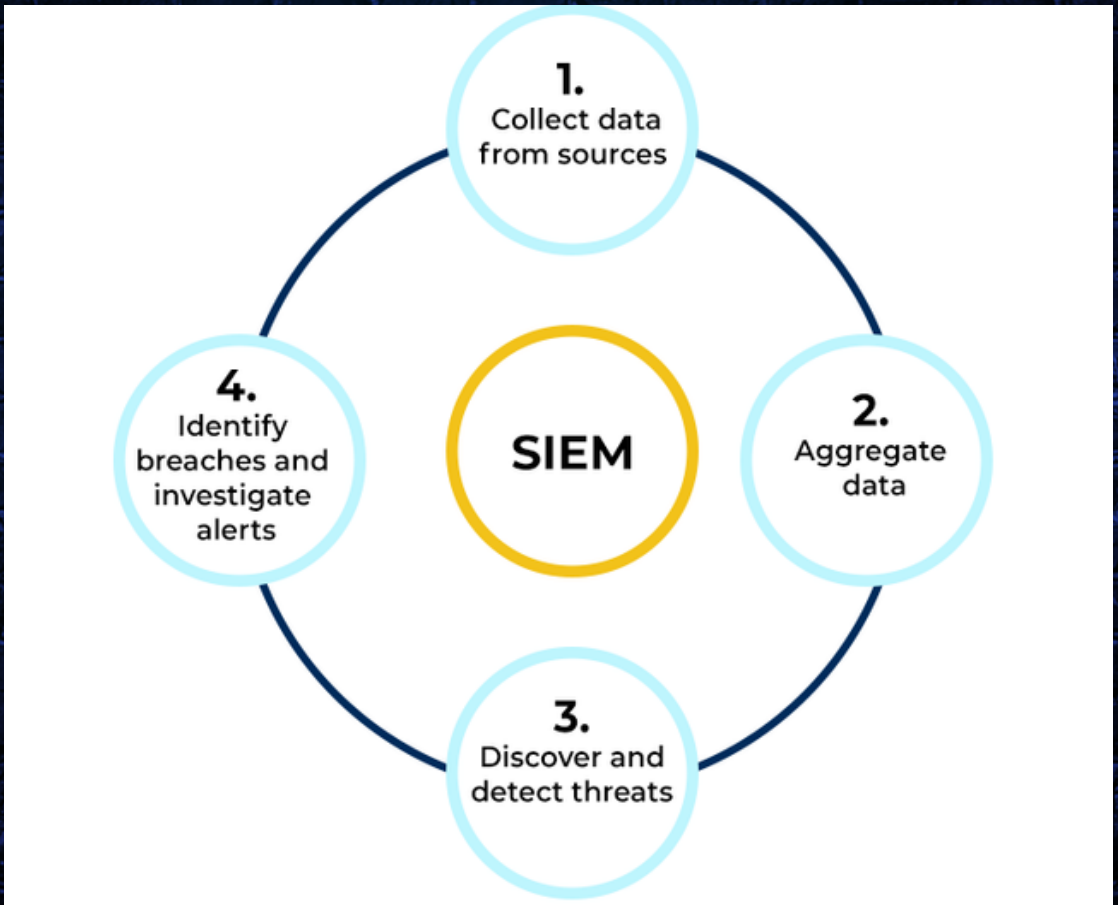
HOW SIEM WORKS?

WHAT IS SIEM?

SIEM stands for Security Information and Event Management which is a centralized solution used to monitor real-time logs, security alerts, for threat detection, incident handling, investigation & compliance.

SIEM WORKING



- First it collects logs from different devices, processed those logs by performing normalization which is then available to us for searching and analyzing on dashboards.
- It creates alerts when certain abnormality occur (we configure correlation rules using use-cases and when an event matches with the specified condition it generates an alert) and stores all event details which then used by security professionals to investigate and also enables them to respond to that incident.

SIEM CAPABILITIES

- Real-time log Ingestion
- Threat Detection, Investigation and Response
- Alerting against abnormal activities
- 24/7 Monitoring and visibility
- Protection against the latest threats through early detection
- Data Insights and visualization
- Ability to investigate past incidents.

TOP SIEM SOLUTIONS

- Splunk
- ELK
- Qradar
- LogRythm

Example

SPLUNK WORKING

COMPONENTS

1. Spunk Forwarder
2. Splunk Indexer
3. Splunk Header

SPUNK FORWARDER

- It works like a shipping agent which is installed on endpoint to send logs to Splunk.

SPLUNK INDEXER

- It perform Normalization on logs.
- Normalization refers to the process of standardizing and organizing log data from various sources into a common format.

SPLUNK HEADER

- It is like a search bar used to search/filter data.

WHEN SELECTING A SIEM TOOL, WHAT KEY FEATURES WOULD YOU PRIORITIZE TO ENSURE EFFECTIVE CYBERSECURITY, AND WHY?