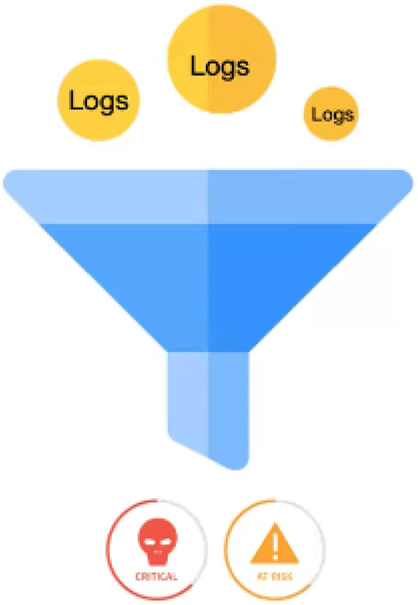
SIEM

Comprised of 2 things:

- SIM - Security Information Management
- SEM - Security Event Management

Security Information and Event Management

- System that stores logs files and security events.
- Helps in the easy analysis of data.
- Log management system specialised for secuirty.
- Collects information from all the mechanisms like Endpoint Security, Firewalls, Itrusion Detection systems etc.



UEBA
User and Entity Behavior Analystics
Responsible for tracking user's normal and abnormal data for helping analysts to find abnormal activities like new location login and machines tansfering unusual amount of data.
Basically this spots the abnormal activities for analysts to look into.

SOAR
Security Orchestration Automation and Response
This basically helps in automating things so the resonse teams does not have to individually and manually do so.

SIEM Functions

1. Collection:
    - Agent Based - The agent from each device collects the data parses it and forwards those logs to the system. eg : SYSMON, NXLog etc.
    - Agent Less: These are API based which directly send the log to the SIEM system.
2. Aggregation: Collecting logs from all the different devices and setting it up in such a way that it is useful for the later referencing and understanding. This would be done with PUSH or PULL methods. In PUSH the devices send the data to the server and in PULL the server is responsible for extracting data from the devices.
3. Parsing: This is a software based mechanism responsible for framing the logs collected from different devices in different formats to a structured data format. These use REGEX for porforming the task. Parser is setup for all the deivces cause mostly all have diferent format for saving logs.