- **Log is a record of events that occur within an organization's systems and networks**
    - Firewall log is a record of attempted or established connections for incoming traffic from the internet. It also includes outbound requests to the internet from within the network.
    - Network log is a record of all computers and devices that enter and leave the network. It also records connections between devices and services on the network.
    - Server log is a record of events related to services such as websites, emails, or file shares. It includes actions such as login, password, and username requests.
- Security information and event management (SIEM): An application that collects and analyzes log data to monitor critical activities in an organization
- Security orchestration, automation, and response (SOAR): A collection of applications, tools, and workflows that use automation to respond to security events
- Splunk Enterprise: A self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time
- Splunk Cloud: A cloud-hosted tool used to collect, search, and monitor log data
- Chronicle: A cloud-native tool designed to retain, analyze, and search data
- Metrics: Key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application