filename:comptia-secplussy0601-9-4-1-siem-and-soar-systems
Showname: Security+ (SY0-601)
Topic: Operational Security and Incident Response
Episode: SIEM and SOAR Systems

*Summarize the techniques used in security assessments.*

Description: In this episode, the viewer will identify the components that make up a security information and event management (SIEM) solution as well as security orchestration, automation and response systems (SOAR)

---

- What the need for SIEM?
    - Immense amount of event-related data
- Security information and event management (SIEM)
    - Security Information Management
        - Devices and Software
            - Sensors
                - Software Agent
                - Physical or Virtual
                - Cloud and on-premise
    - Security Event Management
        - Real-time analysis
        - Visualization
        - Uses anomaly-based threat detection
        - Threat intelligence feeds
        - Intelligence Fusion (advanced Threat hunting)

        - Exchange of intelligence infomation
    - Sentiment analysis
        - Opinion mining
        - Are comments good/bad/neutral
        - Leverages Natural Language Processing
- Security orchestration, automation, and response (SOAR)