CYS 4 109

Security Information and Event Management system

Based on «Introduction to SIEM on Tryhackme.com»

Dr. Abdelaziz AMARA-KORBA

amarakorba.abdelaziz@gmail.com

Outline

- What is SIEM, and how does it work?
- Why is SIEM needed?
- What is Network Visibility?
- What are Log Sources, and how is log ingestion done?
- What are the capabilities a SIEM provides?

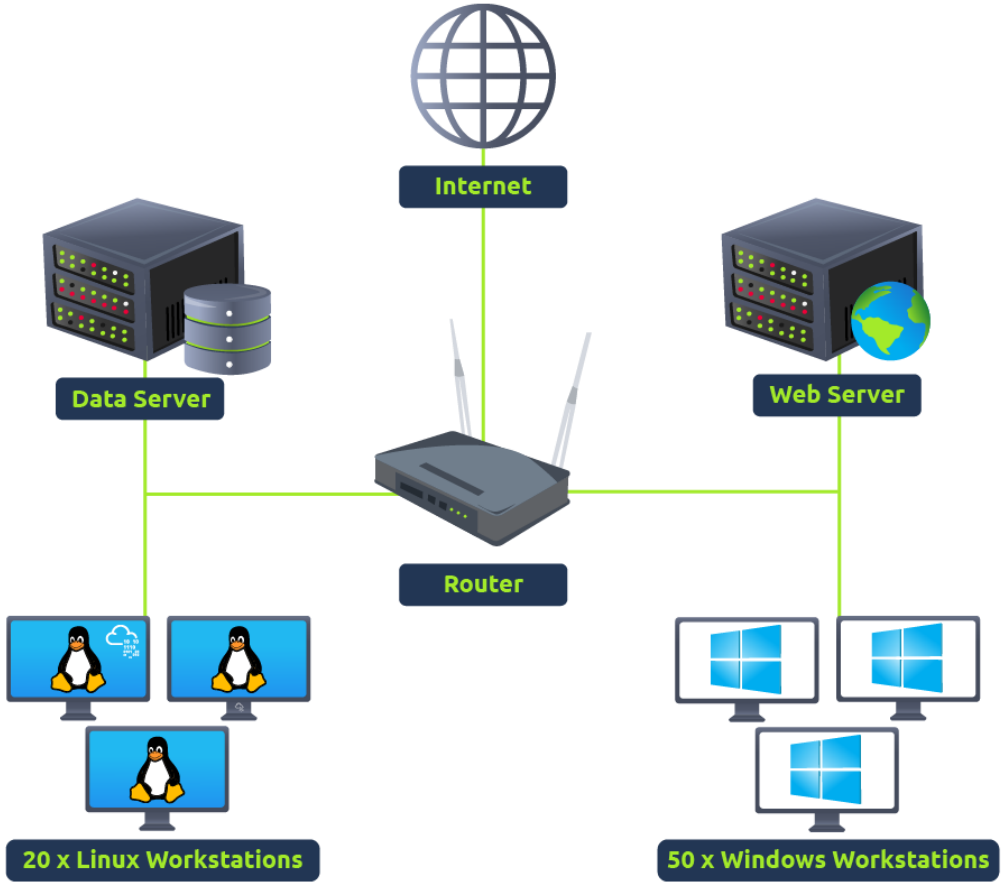
What is SIEM

- SIEM stands for Security Information and Event Management system.

- It is a tool that collects data from various endpoints/network devices across the network, stores them at a centralized place, and performs correlation on them.

Network Visibility through SIEM

- Each network component can have one or more log sources generating different logs.
- Example: setting up Sysmon along with Windows Event logs to have better visibility of Windows Endpoint.
- We can divide our network log sources into two logical parts:
  - Host-Centric Log Sources
  - Network-Centric Log Sources



Host-Centric Log Sources

- These are log sources that capture events that occurred within or related to the host.

- Some log sources that generate host-centric logs are Windows Event logs, Sysmon, Osquery, etc. Some examples of host-centric logs are:
  - A user accessing a file
  - A user attempting to authenticate.
  - A process Execution Activity
  - A process adding/editing/deleting a registry key or value.
  - Powershell execution

Network-Centric Log Sources

- Network-related logs are generated when the hosts communicate with each other or access the internet to visit a website.

- Some network-based protocols are SSH, VPN, HTTP/s, FTP, etc. Examples of such events are:
  - SSH connection
  - A file being accessed via FTP
  - Web traffic
  - A user accessing company's resources through VPN.
  - Network file sharing Activity

Importance of SIEM

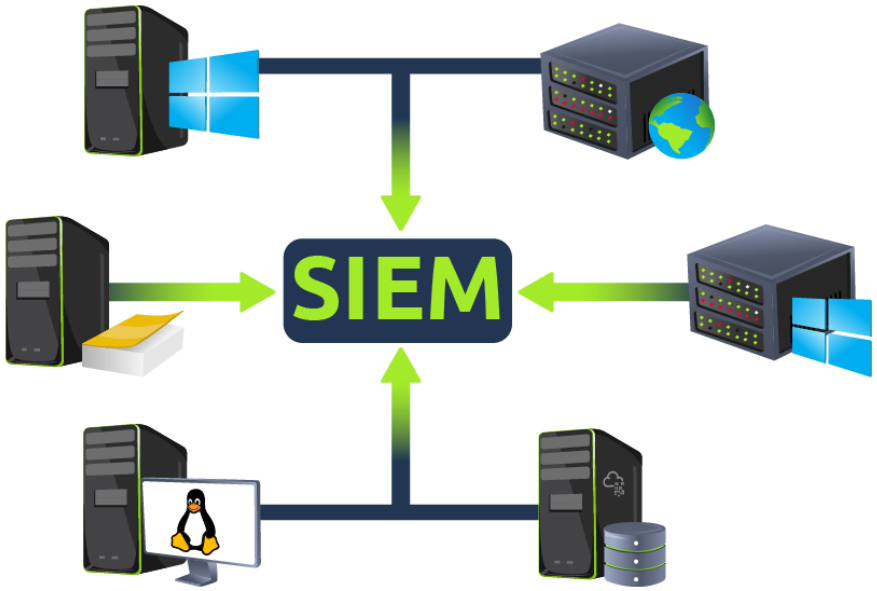
- Some key features provided by SIEM are:
  - Real-time log Ingestion
  - Alerting against abnormal activities
  - 24/7 Monitoring and visibility
  - Protection against the latest threats through early detection
  - Data Insights and visualization
  - Ability to investigate past incidents.

Log Sources and Log Ingestion

- Every device in the network generates some kind of log whenever an activity is performed on it, like a user visiting a website, connecting to SSH, logging into his workstation, etc.
  - **Windows**: records every event that through the Event Viewer utility. It assigns a unique ID to each type of log activity
  - **Linux**: stores all the related logs, such as events, errors, warnings, etc. Which are then ingested into SIEM for continuous monitoring

Log Ingestion

- Each SIEM solution has its own way of ingesting the logs. Some common methods used by these SIEM solutions are explained below:
  - Agent / Forwarder: a lightweight tool called an agent that gets installed in the Endpoint. It is configured to capture all the important logs and send them to the SIEM server.
  - Syslog: 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: Some SIEM solutions, like Splunk, ELK, etc., allow users to ingest offline data for quick analysis. Once the data is ingested, it is normalized and made available for analysis.
  - Port-Forwarding: SIEM solutions can also be configured to listen on a certain port, and then the endpoints forward the data to the SIEM instance on the listening port.



SIEM Capabilities

- SIEM is one major component of a Security Operations Center (SOC) ecosystem.
- SIEM starts by collecting logs and examining if any event/flow has matched the condition set in the rule or crossed a certain threshold

- Some of the common capabilities of SIEM are:
  - Correlation between events from different log sources.
  - Provide visibility on both Host-centric and Network-centric activities.
  - Allow analysts to investigate the latest threats and timely responses.
  - Hunt for threats that are not detected by the rules in place.

SOC Analyst Responsibilities

- SOC Analysts utilize SIEM solutions in order to have better visibility of what is happening within the network.

- Some of their responsibilities include:
  - Monitoring and Investigating.
  - Identifying False positives.
  - Tuning Rules which are causing the noise or False positives.
  - Reporting and Compliance.
  - Identifying blind spots in the network visibility and covering them.

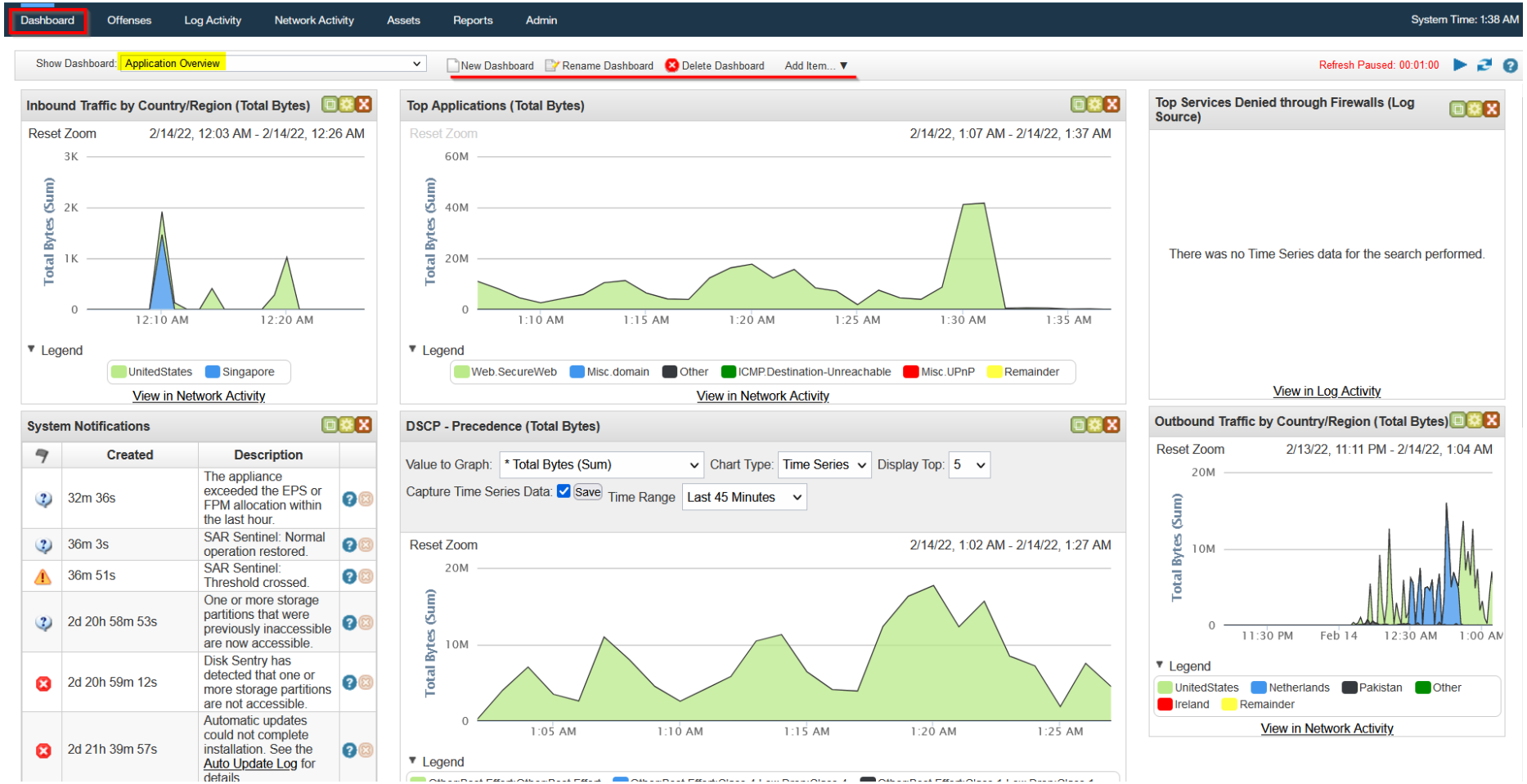
Analysing Logs and Alerts

- Dashboards: are the most important components of any SIEM.
  - SIEM presents the data for analysis after being normalized and ingested.
  - The summary of these analyses is presented in the form of actionable insights with the help of multiple dashboards.

- Some of the information that can be found in a dashboard are:
  - Alert Highlights
  - System Notification
  - Health Alert
  - List of Failed Login Attempts
  - Events Ingested Count
  - Rules triggered
  - Top Domains Visited

Dashboard

An example of a Default dashboard in Qradar SIEM is shown below:



Correlation Rules

- Correlation rules are pretty much logical expressions set to be triggered.
  - Ex. If a User gets 5 failed Login Attempts in 10 seconds - Raise an alert for Multiple Failed Login Attempts

- To explain how the rule works, consider the following Eventlog use cases:
  - **Use-Case**: adversaries tend to remove the logs during the post-exploitation phase to remove their tracks.
    - A unique Event ID 104 is logged every time a user tries to remove or clear event logs.
  - To create a rule based on this activity, we can set the condition as follows:
    - Rule: If the **Log source is WinEventLog AND EventID is 104** - Trigger an alert Event Log Cleared

Alert Investigation

- Once an alert is triggered, the events/flows associated with the alert are examined, and the rule is checked to see which conditions are met. Based on the investigation, the analyst determines if it is a True or False positive.

- Some of the actions that are performed after the analysis are:
  - Alert is False Alarm. It may require tuning the rule to avoid similar False positives from occurring again.
  - Alert is True Positive. Perform further investigation.
  - Contact the asset owner to inquire about the activity.
  - Suspicious activity is confirmed. Isolate the infected host.
  - Block the suspicious IP.

SIEMs

- **Splunk Enterprise Security:** Splunk is well-known for its ability to ingest vast amounts of data and offers a robust platform for security analysis and data visualization.

- **Elastic Security:** Part of the Elastic Stack, Elastic Security combines search, machine learning, and log analytics for effective threat detection and security monitoring.

- **Wazuh:** An open-source security tool for intrusion detection, integrity monitoring, asset inventory, and incident management. Integrating with ELK Stack, it offers advanced SIEM capabilities, making it a comprehensive and free security management platform.

- **IBM QRadar Security Intelligence**: QRadar provides a comprehensive solution that offers advanced behavioral analytics, threat detection, and incident management capabilities.