Introduction to SIEM

SIEM

- Security Information and Event Management system
- tool that collects data from various endpoints/network devices across the network, stores them, and performs correlation on them

Network Visibility through SIEM

- understand why it is important to have better visibility of all the activities within a network

Example of a simple network:
- multiple Linux/Windows based endpoints
- 1 data server
- 1 web server
- devices communicate and access the internet through a router

- each network component can have one or more log sources generating different logs

Divide our network log sources into 2 logical parts:

1) Host-Centric Log Sources

These are log sources that capture events that occurred within or related to the host.
- log sources that generate host-centric logs are: Windows Event Logs, Sysmon, Qsquery

Host-Centric Logs are:
- user accessing a file
- user attempting to authenticate
- a process Execution Activity
- Powershell execution
- a process adding/editing/deleting a registry key or value

2) Network-Centric Log Sources

Logs are generated when hosts communicate with each other or access the internet to visit a website.
- network based protocols: SSH, VPN, HTTP/s, FTP

Events:
- SSH connection
- a file being accessed via FTP
- web traffic
- user accessing company resources through VPN

Important of SIEM
- all devices on network generate hundreds of events per second > examining logs on each device can take a long time
- advantage of SIEM > ability to correlate between events, search through the logs, investigate incidents and respond promptly

Key features of SIEM:
- 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

Log Sources and Log Ingestion
- every device on the network generates some kind of log

Windows machine
- records every event > Event Viewer
- assigns a unique ID to each type of log activity
- Event Viewer > Windows Logs > Application/Security/Setup/System

Linux machine
- stores all related logs, events, errors, and warnings
Common locations for Linux logs:
/var/log/httpd: contains HTTP request / response and error logs
/var/log/cron: events related to cron jobs are stored in this location
/var/log/auth.log and /var/log/secure: store authentication related logs
/var/log/kern: stores kernel related events

Web Server
- important to keep an eye on all the requests/responses coming in and out of the webserver
In Linux, common locations to write all apache related logs:
/var/log/apache or /var/log/httpd

Log Ingestion
- all the above logs provide a wealth of information and can help identify security issues
- each SIEM solution has its own way of ingesting the logs

SIEM solutions:
1) Agent/Forwarder

- SIEM solution provides a tool called an agent (forwarder by Splunk) that gets installed in the Endpoint
- it is configured to capture all the important logs and send to SIEM server

2) Syslog

- widely used protocol to collect data from various systems like web servers + databases
- send real time data to the centralized destination

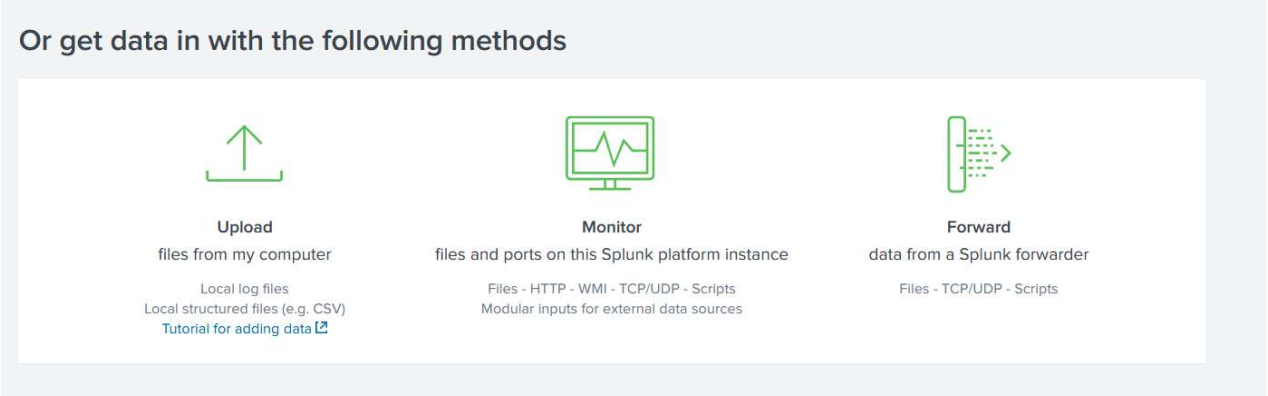
3) Manual Upload

- some SIEM solutions (Splunk and ELK) allow users to ingest offline data for quick analysis
- once the data is ingested, it is normalised and made available for analysis

4) Port Forwarding

- SIEM solutions can also be configured to listen on a certain point, and then endpoints forward the data to the SIEM instance on listening port

Example of how Splunk provides various methods for log ingestion:



Why SIEM?

- used to provide correlation on the collected data to detect threats
- once threat is detected > alert is raised
- provides a good visibility of what is happening within the network infrastructure

SIEM Capabilities

- major component of a SOC
- SIEM starts by collecting logs and examining if any event/flow has matched the condition set in the rule

- 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

Analysing Logs and Alerts

- once the logs are ingested, SIEM looks for unwanted behaviour for suspicious pattern within the logs with the help of conditions set in the rules
- if condition is met > rule gets triggered > incident is investigated

Dashboard

- SIEM presents the data for analysis after being normalized and ingested
- each SIEM solution comes with some default dashboards and provides an option for custom Dashboard creation

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

Correlation Rules

- important role in the detection of threats
- logical expressions set to be triggered

Examples:

- IF user gets 5 failed login attempts in 10 seconds > Raise an alert for multiple failed login attempts
- IF login is successful after multiple failed login attempts > Raise an alert for successful login after multiple login attempts
- rule is set to alert every time a user plugs in a USB

How a correlation rule is created

Example 1:

- attackers tend to remove the logs during post exploitation phase to hide their tracks
- a unique EventID is logged every time a user tries to remove/clear logs > 104
- create a rule based on this

Rule: if the log source is WinEventLog AND EventID is 104 > trigger an alert [Event Log Cleared]

Example 2:

- attackers use commands like whoami (privilege escalation)

Rule: if log source is WinEventLog AND EventCode is 4688, and NewProcessName contains whoami > trigger an alert [WHOAMI command Execution DETECTED]

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

Actions 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