Security Tools

By: Lazaro, Chris, Zanovia, and Ethan

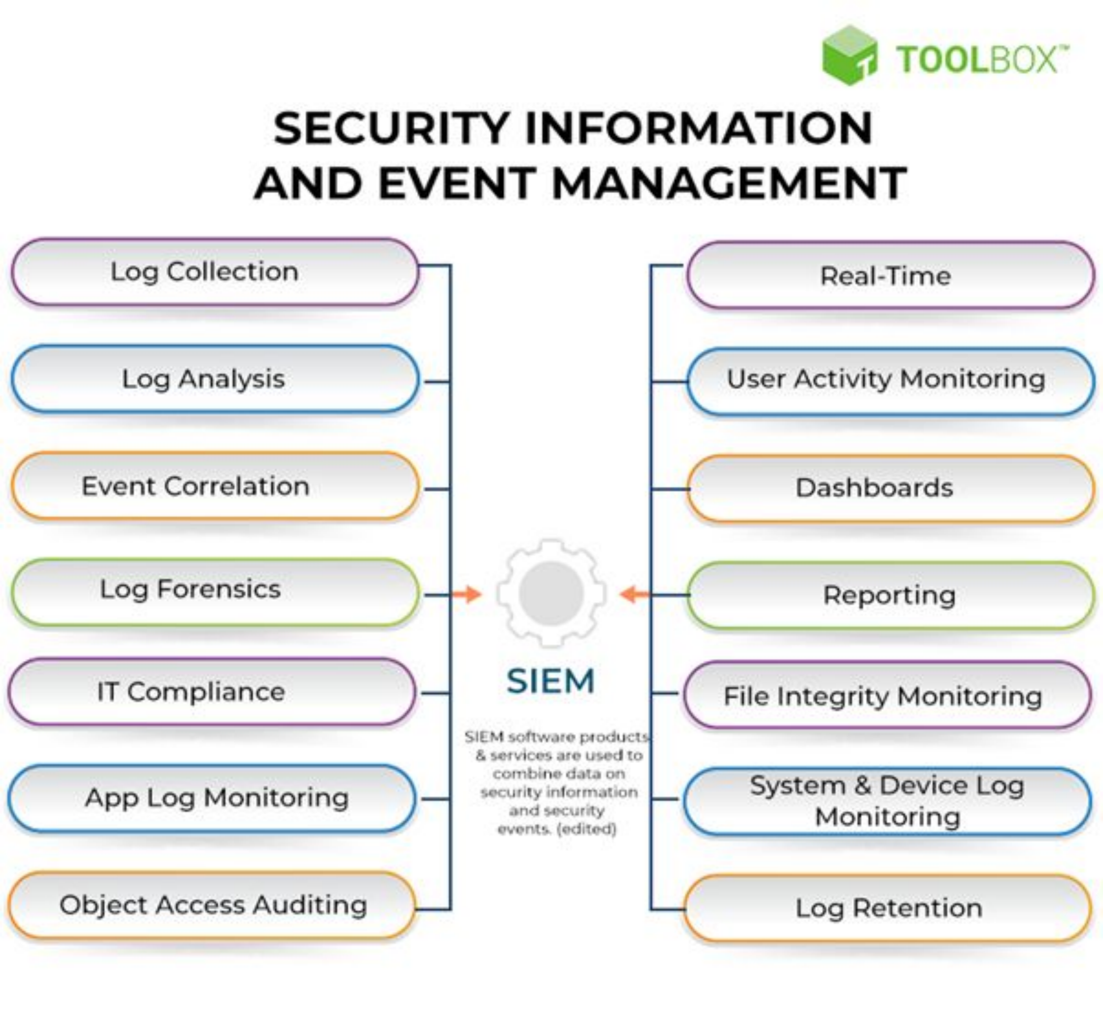
SIEM (Security Information and Event Management)

- SIEM is a combination of security information management (SIM) and security event management (SEM)
- Alerts organizations about potential attacks, information security incidents, or even compliance issues
- SIEM solutions offer real-time monitoring and analysis of events
  - The practice of strengthening threat detection and security incident management through pulling live data and historical security event data

What does SIEM do?

- Monitor, audit, and re-engage with all of the logs that their systems generate
    - Can include applications, devices, or home computers
    - This will alert them about any security issues before they occur instead of relying on responsive action

- SIEM software helps collect the data generated by various applications, network devices, and security systems such as host systems, networks, firewalls, and antivirus events, to name a few. It then brings all the information together into a single central place



TOOLBOX™

SECURITY INFORMATION AND EVENT MANAGEMENT

- Log Collection
- Log Analysis
- Event Correlation
- Log Forensics
- IT Compliance
- App Log Monitoring
- Object Access Auditing

SIEM

SIEM software products & services are used to combine data on security information and security events. (edited)

- Real-Time
- User Activity Monitoring
- Dashboards
- Reporting
- File Integrity Monitoring
- System & Device Log Monitoring
- Log Retention

How can SIEM help with investigations?

- A perfectly configured SIEM system will react quickly if an abnormal event occurs
  - Monitors activities
  - Analyzes events
  - Alerts users
  - Takes automated action to detect and respond to cyber security threats and vulnerabilities before they wreak havoc
- SIEM programming works by gathering log and event data created by various applications, security gadgets, and host frameworks and uniting it into a unified platform
- SIEM implementations provide:
  - Unified alerts
  - Advanced full-packet logging capabilities
  - Intelligent correlation to enhance security operations

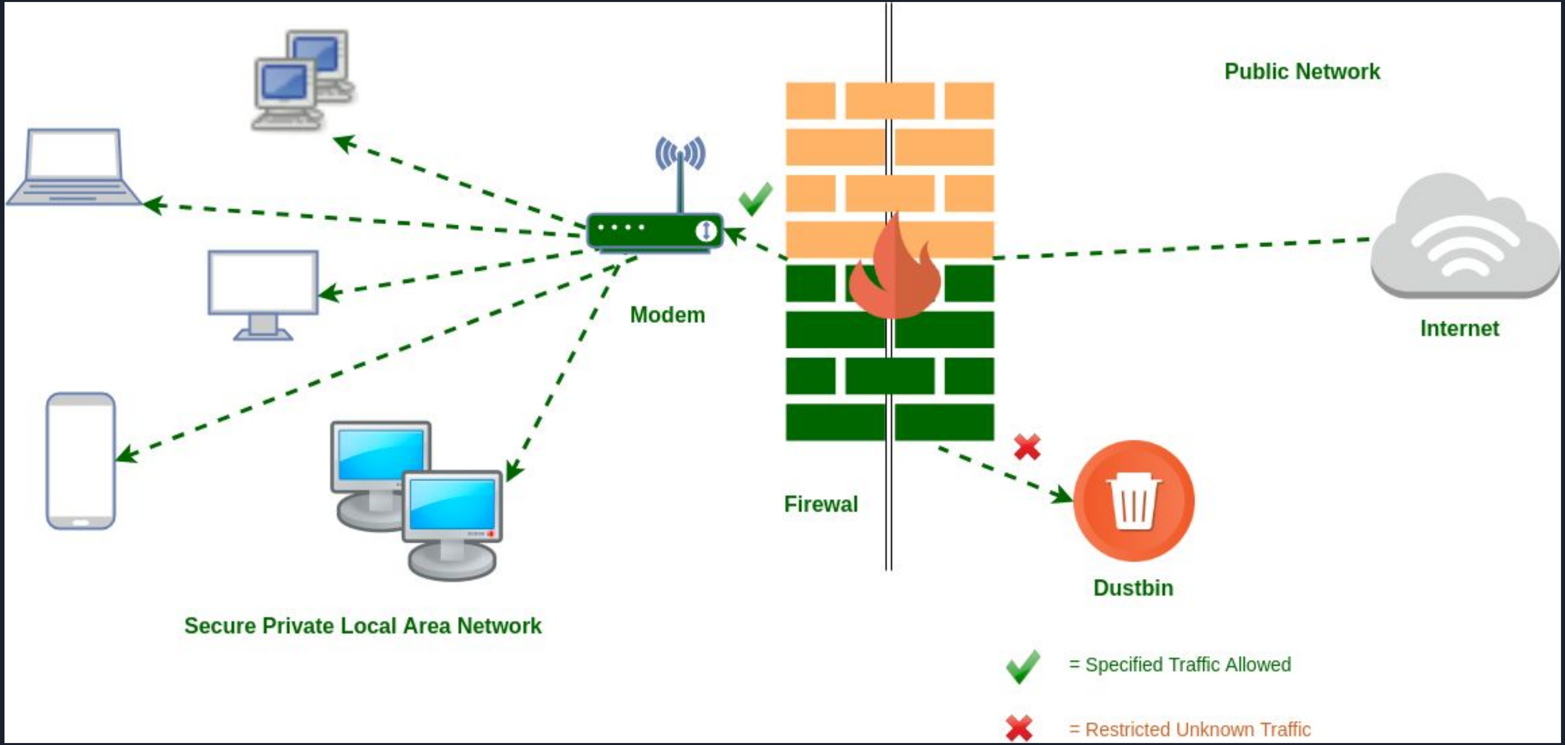
Firewall

- What is it?
  - Network Security device
  - Barrier that sits between an internal network and the public internet

- What does it do?
  - Monitors and filters incoming and outgoing network traffic based on an organization’s security
  - Policies
  - Shields your computer from malicious traffic

- How can it help in my investigation?
  - Provides insight in your network
  - The log records provide information
  - can also be used by a SIEM

Firewall Diagram


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ = Specified Traffic Allowed
✗ = Restricted Unknown Traffic

What is an IDS/IPS?

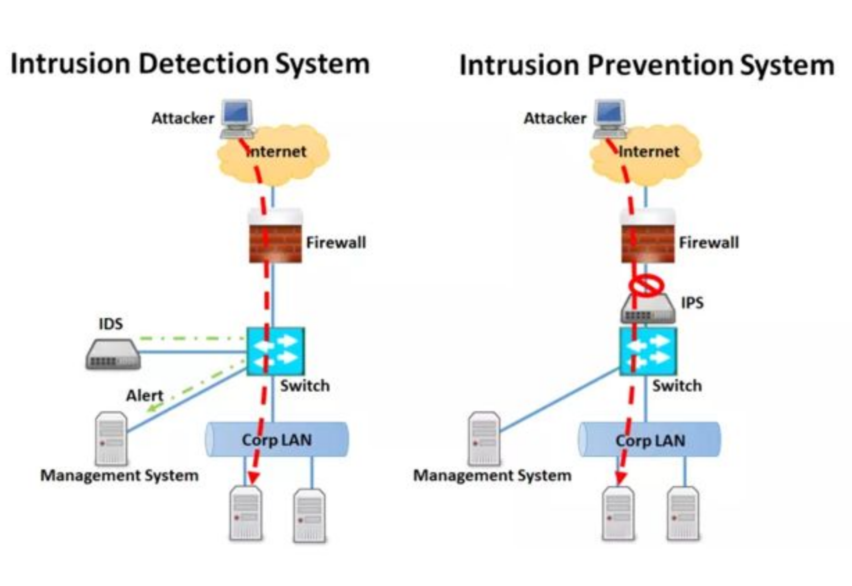
IDS - Intrusion Detection System
IPS - Intrusion Prevention System

2 different systems for the same threats

IDS systems are used to detect/alert intrusions, rather than remediate or prevent them.
- sits sideline

IPS systems are used to prevent system intrusions, and don’t always require human intervention.
- sits in line

Both should be used with a firewall, SIEM, UTM, etc., and never by themselves



So... Why do you need an IDS/IPS?

Automation

- Less man hours = More $$$

Policy Reinforcement

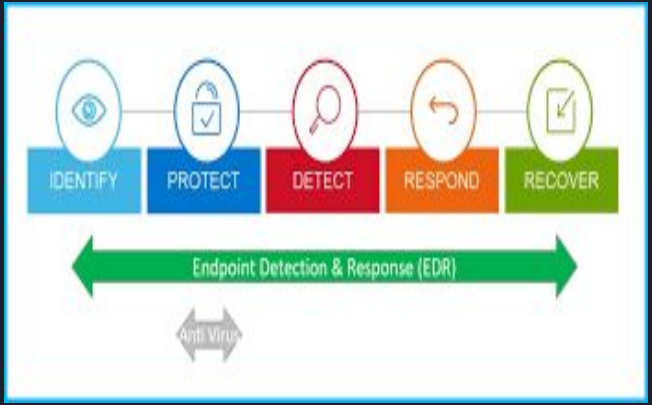
- Being automated logs will be consistent and will reinforce:
    - Company Policies
    - Security Regulations

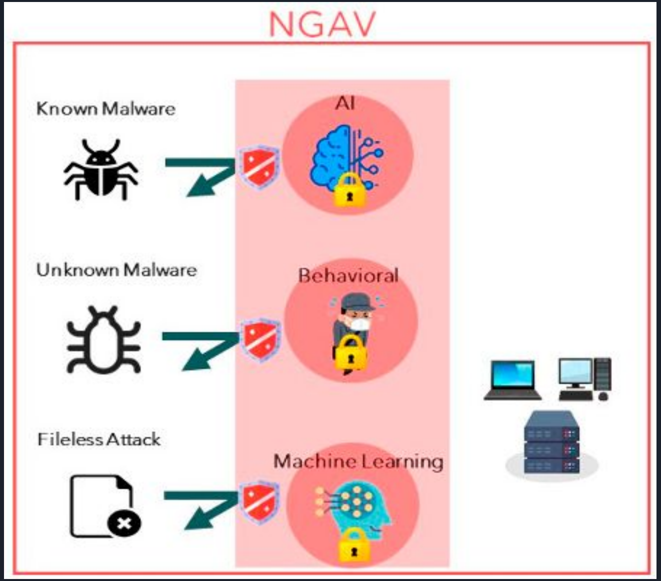
In the event of an attack,

- Logs are automatically kept
- Decreases time to react, potentially saving more $$$

EPP (EDR and NGAV)

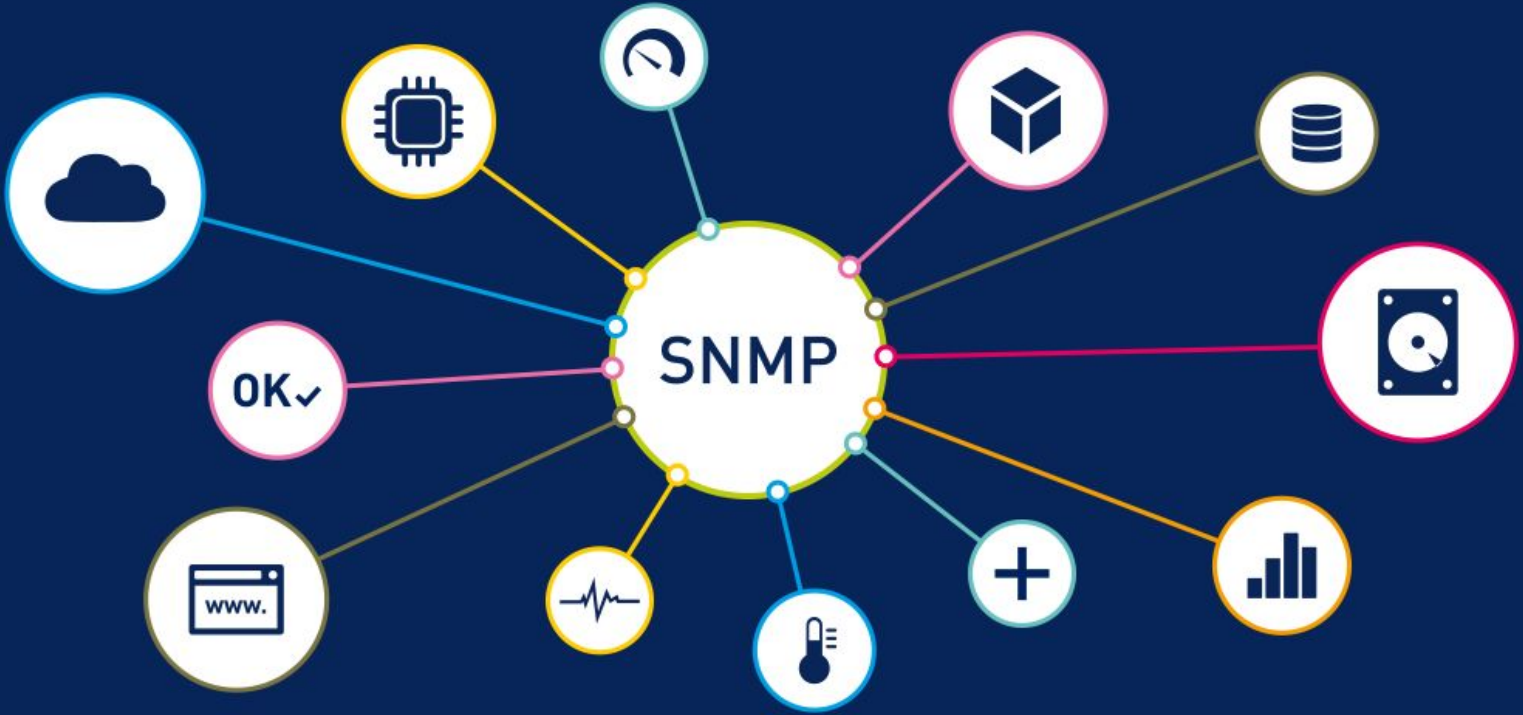
- What is an EPP?
  - Endpoint Protection Platform is a solution deployed on endpoint devices to prevent malware-based attacks
- What is an EDR?
  - Endpoint Detection & Response is a foundational element within an EPP
- What is NGAV
  - Next-Generation Antivirus uses AI to learn from previou threats to anticipate and prevent future attacks





SNMP Monitor

- What is it?
  - Can be used to collect information from all your networked devices
    - Collects data related to network changes
    - Determine status of network-connected devices
- What does it do?
  - Collect and analyze SNMP data
    - Status, performance and usage
- How can it help with my investigation?
  - Collects information from your entire fleet of network devices


SNMP
OK✓
www.