Security Signals

Three categories, focused on how different tools and systems generate, triage, and alert based on security signals:

1. Things That Create Signals

These are **systems and tools designed to generate raw data or signals that could indicate potential security incidents.** They monitor network traffic, system activity, or user behavior to detect anomalies, threats, or suspicious activity.

- **Honeypots**: Honeypots are decoy systems set up to attract and detect attackers. They mimic real systems and services to trick attackers into interacting with them. When attackers engage with a honeypot, it generates alerts and logs that provide insights into their tactics and techniques, creating valuable signals for further analysis.
- **Snort**: Snort is an open-source intrusion detection system (IDS) and intrusion prevention system (IPS). It inspects network traffic in real time and uses predefined rules to detect potential threats. Snort generates signals (alerts or logs) when it detects suspicious traffic, such as a known attack signature or abnormal behavior.

These tools create raw signals that form the basis for further analysis by triage systems.

2. Things That Triage Signals:

Triage tools collect, correlate, and prioritize signals from multiple sources to identify which ones need immediate attention. These systems help security teams manage the vast amount of data generated by security tools and focus on the most critical threats.

- **SIEM (Security Information and Event Management)**: A SIEM, like Splunk, collects and aggregates logs and security data from various sources across the network (e.g., honeypots, IDS/IPS systems, firewalls). **SIEMs perform real-time analysis and correlation of events to detect potential incidents.** They prioritize alerts based on severity, risk, and context, enabling security teams to investigate the most important ones.
- Example:
    - Splunk: Splunk collects and analyzes log data from various sources and uses its search and reporting features to identify patterns, anomalies, and potential threats. It helps triage large volumes of data into actionable alerts.

The triage process **helps filter out false positives and ensures that only relevant security events are escalated for further action.**

3. Things That Will Alert a Human:

These tools and systems take the signals that have been triaged and **notify human analysts about potential threats.** They often employ automation, machine learning, and other techniques to reduce the burden on security teams.

- Automatic Triage and Machine Learning: **Machine learning models can be applied to the collated logs and signals to automatically triage and detect patterns that might not be visible to rule-**

based systems. These systems help **reduce false positives and flag suspicious activity** that warrants human investigation. For example, machine learning might help detect anomalous login patterns, suspicious behavior, or previously unseen attack vectors.

- These systems are designed to prioritize critical alerts and **reduce "noise,"** making it easier for security analysts to focus on genuine threats.
- Notifications and Analyst Fatigue: Continuous alerts can lead to alert fatigue, where security analysts become overwhelmed by the volume of notifications, potentially leading to missed threats. Modern systems aim to **minimize this by filtering irrelevant alerts and only notifying analysts when a true threat is suspected.**
- Systems That Help Analysts Decide: Tools that combine machine learning, context from threat intelligence, and past incident data **help security teams quickly decide whether an alert represents an actual hack or a false positive.** These systems often provide additional context, such as related events, indicators of compromise (IOCs), or historical patterns, to help analysts make informed decisions.

Summary:

1. Things that create signals: Tools like honeypots and Snort generate raw security signals by monitoring traffic and user behavior.
2. Things that triage signals: Systems like SIEMs (e.g., Splunk) aggregate and prioritize these signals, correlating them with other events to focus on the most significant threats.
3. Things that alert a human: Tools that use automatic triage, machine learning, and smart notification systems alert human analysts only when there's a high probability of an actual threat, reducing alert fatigue and making it easier to decide if an alert is a real attack.