Open Threat Hunting Framework Analysis Techniques

# Analysis

# Technique: Stacking

Technique: Stack Counting

Stacking is when a data set of similar or equal values is inspected by an investigator with the hope of finding similarities within the information provided. Sometimes a noticeable variance completely out of range for a particular metric is detected, which gives investigators a clue as to what could be producing such results.

One example might be a search for outgoing traffic on a specific port, executed from a particular host name. If you were to filter this information, you would end up with a stack of data specific to that query, helping you to quickly analyze the required data that you were after.

# Technique: Enrichment

The process of data enrichment adds event and non-event contextual information to security event data in order to transform raw data into meaningful insights. Security events can enriched with contextual information from threat intelligence sources, reputation sources, asset inventory, geo-location tools, etc.

Enriched data allows an analyst to better perform threat detection, threat hunting, and incident response.

Threat detection is significantly enhanced by using real time enrichment. Threat intelligence context can be used to enhance detection analytics, improving the analyst’s ability to identify threats. It can also be used to increase a threat’s risk score, prioritizing higher risk threats for investigation.

In threat hunting and incident response the additional context provided through enrichment allows for quick investigation and action.

For example, additional context from a threat intelligence feed might identify an executable name as a known malicious binary.

Another example would be utilizing endpoint mission. By being able to identify the mission or criticality of systems (such as servers, workstations, domain controllers, and exchange servers), an analyst can prioritize investigating threats to critical assets.

In each of these scenarios context plays a key role in improving signal to noise ratio and triaging threats.

The typical contextual information used for security data enrichment includes:

1. Threat intelligence feeds
2. Reputation feeds
3. System mission info
4. Network locations and geo-location (such as internal network classification for cross border analytics)

# Technique: Grouping

Grouping is another method commonly employed by threat hunters, and it usually involves the use of multiple unique artifacts: running them through a series of elimination filters and seeing which ones appear together. This is useful, because seemingly-unrelated artifacts have the potential to be grouped together, giving the analyst a clue as to their relation to one another and to the possibility that there is interoperability between them. This would suggest that some sort of threat could be at work and provides good clues for investigators to work with.

Grouping can be thought of as a separate step after clustering, as it uses an implicit set of search criteria against a data set that is already suspicious and of interest to the investigator.

# Technique: Keyword Searching

This is the first avenue that most threat hunters will start at, and by the name it is quite obvious why: you need to find a threat and searching is the best way to do that.

The process entails the use of specialized queries that return results and artifacts. Because of the speculative nature of threat hunting, it is not always possible to know exactly what you are looking for when you start searching for threats. For this reason, it is important to not make your searches too broad, encompassing too many factors and receiving too many results. By contrast, making your search too narrow is also not ideal; you will miss out on potential threats that you did not include in the search.

Security professionals that engage in threat hunting activities need to analyze a lot of data, so knowing where to search is essential. But before any searching can start, evidence of some kind of threat must be apparent to some degree. Without this, it is impossible for an analyst to make any reasonable determinations about where to begin their search. Environmental data must be generated in order for any meaningful searching to be accomplished.

# Technique: IOC Searching

Indicators of Compromise (IOC) indicators include (but are not limited to) IP addresses, domain names, file names or file hashes. IOC Sweeping is the process of searching a data set for matches for IOCs to quickly identify data associated with malware or threat actors.