I am looking to build out a small section of technical overview on the topic of: Threat Hunting. Subsections should include: What is Threat Hunting? Why Companies Use Threat Hunting Threat Hunting Techniques Threat Hunting Tools Threat Hunting Platforms Training for Threat Hunting Shortcomings of Threat Hunting Solutions The content should be written without voice, be agnostic and informative providing useful links and references to any factual claims. 1,500 words.

What is Threat Hunting?

Threat hunting is the process of searching for cyber-attacks before they can successfully implement an attack. It is an advanced process that takes place in the early stages of threat detection and is used to identify advanced persistent cyber threats at the earliest possible phase of an attack by exploring the inner workings of a network for signs that it has been compromised. It employs the proactive measures that combine human instinct and analysis with analytics, threat intelligence and security tools to stop attacks before they are well executed or have gotten too deep. While the concept of threat hunting is not new, security operation centers of enterprises are increasingly prioritizing programmable threat hunting in their cybersecurity strategies in response to attackers' improving ability to circumvent traditional detection methods.

A hypothesis is usually the starting point of the threat hunting process. The hypothesis suggests that there are embedded attackers in a network that are actively working to cause damage. The formation of the hypothesis that a concealed threat exists in a system is spurred by a risk assessment, external intelligence, security alerts or by some other indication of anomalous activity. It is not unusual for attackers to be working covertly inside a network for weeks or months readying and executing attacks while going unobserved by the network's automated defense mechanisms. The threat hunting process explores and tests the hypothesis using analytical, investigative or preemptive exercises looking for undetected latent threats.

In order to achieve an optimal level of detection in the threat hunting process that includes the continuous monitoring of daily network activities and traffic and a successful investigation, certain components have to be in place:

- Methodology
- Technology
- Personnel
- Threat intelligence

Why Companies Use Threat Hunting

Threat hunting is being used by a growing number of enterprises to search for potential advanced security threats, instead of waiting for attackers to set off alarms after a network has been compromised. There are multiple reasons why the enterprises consider threat hunting a necessary aspect of a efficient cybersecurity strategy:

- **Intrusion prevention is not always successful.** Attackers are increasingly employing stealthy methods to ensure that the malware they create can avoid detection.
- **Attacks are evolving quickly.** Threat hunting is necessary because attackers, or the methods they use, and the networks are always evolving, and in order to provide proper network security, it is necessary to be cognizant of these changes as soon as they occur. Modern cyber threats are multifaceted and complicated and require that security analysts employ dynamic hunting techniques in order to contain them.
- **Being proactive is a necessity.** According to a poll of security options centers, 44 percent of the respondents estimated the financial ramification of a single undetected data breach resulted in a loss of more than half a million dollars. It is not feasible for enterprises to become aware of and respond to

a network security breach days or weeks after it has occurred. In order to limit the financial damage cyber threats can cause, enterprises have to actively hunt for them.

There are also a number of benefits enterprise can derive from threat hunting. Security operation centers that were surveyed report that that the main threat hunting benefits include:

- Enhanced detection of advanced persistent threats (64 percent)
- A reduction in investigation time (63 percent)
- Time saved by use of machine learning to correlate events (59 percent)

Threat Hunting Techniques

Searching and Cross-Source Correlation. A process that involves utilizing specialized queries with specifically defined search criteria. Without this technique, determining what should be searched can be difficult. The searches should be too broad, encompass an excessive number of factors or result in too many searches. The searches also cannot be too narrow, as they would exclude possible threats.

Lookup. Lookup technique entails determining the origin of network indicators, such as IP addresses or names. Specifically, it determines the owner of the indicator, how long that owner had the indicator and for what purposes. There are several types of attribution searches that can be conducted. The most typical searches include geolocations, WHOIS lookups, reverse lookups and ASN lookups. Lookup can be difficult to implement and the results can sometimes be uncertain.

Clustering/Cluster Analysis. This is a statistical technique that uses artificial intelligence to produce correlations within arrays of records, log files and other types of data obtained from threat hunting investigations. Groups or clusters of similar data points are separated into groups using certain characteristics selected out of a larger data set. The amount of data involved requires the use of the machine learning-based cluster analysis, as it would be complicated and time-consuming for humans to assemble.

Stack Counting. Stacking counting is the most straightforward tool for highlighting outliers in sets of data. In order to identify similarities with a set of data or equal or similar values, the data undergoes inspection. The technique entails obtaining a count of all of the elements in all of the categories and then ordering them in order to identify outliers.

Grouping. Grouping entails determining when multiple artifacts out of a set of unique artifacts appear together when certain criteria is applied. Identifying the specific criteria to apply to group the items is a key aspect of this technique.

Threat Hunting Tools

A significant part of the threat hunting process is automated through software. There are additional software tools that threat hunters use to sift through and closely examine the substantial amount of data used in the threat hunting:

- **Data logs.** Typical sources of data may include antivirus longs, endpoint logs, operating system event logs and firewall logs.

- **SIEM systems.** A centralized security information and event management system is used to efficiently correlate log data. SIEM systems are used to form correlations and links from individuals instances of data in order to determine the actual threat.
- **Sources of threat intelligence.** Threat intelligence sources provide information about new, emerging threats and the techniques that attackers are using to breach a network. Specific details are also provided, such as which IP addresses are malicious.
- **Analytics.** Analytics-driven threat hunting tools employ machine learning and behavior analytics to generate hypotheses and risk scores.
- **Security monitoring tools.** Antivirus software, data loss prevention systems and other traditional security products are used to reveal the signs that a network has been compromised.

Threat Hunting Platforms

Threat hunting platforms are software solutions that are able to use threat intelligence in conjunction with machine-learning methodologies to automate much of the threat hunting process. They gather threat intelligence, typically from multiple feeds, and create threat analysis reports. The platforms provide security operation centers with the tools necessary limit dwell time, detect threats earlier and enhance the defenses of a network in preparation for subsequent attacks.

Enterprises are able to integrate a wide range of technologies in threat hunting platforms, using them to improve the accuracy, scope and speed of threat detection and remediation. The top technologies security professionals prefer to have incorporated into their threat hunting platforms include incident response, SIEM, ticket systems and Active Directory.

Training for Threat Hunting

Threat hunting is an advanced process. A practitioner of threat hunting has to have a combination of certain skills related to intelligence analysis, information security, statistics, visualization and forensic science. These skills are necessary to engage in an effective and proactive discovery of threats and to immediately conduct effective investigations:

- Statistical knowledge to interpret the significance of complex statistical data
- The ability to theorize attack and the resultant impact on the enterprise
- Deep contextual understanding of the enterprise and its IT environment
- Investigative ability to determine the origin of an attack and construct an accurate timeline of events using endpoint and network forensic

These skills can be obtained through IT security training programs. These programs, many of which are based online, typically examine the key principles of risk management and network security. They also provide opportunities for participants to conduct threat analysis and to take the appropriate responsive actions. Participants may take courses that demonstrate how to:

- Cultivate critical threat intelligence sources
- Determine when and how a breach has occurred
- Conduct damage assessments to determine which systems have been compromised
- Restrict and remediate attacks
- Use the knowledge of threats to pursue additional breaches

After successfully completing one of these programs, the participants may obtain a certification in threat hunting.

Shortcomings of Threat Hunting Solutions

The use of threat intelligence without context. Threat intelligence is an important factor in the use of threat hunting platforms. However, issues can arise if the threat intelligence is obtained from an excessive number of feeds and sources with without sufficient context. This can result in security analysts being bombarded with false positives.

Limited quality data. The data that is used in the threat hunting process has already been compromised by the incident that is being investigated.

Requires highly skilled personnel. The lack of highly skilled workers who are properly trained is one of the barriers enterprises face when implementing trying to implement threat hunting. Hiring experienced threat hunters can be difficult, which can result in existing personnel being compelled to engage in threat hunting with their other work tasks.