cybereason

Threat Hunting: Answering "Am I Under Attack?"

With every vendor offering some type of threat hunting service, security professionals may wonder if hunting can actually benefit a company or if it's just a fad. But threat hunting isn't based on flashy technology that will become irrelevant in a few months. It's a return to one of the basic tenets of information security: reviewing your IT environment for signs of malicious activity and operational deficiencies. With hunting, you can answer the question, "Am I under attack?"

Threat hunting presents a proactive approach to security

Traditional defenses can't keep up with new attacker techniques, leaving companies vulnerable to hacks. Even if the good guys could match their adversaries' offensive measures, there would still be times when their defenses would fail. Inevitably, an employee will click on malicious link in an email or visit a dicey website or a firewall will be improperly installed.

Unlike traditional, reactive approaches to detection, hunting is proactive. With hunting, security professionals don't wait to take action until they've received a security alert or, even worse, suffer a data breach. Instead, hunting entails looking for opponents who are already in your environment. Hunting leads to discovering undesirable activity in your environment and using this information to improve your security posture. These discoveries happen on the security team's terms, not the attacker's. Rather than launching an investigation after receiving an alert, security teams can hunt for threats when their environment is calm instead of in the midst of the chaos that follows after a breach is detected.

Threat hunting can help security teams defeat advanced adversaries by:

Elevating threat detection beyond IOCs

With attackers growing increasingly sophisticated, detection using indicators of compromise is no longer an effective way to determine if an organization is being attacked. Changing IOCs, whether it's an IP address or a malware signature, is an incredibly easy task for attackers and allows them to make an old threat new again and capable of getting past traditional security products like firewalls and antivirus.

Identifying malware-free and fileless malware attacks

Attackers are turning to legitimate administration tools including PowerShell, Windows Management Instrumentation (WMI) and Remote Desktop Protocol to help them carry out fileless malware attacks. Malicious code is being injected into valid applications to evade legacy blacklisting and detection technologies and scheduled tasks are being used for lateral movement.

Discovering deficiencies that could help attackers

Undesirable activity doesn't necessarily mean malicious activity. However, these activities can potentially become security problems in the future. Pointing out these activities before they lead to a security incident gives defenders a better understanding of the possible weaknesses in their environment and the opportunity to harden them.

For instance, a health-care organization used a threat hunt to discredit assumptions about its IT and security environments. The company's CISO prohibited employees from using FTP under the assumption that this would keep the company safe. His logic: banning FTP eliminated the possibility that attackers could use ftp.exe for data exfiltration.

But a hunting exercise revealed that despite the ban, some employees were using FTP. In fact, approximately 50GB of data was leaving the company every day. Had the company not engaged in a threat hunt, it would have never gained visibility into its IT environment and continued to operate under false assumptions that could have potentially jeopardize its security.

Threat hunts can also be used for preemptive defense. If banks are being targeted by attackers, for instance, a financial services company, assuming that it could be the next victim, could use a threat hunt to figure out how to bolster its defenses.

Providing peace of mind

Threat hunts aren't just for discovering a breach and seeing if the bad guys are in your environment. For example, if an enterprise is using a managed security service provider (MSSP) to run its day-to-day security operation, a threat hunt could be used to audit the MSSP's work and determine if the service provider missed any security incidents.

A new CISO could use a threat hunting engagement to take stock of the security team's people, processes and technologies.

Threat hunts can also be used for conducting security due diligence before a merger is finalized. A threat hunt can be used to evaluate the security posture of the company that's being acquired and identify any deficiencies or breaches. This could save the business that's making the purchase from having to deal with the fallout surrounding a data breach or security incident.

How to Conduct a Hunt

Decide on internal vs. outsourced

If you decide to conduct a threat hunting exercise, you first need to decide whether to use your internal security team or outsource it to an external threat hunting service provider. Some organizations have skilled security talent that can lead a threat hunt session. To enable a proper exercise, they should solely work on the hunting assignment for the span of the operation, equipping them to solely focus on this task.

In most cases, security teams are unable to dedicate the time and resources required for hunting, and should therefore consider hiring an external hunting team for this purpose. You can learn about Cybereason Hunting Services here.

Begin with proper planning

Whether using an internal or external vendor, the best hunting engagements start with proper planning. Putting together a process for how to conduct the hunt yields the most value. Treating hunting as an ad hoc activity won't produce effective results. Proper planning can assure that the hunt will not interfere with an organization's daily work routines.

Select a topic to examine

Next, security teams need a security topic to examine. The aim should be to either confirm or deny that a certain activity is happening in their environment. For instance, security teams may want to see if they're targeted by advanced threats, using tools like fileless malware, to evade the organization's current security setup.

Develop and test a hypothesis

The analysts then establish a hypothesis by determining the outcomes they expect from the hunt. In the fileless malware example, the purpose of the hunt is to find hackers who are carrying out attacks by using tools like PowerShell and WMI.

Collecting every PowerShell processes in the environment would overwhelm the analysts with data and prevent them from finding any meaningful information. They need to develop a smart approach to testing the hypothesis without reviewing each and every event.

Let's say the analysts know that only a few desktop and server administrators use PowerShell for their daily operations. Since the scripting language isn't widely used throughout the company, the analysts executing the hunt can assume to only see limited use of PowerShell. Extensive PowerShell use may indicate malicious activity. One possible approach to testing the hunt's hypothesis would be to measure the level of PowerShell use as an indicator of potentially malicious activity.

Collect information

To review PowerShell activity, analysts would need network information, which can be obtained by reviewing network logs, and endpoint data, which is found in database logs, server logs or Windows event logs.

To figure out what PowerShell use looks like in a specific environment, the analyst will collect data including process names, command line files, DNS queries, destination IP addresses and digital signatures. This information will allow the hunting team to build a picture of relationships across different data types and look for connections.

Organize the data

Once that data has been compiled, analysts need to determine what tools they're going to use to organize and analyze this information. Options include the reporting tools in a SIEM, purchasing analytical tools or using Excel to create pivot tables and sort data. With the data organized, analysts should be able to pick out trends in their environment. In the example reviewing a company's PowerShell use, they could convert event logs into CSV files and uploaded them to an endpoint analytics tool.

Automate routine tasks

Discussions about automation may turn off some security analysts. However, automating some tasks is key for hunting teams' success. There are some repetitive tasks that analysts will want to automate, and some queries that are better searched and analyzed by automated tools.

The Cybereason platform, for example, automates threat hunting by using an in-memory graph that collects information, in real time, from all endpoints and servers and asks millions of questions every second to identify malicious behavior. This spares analysts from the tedious task of manually querying the reams of network and endpoint data they've amassed. For example, Cybereason automates the search for tools that use DGAs (domain generation algorithms) to hide their command and control communication. While an analyst could manually dig through DNS logs and build data stacks, this process is time consuming and error-prone.

Get your question answered and plan a course of action

Analysts should now have enough information to answer their hypothesis, know what's happening in their environment and take action. If a breach is detected, the incident response team should take over and remediate the issue. If any vulnerabilities are found, the security team should resolve them.

Continuing with the PowerShell example, let's assume that malicious PowerShell activity was detected. In addition to alerting the incident response team, security teams or IT administrators should change the Group Policy Object settings in Windows to prevent PowerShell scripts from executing.

Threat hunting lets defenders take immediate action against the adversary

While security professionals can't plan for every scenario that could potentially lead to a data breach, they can proactively look for signs that indicate something is wrong in their environment and take immediate action. Adversaries aren't invisible and do leave patterns of behavior in the networks they've infiltrated. Threat hunting allows defenders to discover those behavior patterns and stop adversaries before they cause additional damage.

About Cybereason

Cybereason is the leader in endpoint protection, offering endpoint detection and response, next-generation antivirus, and managed monitoring services. Founded by elite intelligence professionals born and bred in offense-first hunting, Cybereason gives enterprises the upper hand over cyber adversaries. The Cybereason platform is powered by a custom-built in-memory graph, the only truly automated hunting engine anywhere. It detects behavioral patterns across every endpoint and surfaces malicious operations in an exceptionally user-friendly interface. Cybereason is privately held and headquartered in Boston with offices in London, Tel Aviv, and Tokyo.

cybereason