The IR Boost: How Threat Hunting Enhances Incident Response

Whether it's referred to as threat hunting or hunt teaming, companies are increasingly taking a proactive approach to security by looking for evidence of threats that are already in their environments. Organizations have realized that waiting for antivirus, SIEMs and other security solutions to trigger an alert is not a practical approach to detecting sophisticated and stealthy adversaries since they know how to evade these tools. Hunting enables security teams to proactively answer the question "Am I under attack?"

An often overlooked benefit of threat hunting is how it aids incident response teams. To show what's possible when the two are used together, in this white paper we'll present several examples that demonstrate how threat hunting boosts incident response efforts.

Marrying threat hunting and incident response

In our whitepaper Threat Hunting: Answering “Am I Under Attack?” we explained that a hunting engagement starts with a security team presenting a hypothesis. Trying to identify the blind spots in a company’s security plan can serve as the hypothesis for a hunt, for example. A more basic and direct question for security professionals to ask is, “What do we suck at doing?” and use the answer as motivation for a hunt.

Take the perennial phishing email, which still manages to slip past even the best email filters. Let’s assume your organization is getting slammed with them, causing your security team to fear that a nasty security incident could be a few clicks away. Use a hunt to learn what kinds of documents are attached to the emails. Word Documents with malicious Visual Basic for Applications macros are a common way for attackers to spread malware. The hunt could reveal that 77 percent of the emails received by the organization contain Word documents. Out of that 77 percent, 22 percent contain Visual Basic for Applications macros. The question then becomes what’s the likelihood that your company will get hit by malware that uses Visual Basic script as a delivery method?

The hunt could show that only 0.5 percent of the attached Word documents are used for valid business purposes. This information could motivate the IT and security departments to find ways for people to complete their jobs without using Word documents or using them as infrequently as possible, reducing the attacker’s potential footprint.

Respond to incidents faster

When the incident response team is called in to handle a security incident unearthed during a hunt, they’ll be better equipped to handle the situation since a significant amount of scoping and triaging was completed during the hunt. Your organization’s hunters have analyzed the data they collected. They grasp the problem, know what machines are affected and understand the incident impact. All of this information is passed along to the incident response team. With the some of the preliminary work done, incident response team will have less work to do and can remediate the threat quicker.

How to use threat hunting to detect advanced attacks

A hunt is probably the best approach to deal with attacks that use advanced threats like fileless malware or PowerShell. Fileless techniques are becoming the bad guys' preferred attack vector since this method uses legitimate programs to mask malicious behavior and evade detection by most security tools.

Let's say a hunt at a large manufacturing company revealed all kind of suspicious activities. The hunting teams spotted a service named TCP/IP NetBIOS Helper with a command line argument showing PowerShell with bypass hidden calling off regular named ps file, a tactic used to maintain persistence in an environment. There's data exfiltration using PowerShell where files are uploaded to a remote location through your proxy. The hunt also looked at how PowerShell performed DNS queries by doing data stacking between process execution and DNS requests. This revealed that PowerShell was establishing a network connection to the Internet. The question then became what outside addresses were being talked to; was PowerShell making DNS queries to domains that the company didn't own.

So what happens after the hunting team identifies these activities? First, they need to be escalated to the level of an incident since there's proof that malicious activity is occurring in the environment.

Then, the information from the hunt can be used to establish an intelligent prevention program. For example, if the hunting team discovers that 99 percent of PowerShell activity in the company occurs on servers and the remaining one percent is on clients and it's all malicious, PowerShell could be blocked on end user systems, especially if they're not being used for administrative purposes.

Or use the application control capabilities in your company's antivirus software to prevent browsers from spawning PowerShell or Windows Management Instrumentation from spawning PowerShell. If you use PowerShell scripts in your server environment and not in your client environment, anchor those scripts to a specific directory and then sign them so that you only run signed PowerShell scripts from a specific location. This builds resiliency into the environment.

Following this approach allows hunting to strengthen the organization's security posture while slowing down the adversary and decreasing their dwell time. The results of a hunt can be used to build new prevention mechanisms, ensuring that the discovered security incidents do not happen again.

About Cybereason

Cybereason is the leader in endpoint protection, offering endpoint detection and response, next-generation antivirus, and managed monitoring services. 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.