Guide

Bitdefender®

Cyber Threat Hunting Guide

What is Cyber Threat Hunting?

Like 'AI', 'machine learning', or 'actionable intelligence', '**Cyber Threat Hunting**' has become an industry buzzword that is used in multiple contexts and now has no clear definition. But understanding how to hunt across an environment requires that we must first understand exactly what Cyber Threat Hunting is.

Threat hunting is the practice of proactively searching for cyber threats that are prowling unnoticed in a network and digs deeper to identify adversaries in an environment that may have slipped past initial endpoint security defenses.

Bitdefender Threat Hunting Definition

Deliberate process using contextualized data designed to define potential cyber threat and proactively seek them out within an environment.

Understand your adversaries

Even in today's climate, with cyber security so prominent in the news, the number of successful breaches is continuing to climb and taking a proactive approach to detect them will help maintain a secure network. Security analysts cannot just sit around and wait for an automated alert to notify them of a breach. Actively seeking out potentially malicious behavior on your network will help maintain a more secure position against adversaries.

Adversaries are extremely skilled at obtaining access and experts at going unnoticed; and it is not uncommon for an organization to be unaware of an intrusion for days, weeks, or even months. Before you can begin threat hunting, you must first understand the adversaries you will be facing. Their techniques may be similar, however the motivation behind each can be very different.

If you can determine who would want to do harm and what you have that is valuable to them, you can be better prepared to protect the business. Searching for adversaries that successfully get around tooling requires a clear understanding of what normal looks like. Normal for users, normal for systems and normal for networks. Baselining an environment is a key to being able to understand who may attack. Understanding how the physical connectivity, normal network utilization, protocol usage, peak network utilization and average throughput of the network will help you determine when something doesn't appear to be normal. Adversaries/hackers are people and in order to effectively hunt for threats, you need to think like they do by understanding the tricks and techniques that are frequently used. Unfortunately, cybercriminals don't follow a specific play book. There isn't a single process or simple path of execution when executing an attack. Nor is there an exact way for detecting that attack. Nonetheless, it's useful to understand how a typical attack unfolds. Keep in mind that hackers/adversaries can skip, add and even backtrack steps.

Author:
Joshua Armstrong - Cybersecurity Team Lead

Bitdefender Cybersecurity Team Lead, Joshua Armstrong, has over 10 year of experience in cutting-edge technology and cybersecurity. He leads his team in managing projects to work efficiently in a dynamic environment with demanding deadlines and provides technical support and guidance to facilitate the identification of network intrusions and malicious activities. He is an experienced professional in the cybersecurity field and thrives at managing complex programs that have far-reaching implications for customers. Josh is based in San Antonio, Texas and in his free time he enjoys traveling, competitive sports and refining his BBQ skills on the grill!

The steps of a cyberattack

There is a progression involved when dealing with a cyberattack. Research, Penetrate, Expand and Exploit are the steps in a typical cyberattack.

1. Research

The progression of a typical cyberattack starts first with Research. Before launching an attack, cybercriminals try to gather as much publicly available information about the organization and its network as possible. This is the same concept for a thief when he/she wants to take that brand-new high def flat screen TV on your wall at home, they are going to do some research. This thief will potentially try and figure out everything they can that will help them successfully get that TV, for example knowing your schedule, knowing your house layout, does it have an alarm, do you have animals, security cameras, etc.... Just like a thief trying to get your TV, some of the things a cybercriminal goes after can include network ranges, IP addresses, and domain/host names. Part of the reconnaissance/research may include looking for email addresses of key players in the organization like Managers, IT Staff, C-level employees. The adversary can leverage these people to launch a phishing attack during the exploit phase.

2. Penetrate

Second the adversary will attempt to penetrate the network. Once the attacker has gathered the information they need, now they are ready to engage with the proposed target and sabotage the perimeter defenses. Typically, this is achieved through a phishing attack or another common attack vector like malware, domain shadowing, malvertising, denial-of-service and drive-by-downloads. Adversaries also can utilize other tools to gain entry. These include vulnerability exploitation tools, traffic monitoring tools, port scanners, encryption tools and password crackers.

3. Expand

Third the expand phase: Now that the adversary has gained entry, they will utilize a technique called pivoting, where they use a compromised device to access other devices that would not otherwise be accessible. This lateral movement enhances transparency into available network assets in order to obtain high-value, sensitive information. Various procedures are deployed to escalate privileges and gain system administrator credentials.

4. Exploit

Once the attacker finds what they are looking for, they take the final steps to achieve their goal, with the Exploit phase. Successful outcomes can include the following: gaining administrative access, opening command and control communications, achieving persistence, exfiltrating data, destroying data, denying access to systems and covering their tracks.

How does Threat Hunting help?

Threat Hunting is a bit focused on the “Expand” and “Exploit” phase as hunting typically will not find 0 days. While an adversary is in the expand phase knowing how to hunt across an environment, it will help knowing where an adversary may pivot to and at least it will help determine where the attacker currently is at.

When hunting, you would want to start with how the adversary entered, and hunt around this to identify the adversary's capabilities and what they are after. Better than waiting for a known adversary, become the adversary mentally and attempt to pivot your way through a network. This will notify you of the known capabilities of movement and even the unknown. The unknown can sometimes be more important because this forces you to dig deeper into the network so that you can better improve security of the environment. Utilizing the data from an exploit gives you another avenue of hunting.

The goal of hunting obviously is to attempt to stop an adversary before they can get data exploited. However sometimes, with all the hunting and analysis, the bad guy finds a way. When they do, a skilled security analyst will take this data and utilize it to hunt over the entire environment in order to try and eliminate the issue from happening moving forward. This may even provide more information/ideas to hunt over other environments if you support multiple customers.

What do you need to start threat hunting?

Before you start, it's imperative to ensure that your organization is ready to threat hunt. You should have a mature security setup capable of ingesting multiple sources of information and storing it in a way that lets you access it. A basic set up should include automated blocking and monitoring tools such as firewalls, antivirus, endpoint management, network packet capture, and security information and event management (SIEM). You will also need access to threat intelligence resources so you can look up IP addresses, malware hashes, indicators of compromise (IoCs) and more.

Finally, you will need a tool that enables you to bring together your disparate data sets and slice and dice them in a way that exposes insights with the least possible effort. Threat hunting can involve a enormous amount of information, so while it is a human-led effort, you'll certainly need some computer assistance to make the task more manageable. Once you have all the tools in place and working together, you will also need a team with enough people to manage the technology and data.

Setting up a threat hunting team

Threat hunting leverages enterprise network traffic in a contextual setting in order to identify areas of concern at best, and compromise at worst; the process has proven itself to be very effective and is gaining momentum as companies look for better ways to increase their security posture and eradicate malware and persistent threats. As emerging and Advanced Persistent Threats (APT) continue to challenge analysts, they, in turn, continue to utilize threat-hunting platforms to uncover attacks. Cyberthreat Intelligence activities enable teams of analysts to focus their resources in order to achieve maximum effect, while they anticipate threat identification using a threat-hunting approach. It's a strategy which is shifting from reactive to proactive, as companies look for ways to deal with issues in a faster, more efficient way and to gather enough data to prevent further issues and build stronger defenses.

Finding the right set of skills

The industry is becoming aware that security is not a technology problem alone, it's a people problem too. Cyber Threat Hunting is a high skill, high maturity endeavor and while this is challenging in the midst of a debilitating global cyber skills shortage, it is a critical component of any security program if the 'Defenders' are going to start winning the cyber war.

What is Managed Threat Detection?

Because 100% detection is impossible to achieve, and since existing security measures and solutions like IDS and SIEM are simply not enough anymore, there is a growing need to establish security teams who will proactively “hunt” for threats targeting organizations.

However, that is not always an easy task, as demonstrated above because it requires a specific set of skills and capabilities. All these come with a high cost which might burden the business and even derail it from its main goals.

In such cases, investing in a managed threat detection service is the better option: timely and cost efficient for the business.

- Managed Detect and Respond teams have already found the talent and built their teams.
- Such operations have been designed to defend businesses in many industry verticals, who are at risk to every type of attack providing a more comprehensive Threat Hunting operation.
- The threat landscape is static, it evolves every day and security teams must keep up. This is a complex and resource-heavy endeavor, but MDR organizations are validating their operations every day, often at significant scale.

Bitdefender is a global security technology company that delivers solutions in more than 100 countries through a network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology, and is a leading security provider in virtualization and cloud technologies. Through R&D, alliances and partnership teams, Bitdefender has elevated the highest standards of security excellence in both its number-one-ranked technology and its strategic alliances with the world's leading virtualization and cloud technology providers.

More information is available at http://www.bitdefender.com/.

Bitdefender-Guide-GTHG-CREA4120-en_EN