Microsoft Security

MICROSOFT SECURITY EXPERTS

THREAT HUNTING SURVIVAL GUIDE

Table of Contents

Why Prepare

The benefits of proactive threat hunting

Like wilderness survival experts, threat hunters succeed because of impressive skills, an eagerness to learn and adapt, and vigilance to potential threats. Adversaries are getting more adept at sneaking into networks and lurking there without detection for weeks or even months as they gather information and escalate privileges. Human-operated attacks can seem as daunting as crossing an ice bridge over a 100-foot crevasse on a snow-covered mountain. However, successful threat hunters thrive rather than merely survive due to proactive preparation.

Benefits of proactive threat hunting

Proactive threat hunting is built around an "assume breach" mindset rather than a traditional approach of waiting for endpoint detection tools to identify potential threats. While the latter approach works for automated and well-known attacks, today's human-operated attacks are more complex. Proactive threat hunting helps to uncover hidden security threats that hide in your environment and discover vulnerabilities. Like wilderness survival expert training for rugged environments, modern threat hunters are harnessing their knowledge and resources to outthink attackers.

Be Proactive

Proactive threat hunting helps familiarize your team learn your environment better, making it easier to detect outliers. This enables you to identify opportunities for standardization, thus making it easier to detect suspicious activity in the future.

Gain Perspective

Threat hunters benefit significantly from having a "home field advantage". This advantage is multiplied when supplemented by perspective from hunters specializing in the threat landscape. Your knowledge of your enterprise paired with our knowledge of the threat landscape will help identify suspicious activity more rapidly.

Standardize

Modern cybersecurity is intrinsically complex and requires a data from a variety of sources, and everything looks like an anomaly without consistency. Standardizing your enterprise will make suspicious activity more apparent and increases the likelihood that you will detect suspicious activity earlier in an attack.

The ongoing security labor shortage has caused a national security risk. Until more roles are filled, today's cybersecurity professionals will be tasked with what may seem like an overwhelming responsibility. We created this threat hunting guide to help support these defenders. In this guide, we'll dive into how to identify if a human-operated attack has occurred and share strategies for proactive threat hunting and human-operated attack investigation. Guided by these survival strategies, you'll be able to assess potential threats you face and rapidly identify signs of a human-operated attack.

Identity attacks by the numbers

83

million identity-based attacks in a month in 2021

45%

of CISOs (Chief Information Security Officer) report an increase in phishing campaigns and identity fraud

4.9

billion attacker-driven sign-ins in one month alone

Source: Understanding identity theft protection and Cyber Signals: Identity is the New Background, Microsoft

HELPFUL RESOURCE: Understanding Identity Threat Protection Infographic

Modern Attacks

Why threat hunting must extend beyond endpoints

Surviving in the wild takes an understanding of dangers like weather, terrain, and predators, including knowing their activity patterns, methods of attack, and weaknesses. Threat hunters also are constantly mindful of threats and realize that an attack can happen anywhere, at any time, so they must understand those threats – and be agile enough to adapt whenever necessary.

Humans form the backbone of threat hunting. Perhaps not surprisingly, the most formidable threats are also often operated by humans. Understanding these attackers means developing a deep knowledge of the tactics, techniques, and procedures (TTPs) they use to access an organization's environment.

Extending your security visibility

Endpoint security matters and will continue to matter in perpetuity. In fact, the rise of human-operated attacks makes it even more important to bolster endpoint security. Malware continues to cause harm to the reputations and bottom lines of businesses of all sizes. Moving beyond endpoints-only is an evolution that can hugely benefit businesses. One strategy is for threat hunters to use extended detection and response (XDR).

HELPFUL RESOURCE: Modernizing security operations with XDR

What is XDR?

Extended detection and response, often abbreviated as XDR, is a fully integrated set of security tools that offers holistic, optimized security by integrating security products and data into simplified solutions. XDR combines prevention, detection, investigation, and response, providing visibility, analytics, correlated incident alerts, and automated responses to improve data security and combat threats.

A modern organization's cybersecurity assets span a variety of first-party and third-party networks, applications, cloud databases, mobile devices, and identities. The digital perimeter as it exists now is a dynamic and ever-evolving landscape.

What is Zero Trust?

Besides XDR, one of the best ways to move beyond endpoints is to follow the principles of Zero Trust. The main tenets of a Zero Trust philosophy are to authenticate and authorize access every time, limit user access to just what they need for what they're working on and assume breach by implementing end-to-end encryption verification and analytics in threat detection efforts.

A Zero Trust approach should extend throughout the entire digital estate and serve as an integrated security philosophy and end-to-end strategy. This is done by implementing Zero Trust controls and technologies across six foundational elements – Identity, Endpoints, Data, Apps, Infrastructure, and Network. Each of these is a source of signal, a control plane for enforcement, and a critical resource to be defended.

Top XDR use cases

- **Detect endpoint device vulnerabilities**
- **Hunt threats across domains**
- **Investigate cross-workload security events**
- **Ensure security posture across your digital estate**
- **Prevent future attacks**
- **Prioritize and correlate alerts**

Know the terrain

Commodity vs. human-operated malware

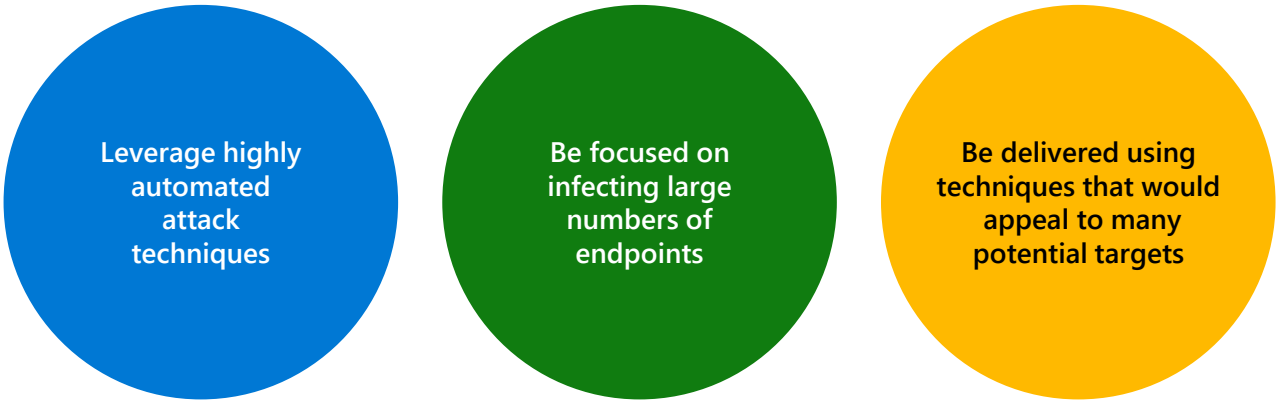
Successful wilderness survivalists aren't content to hide out in their shelter. Instead, they strap on their packs, lace up their hiking boots, and explore the terrain. Besides giving them potentially life-saving intelligence about predators in the area, they also learn the waterways, vegetation, and other unique characteristics of the land to help them thrive.

Threat hunters must trek the digital landscape and learn where attacks could occur. The two major types of attacks that hunters stay alert for are commodity malware and human-operated attacks.

Commodity malware attacks

Commodity malware attacks are the hazards you encounter every day as users click on the wrong link or install the wrong program. In these situations, much of the attack logic is contained within the malware, so remediation is typically as simple as removing the malware, rebuilding the device, and / or potentially resetting the user's credentials.

Commodity malware attacks are likely to target a broad audience and focus on infecting as many systems as possible. To achieve this, commodity malware is likely to:



Human-operated attacks

Human-operated attacks invest significantly more effort into the compromise of a specific target than commodity malware attacks. Once attackers gain a foothold within a system, they use their attack experience and motives to decide what to do at each stage based on what they find in their target's network. Because humans are behind these attacks, their impact – and the variety of techniques used – vary significantly.

Threat hunters must research to determine which systems and identities need to be remediated. Addressing such threats can feel like a chess game as attackers respond to each remediation attempt that does not completely evict them from the enterprise. Evicting a human-operated attack means eliminating any identities or devices they control and will require the vigilance of trained security staff paired with effective security products, and modern enterprise configuration.

These human-operated attacks are a big reason why companies upgrade to XDR from their existing Endpoint Detection and Response (EDR) solutions. XDR gives you that broad security view across the landscape.

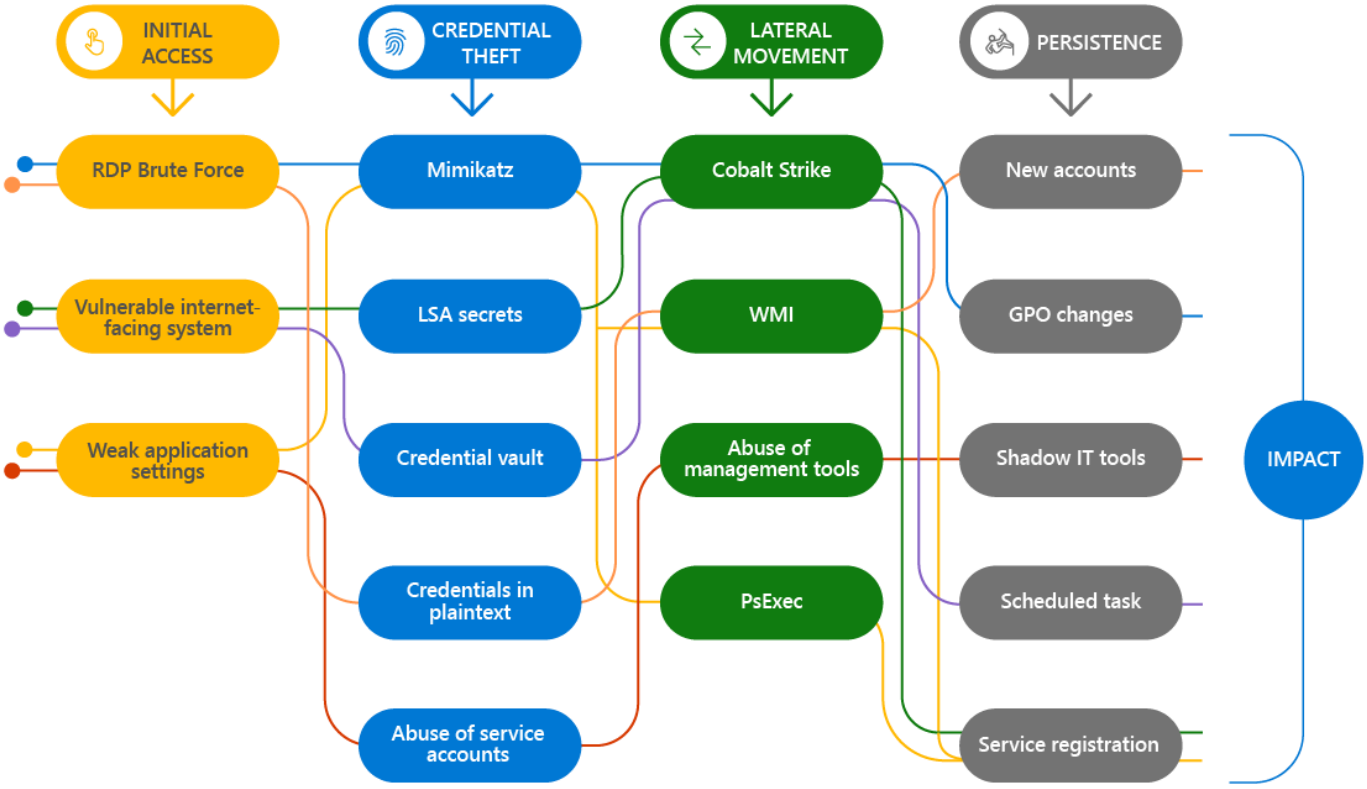
Human-operated attacks might:

- Focus on specific targets
- Evade specific organizational protections
- Use customized tools designed specifically for the target
- Abuse legitimate administrative tools to avoid detection

Understanding the human-operated attack pathway

Human adversaries can use a variety of techniques to achieve the same impact. These attack vectors may include malware, abuse of legitimate administration tools or capabilities, social engineering, software exploitation, or a variety of other techniques. The important thing to remember is that many of the steps involved in a human operated attack may appear like normal administration activity.

XDR enables an analyst to go beyond antimalware and other technologies that solely react to malicious activity, thus enabling a unified view of how identities, endpoints, e-mail, and cloud apps, and other sources to help piece together individual suspicious elements that might otherwise go unnoticed.



HELPFUL RESOURCE: [Disrupting human-operated attacks]

Identify the signs of a human-operated attack

Catching human-operated attacks in your environment

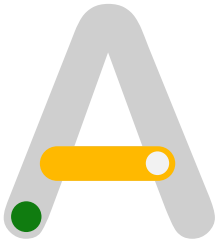
In the wilderness, it's obvious your safety is at risk if you hear the rumbling of an avalanche from higher elevation or see the glowing eyes of a four-legged predator in the shadows. However, there were warning signs in the hours or days before the attack – like pawprints near a watering hole or cracks in the snow. In the same way, effective threat hunters roam their environments for signs of potential threats before they can do serious – and even lasting – damage to the organization.

While most commodity malware can be simply removed, a human-operated attack typically requires coordinated remediation. Since these attacks are operated by humans, people can respond to incomplete attempts to remove their presence from an enterprise. These responses may include changing malware or communication channels, going dormant to avoid detection, or immediately impacting the organization.

Introducing the ABCs of threat hunting

Survival during a human-operated attack relies on your ability to identify signs of the attacker and their activity. These signs are useful in determining the scope of the breach and the list of assets that need to be remediated. Warning signs include both what you can see and what you don't. For instance, if deer sip water from a stream every morning but stay away one morning, it could alert you to a nearby predator in the wild. In cybersecurity, anomalies can include something that is suddenly missing or different in your environment from what you usually see.

Just as there are commonly accepted priorities – shelter, fire, water, and food – in wilderness survival, threat hunters can be guided by the ABCs of threat hunting.



Authentication

Authentication represents the identity aspect of an incident. Identities used by an attacker are valuable for finding other suspicious activity and tracking any accounts that need to be disabled, deleted, or reset. Understanding the authentication aspect of an attack enables you to quickly identify suspicious activity and respond before the adversary has a chance to strike.

Questions to ask when researching the authentication aspect of an attack include:

- What identities did the attacker use to gain initial access?
- What identities did the attacker use after initial access?
- What identities were compromised or potentially exposed to the attacker?
- Were any illegitimate accounts created by the attacker?

Examples of authentication elements

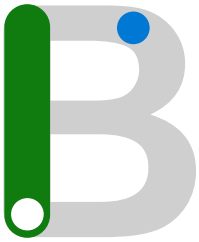
- **User accounts**
- **E-mail addresses**
- **Cloud identities**
- **SAS (Shared Access Signature) tokens**
- **Cookies**
- **Shared credentials (i.e., SSH keys)**
- **Passwords**

Go hunt*

*Go hunt feature applies to the following products:

- Microsoft 365 Defender
- Microsoft Defender for Endpoint

With the go hunt action, you can quickly investigate events and various entity types using powerful query-based advanced hunting capabilities. This action automatically runs an advanced hunting query to find relevant information about the selected event or entity.



Backdoors

Backdoors are intended or malicious ways that an attacker controls a system or service. These can be malware, unintentionally overexposed administrative capabilities, or vulnerable or misconfigured services that an attacker can manipulate to control a system. Researching the backdoor aspect of an attack can provide evidence of attacker techniques that may highlight other potentially compromised applications and systems.

Questions to ask when researching the backdoor aspect of an attack include:

- How did the attacker gain control over the device or service?
- Is there a vulnerability that the attacker abused to control the device or service?
- Did the attacker gain control due to an overly exposed administrative capability?
- What backdoors did the attacker install to provide durable access?

Examples of backdoor elements

- **Malware that provides remote access**
- **Remote administration tools**
- **Built-in management capabilities**
- **Web shells**
- **Accidental or intentional misconfigurations to provide remote access**

Go hunt*

Go hunt feature applies to the following products:

- Microsoft 365 Defender
- Microsoft Defender for Endpoint

With the go hunt action, you can quickly investigate events and various entity types using powerful query-based advanced hunting capabilities. This action automatically runs an advanced hunting query to find relevant information about the selected event or entity.

Communication

The communication aspect of the attack identifies how the attacker interacted with the backdoor. Elements of this communication can be used to help identify other systems the attacker may have interacted with, much in the way that following a wolf's tracks tells you where it went.

Questions to ask when researching communication include:

- How did the attacker communicate with the system compromised during initial access?
- What legitimate or illegitimate apps did the attacker communicate with during the attack?
- Are there any novel attributes of this communication that could be used to track malicious activity elsewhere in my enterprise?

Examples of communication elements

- **IP (Internet Protocol) addresses**
- **DNS (Domain Name System) names**
- **User agent strings**
- **Network routes**
- **Proxies**
- **Network relays**

Go hunt*

Go hunt feature applies to the following products:

- Microsoft 365 Defender
- Microsoft Defender for Endpoint

With the go hunt action, you can quickly investigate events and various entity types using powerful query-based advanced hunting capabilities. This action automatically runs an advanced hunting query to find relevant information about the selected event or entity.

Signs of a human-operated attack

- Credential theft and reuse
- Evidence of human error
- Response to recovery attempts
- Evidence of motive
- Organizational reconnaissance
- Malware that is intended to be interactively controlled*

Is your organization ready?

Microsoft's security operations assessment tool helps you check how prepared your security operations center team is to detect, respond to, and recover from attacks. Find out your organization's security maturity level and learn how to improve processes and tooling to boost preparedness.

Try the assessment tool

*(e.g., Cobalt Strike, which is sometimes deployed alongside other types of malware)

Prepare for common threat scenarios

How to apply the ABCs of threat hunting

Both the wilderness and the cyber landscape are full of surprises. Unfortunately, some of those surprises can hurt you – whether it be a sudden snowstorm that buries your camp or an unforeseen attack that barrels through your organization's defenses and steals sensitive data. Responding to threats quickly and effectively is easier if you've planned for the unexpected.

Preparing for unexpected threats involves searching for and understanding the signs of pending danger. In the wilderness, that might mean seeing menacing clouds in the distance and recognizing that they could dump inches of rain on you if they move closer. In the cybersecurity world, that involves proactively studying common threat scenarios and planning your response BEFORE they become a reality and immobilize your organization.

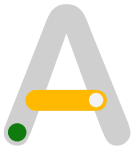
Let's explore how to investigate a few of the most common threat scenarios using the ABCs of threat hunting.

Cloud identity compromise leading to cloud data theft

Cloud data theft can sneak up on you and catch you off guard, much like the appearance of a crevasse in the snow. Plummet into a crevasse and you'll be left staring up at the sky and wondering if there were signs you could have spotted sooner and how in the world you can get out.

Most cloud data theft attacks are the result of a cloud identity compromise, improperly secured information, or an overexposed credential. Cloud data theft attacks can be difficult to detect as they commonly involve detecting anomalous activity being performed using authenticated identities. Luckily, we can use the ABCs of threat hunting to identify and intercept this activity.

Cloud identity compromise investigation



AUTHENTICATION

PROACTIVE THREAT HUNTING ACTIONS:

- Look for suspicious cloud application usage spikes

INVESTIGATION ACTIONS:

Determine if the data is properly secured.

- Review access control lists associated with the data to ensure only intended identities can access it.
- Ensure that anonymous access is not granted to the data.

Determine if any cloud apps have been granted permissions to the data in Defender for Cloud Apps

- Review any apps with high data usage.
- Review highly privileged apps that may have overprivileged access.

Determine if the data was stolen using a compromised credential.

- Review the risky users report in Azure Active Directory. If you see evidence of anomalous logons or leaked credentials, the credential is compromised.
- If the identity performing the suspicious activity is used by an application, review the application for evidence of compromise or abuse.
- If there is evidence that a credential was compromised, consider resetting the password and/or disabling the account.

BACKDOORS

PROACTIVE THREAT HUNTING ACTIONS:

- Suspicious provisioning of permissions to allow remote access
- Providing unusual permissions for one identity over another's (MailboxRead, for example)
- Unusual change in MFA delivery for users (sample device for multiple accounts)

INVESTIGATION ACTIONS:

If a cloud identity was compromised, search for any backdoors created by the attacker anywhere the compromised identity has elevated permissions.

- In Azure Active Directory, search the audit logs for illegitimate accounts, role changes, app approvals, or permission delegation.
- Look for configuration changes that might reduce the security posture of the enterprise, such as file sharing, mail forwarding rules, or ACL (Access Control List) modifications made by the compromised identity.
- Review any apps that may have been granted tenant-wide permissions by the identity.

COMMUNICATION

PROACTIVE THREAT HUNTING ACTIONS:

- Anomalous volumes of cloud identity activity for previously "quiet" identities
- Suspicious authentication patterns (originating from traffic from anonymization services)

INVESTIGATION ACTIONS:

Identify network communication involved with the cloud data theft attack.

- Identify attributes of suspicious logins by cloud accounts associated with the data theft using Defender for Identity or Azure Active Directory audit logs.

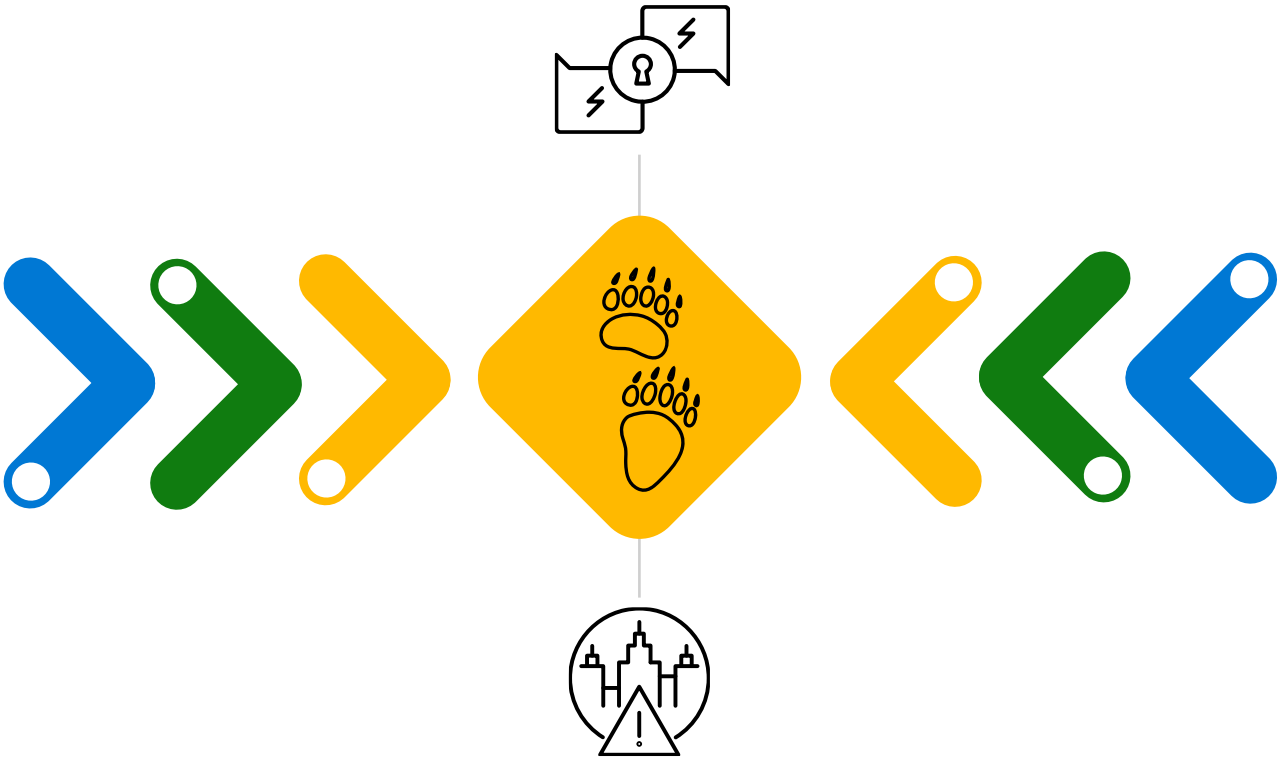
Search for authentication attempts with similar attributes using Defender for Identity or Azure Active Directory.

- Look for other activities performed using the same IP (Internet Protocol) address.
- If the ISP or geolocation of the IP address is not normal for its activity, look for other activity performed from this location, or ISP.

Search for authentication attempts with similar attributes (such as the same IP address, location, or ISP) as the anomalous logon to identify other potentially compromised accounts.

- Use Azure Active Directory activity logs in Azure Monitor and the IdentityLogonEvents table in the advanced hunting schema for support.
- Consider creating custom detection rules in Microsoft 365 Defender to alert you when activity matching the attacker's profile occurs.

Device compromise

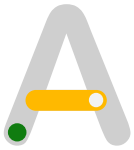


Encountering a snake, alligator, or mountain lion is one of the scariest possible experiences in the wild. Predators are strong and fierce and usually have intimidatingly sharp teeth and claws. Some are ferocious but keep their distance unless you get too close to their young or territory while others are more aggressive.

In a similar way, malware and other device compromise scenarios can be a beastly problem, in large part due to the many paths the attacker can take after compromising a device. This attack can occur when a user is tricked into installing malware or if an attacker gains the ability to log onto a device due to a vulnerability or overexposure.

If you determine that the compromise is the result of a human-operated attack, be sure to size up the situation before acting. Predators in the wild typically leave tracks that alert you to their presence. Human attackers leave signs too, including artifacts that are critical to scoping your situation to ensure that you don't find yourself in the middle of an ambush.

Device compromise investigation



AUTHENTICATION

PROACTIVE THREAT HUNTING ACTIONS:

- Search for anomalous login to device for the user
- Observe any burst of network login activity performed by a typically "quiet" user

INVESTIGATION ACTIONS:

Identify the identity used by the attacker to connect to the device.

- Check for evidence of a logon using a potentially compromised credential.
- Determine if the attacker tricked a user into using their identity to infect the system on their behalf.
- Check if the identity was identified in any known password breaches.
- Identify whether the attack used an account with administrative, root, or system privileges. If so, review other identities that were logged onto the device for evidence of compromise

Check whether the identity used in the attack has administrative or root privileges elsewhere in the enterprise.

- Review any group memberships that may provide elevated privileges within the enterprise or to cloud services. If any are identified, review the activities performed by the identity on these systems.
- If the identity has administrative permissions to your authentication system, review any potential attacks that may have been performed against those systems.

Determine if other credentials were exposed to the attacker.

- Check for evidence that the attacker accessed a password file.
- Determine if the attacker compromised any PKI (public key infrastructure) credentials, such as an exported private key.
- Review activity performed by any cloud identities associated with the identity.

BACKDOORS

PROACTIVE THREAT HUNTING ACTIONS:

- Search for rare or suspicious persistence mechanisms, such as run key entries, cron jobs, startup folder items, or scheduled tasks.

INVESTIGATION ACTIONS:

Identify the backdoor used by the attacker to control the compromised device.

- Determine if any malware detections were raised for the device.
- Check for evidence of illegitimate use of remote administration capabilities like remote desktop protocol (RDP) or Secure Shell (SSH).

Identify if the attacker used remote administration software that is not part of your normal configuration

- Review software installed on the device using the software tab on the device page.
- Use Advanced Hunting to review any processes that may provide remote control capability.
- Check if the device hosts a service that may contain a network-accessible remote code execution (RCE) vulnerability.
- If the device runs in-house developed code, review any activity that may indicate an unknown vulnerability.

HELPFUL RESOURCE: Response actions for a device

Device compromise investigation *continued*

C

COMMUNICATION

PROACTIVE THREAT HUNTING ACTIONS:

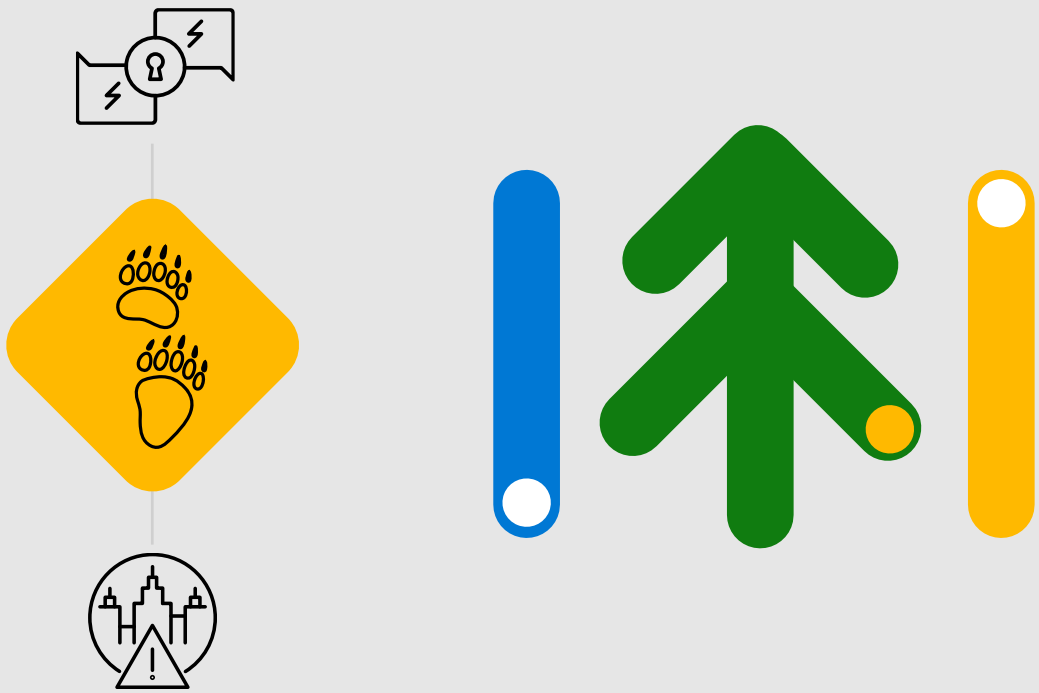
- Search for suspicious beaconing activity from benign EXEs
- Determine if there has been anomalous peer-to-peer communication activity by device

INVESTIGATION ACTIONS:

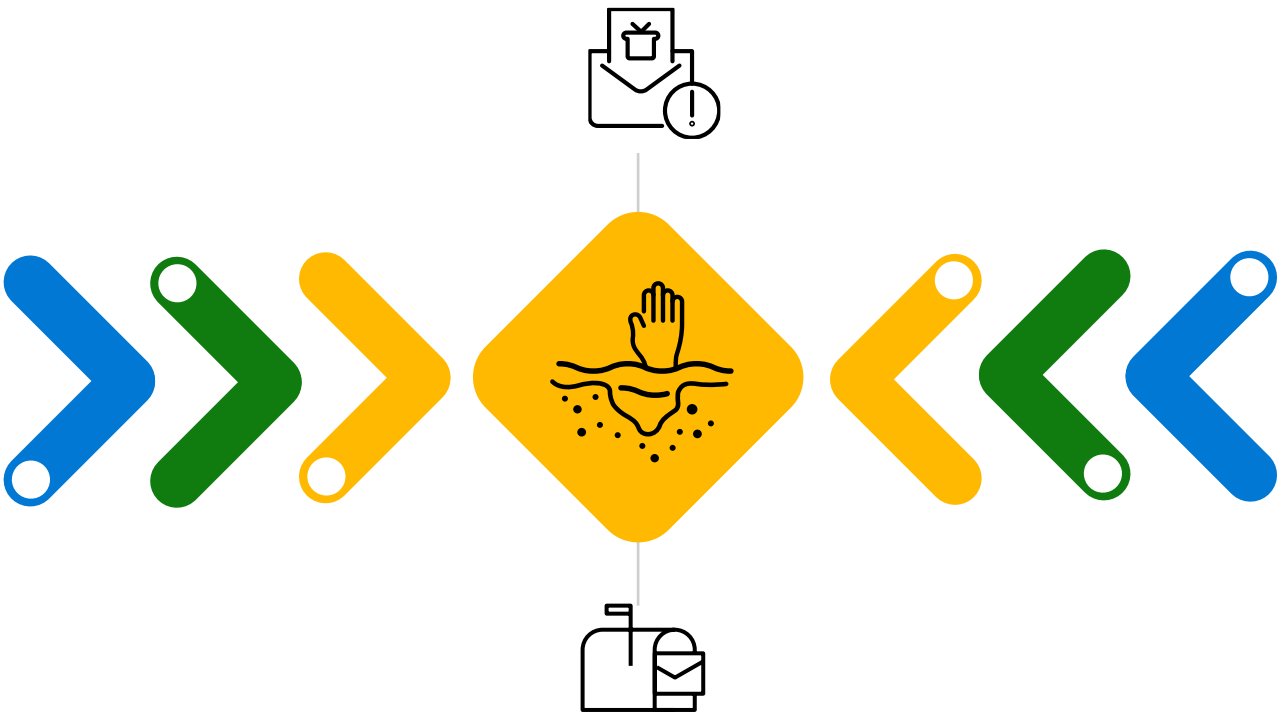
- Determine how the attacker communicated with the system.
- Check if the attacker connected to the system over a network.
- Determine if the attacker used a phishing e-mail to trick the user into compromising the device.
- Identify any identifying characteristics of the communication that could be used to detect other communication from the attacker.

Determine if the malware or attacker communicated with any other systems, domains, or cloud apps.

- Check if there were any suspicious outbound network connections made by the backdoor or identity.
- Look for evidence that the device or identity attempted to communicate to internal systems.
- Determine if there are any new listening network connections created as part of the compromise.



Office 365 mailbox compromise

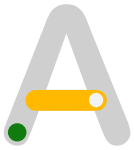


Panicking after stepping into quicksand can make a bad situation much worse – even causing you to sink further. Wading through multiple security alerts can be frustrating and scary.

Email is a top target of attackers looking to steal sensitive information, send fraudulent invoices, or use your email address to trick your business partners into trusting an otherwise immediately suspicious message.

One day, you may have a sinking feeling you're not the only one using your mailbox. Before you know it, you are waist-deep in quicksand wondering how in the world you can get out. Luckily, if you remain calm and make the right moves you can avoid sinking further, prevent data loss, and soon find yourself back on solid ground – thanks to the ABCs of threat hunting.

Office 365 mailbox compromise investigation



AUTHENTICATION

PROACTIVE THREAT HUNTING ACTIONS:

- Check for any anomalous login sources
- Review "Low and slow" password sprays (learn more about hunting for low and slow password sprays)

Investigation actions:

- Determine the identity used to log onto the mailbox
- Check if the identity used was the mailbox owner, a delegate, or an administrator.
- Determine if the identity logged onto more than one mailbox.

Research suspicious activity associated with the identity.

- Check for multiple failed logons to the identity prior to the successful logon.
- Look for suspicious elements to the account logon activity, such as an abnormal location, time of day, or frequency.
- Determine whether other services were accessed by the identity.

BACKDOORS

PROACTIVE THREAT HUNTING ACTIONS:

- Check anomalous inbox rules created by user
- Determine anomalous delegation relationships between users

Investigation actions:

Research whether any mailbox configurations were made during the compromise.

- Check if any mailbox forwarding addresses were created.
- Determine if there were any malicious inbox rules created.
- Check for any suspicious mailbox delegations created by the account.

COMMUNICATION

PROACTIVE THREAT HUNTING ACTIONS:

- Check for anomalous bursts of outbound emails to previously unseen domains (phishing relay)

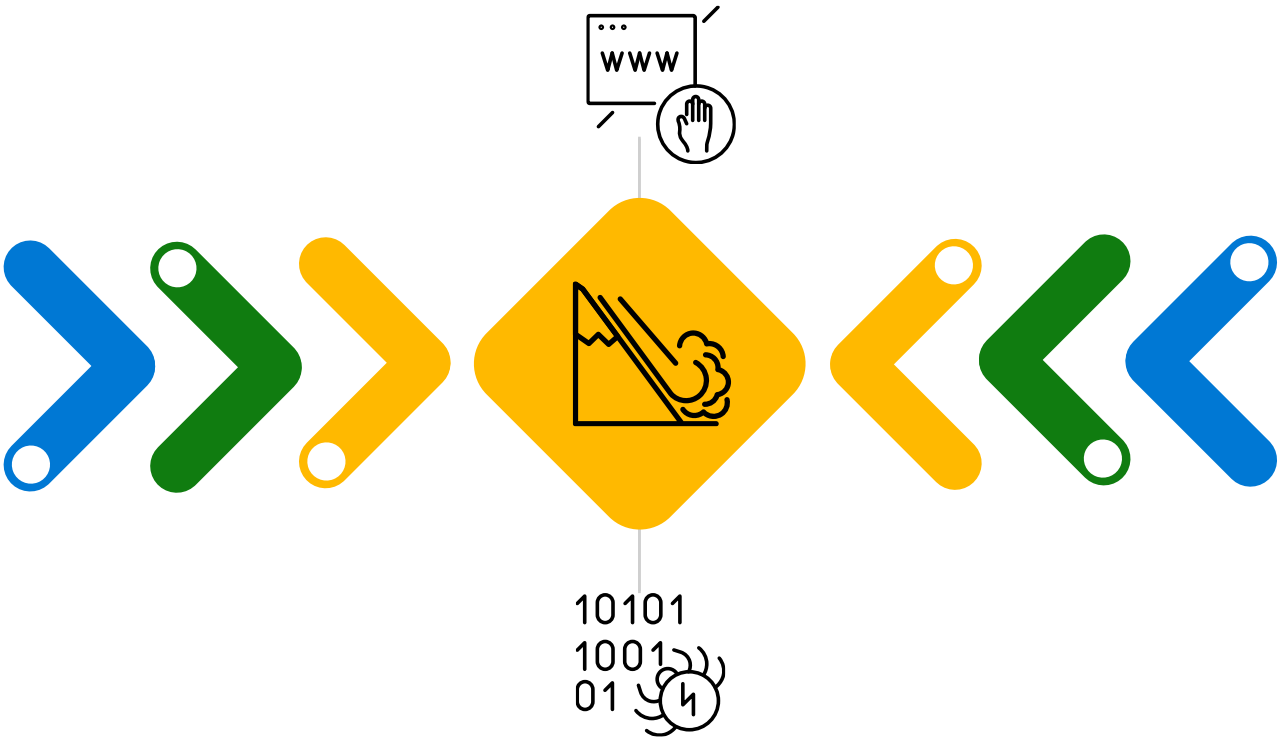
INVESTIGATION ACTIONS:

Research the communication path used by the attacker.

- Check if the IP (Internet Protocol) address of the attacker was seen anywhere else in the enterprise.
- Look for any unique attributes to the communication that could be used for research or detection, such as ISP, location, or user agent string.

HELPFUL RESOURCE: Response actions for a compromised email account

Human-operated ransomware attacks

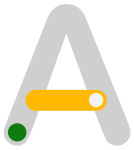


Human-operated ransomware attacks can feel as overwhelming as a powerful avalanche barreling down a mountain and picking up speed as it goes. You detect a rumble, the ground shakes, and your phone rings off the hook. Instead of watching the chaos, act fast before the landslide is directly upon you.

Human-operated ransomware attacks are a coordinated effort that can be significantly damaging to organizations. In these attacks, attackers will use reconnaissance techniques to quickly get a lay of the land and find a way to encrypt as much data as possible in a short amount of time before demanding a ransom.

This scenario is one of the biggest reasons to master the ABCs of threat hunting. In a human-operated ransomware attack, it is important to identify how the ransomware is being distributed and intercept it without causing undue harm. Once distribution has been stopped, use the ABCs of threat hunting to identify how the attacker controlled the source and work to rapidly eliminate their control.

Human-operated attacks investigation



AUTHENTICATION

PROACTIVE THREAT HUNTING ACTIONS:

- Identify unusual login events associated with highly privileged accounts – such as members of the Domain Admins groups or powerful service accounts

INVESTIGATION ACTIONS:

Determine the identity being used to distribute the ransomware.

- Review identities associated with file copies and process identities used by the ransomware.

When the identity used to distribute the ransomware is identified, prevent it from performing further damage by disabling the identity and changing its password.

Review historical activity involving the identity to discover other potential attacker activity.

- Review any suspicious logons that led up to the ransomware distribution.
- Look for any credential attacks associated with the identity or a device where it was exposed.
- Research any recent alerts involving the identity.

BACKDOORS

PROACTIVE THREAT HUNTING ACTIONS:

- Monitor environment for anomalous, large-scale creation of low-prevalence executables

INVESTIGATION ACTIONS:

Determine the mechanism used to launch the ransomware.

- Review recent group policy changes that may include a task to launch ransomware from a central location.
- Look for a sudden increase in the use of remote execution tools, such as *psexec* or *winexesvc*.
- Look for process creation attempts using remote administration capabilities such as WMI (Windows Management Instrumentation) or WS-Man.
- Check system event logs for the presence of malicious data introduced via removable storage device (USB)
- Review system event logs for the installation of software claiming to be updates, as in the incident SocGholish.

When the distribution source is identified, identify the attacker's means of controlling that endpoint.

- Look for suspicious processes that might provide remote control to the attacker.
- Identify any operating system remote administration capabilities that might have been used to control the system, such as RDP, SSH, WMI (Windows Management Instrumentation), or WS-Man.

If you find a backdoor, search for its use elsewhere in your enterprise.

- If the backdoor is not a common tool for your enterprise, use Advanced Hunting to identify similar processes based on file hash, metadata, local TCP (Transmission Control Protocol) port, launch location, or other unique attributes.
- If the backdoor is a common tool for your enterprise, research the source of the network connection used to control the device.

HELPFUL RESOURCE: Response actions for detecting ransomware

Human-operated attacks investigation *continued*

C

COMMUNICATION

PROACTIVE THREAT HUNTING ACTIONS:

- Surface sudden bursts of communication activity to low-frequency domains or IP addresses by multiple, distinct devices

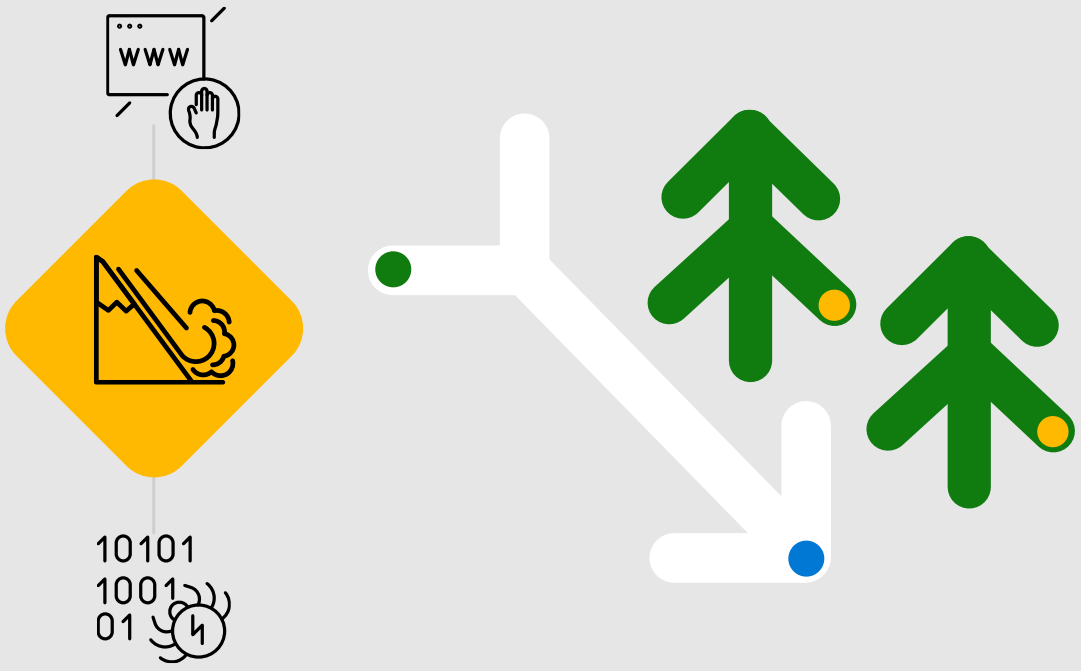
INVESTIGATION ACTIONS:

Look for network connections that may be associated with ransomware.

- Identify the network source used to distribute the ransomware using Advanced Hunting and, if possible, block it.
- Review network connections made by the ransomware in Advanced Hunting to identify any communication channel you may be able to sever and monitor.

Research the communication path used by the attacker to control the distribution point.

- Consider blocking and monitoring the communication path, using Indicators if possible.
- Check whether the IP address of the attacker was seen anywhere else in the enterprise.
- Determine if there are any unique attributes to the communication that can be used for research or detection, such as ISP, location, or user agent string.



Build a shelter

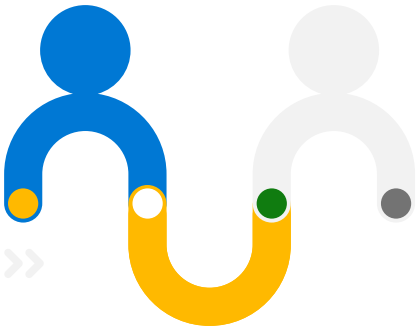
How to develop your own threat hunting program

Surviving in the wild is much easier – many would say necessary – with a sturdy shelter. And it's easier to build such a shelter when you're joined by other people contributing their expertise to its construction.

Given the enormous challenge of detecting and mitigating threats, you may decide to build your own threat hunting team. This requires bringing together the right people and giving them enough time and the right technology and training to succeed in their hunting activities. This section walks through the steps involved in developing a threat hunting program.

Team-building strategies

Microsoft has assembled multiple security operations center (SOC) teams to protect our technical environments and we've come to recognize the tremendous value of SOC culture when building a team.



Use your human talent wisely

Automate repetitive tasks whenever possible so the time of your talent can be better spent on tasks requiring expertise, judgement, and creative thinking. People are the most valuable asset of any SOC.

Choose team players

People with a "lone wolf" mindset are not the best choice for a high-pressure working environment that requires collaboration. Teamwork makes the SOC more productive, fun, and insightful as everyone shares their knowledge.

Adopt a "shift left" mindset

Cybercriminals continuously finetune their approaches. So should SOC teams by shifting their activities "left" in the attack timeline. Our goal is to achieve "faster than the speed of attack" approaches to detect and address attacks sooner.

Steps of creating a threat hunting program

When evaluating an organization's hunting capacity, take three steps:

1 Evaluate your skillset

Undoubtedly, your organization's skill level is the most significant component since strong data analyst skills enable threat hunters to transform data into detections. Consider how effective prospective team members are at utilizing data and tools to uncover security incidents.

The people on your threat hunting team should be knowledgeable about the internals of the operating systems found in your endpoints. They also should be comfortable with basic networking concepts, including the type of network flows per application/service that can be expected. After you know what expertise is needed, figure out who has these expert skills and bring them onto the threat hunting team.

Unless you have an unlimited budget to build your threat hunting team, you need to carve out time from the work schedules of existing staff for threat hunting. The number of hours a week you spend on threat hunting will vary depending on the size of your organization, your security posture, and your risk tolerance. Depending on the size of the organization, and wherever you get them from, you'll likely need to reallocate roles and responsibilities, so you don't leave other teams shorthanded.

Start by dedicating two to four hours a week to proactive hunting. When you see results from your hunts, adjust as needed. The important thing is getting results from your hunts and tweaking existing tools to maximize return on investment (ROI). It's all about allocating time and committing yourself to results.

2 Consider your data's quality and quantity

The quality and quantity of data gathered helps define the maturity of an organization's threat hunting. The more data supplied to a threat hunter from throughout the organization (and the more diverse types of data you provide), the easier it is to uncover useful results. However, that's challenging without automation.

Automation enables people to spend more of their time working on the complex problems that are a given in threat hunting. Automation increases response speed, though it must be regularly adapted as attackers change their approach.

3 Determine tools to benefit your hunting efforts

Threat hunting doesn't just involve people or machines. Without the right tools in place, your threat hunters are going into the wilderness with nothing. Without threat hunting tools, there's no hunt. The right tools offer:

- Visibility into authentication activity
- Visibility into endpoint activity
- Visibility into network activity
- Threat intelligence
- Customizable data correlation and analytics

Bolster your hunt with tools

How Microsoft Defender Experts for Hunting can help

Even the most seasoned wilderness survivalists supplement their vast knowledge with tools and guidance. They rely on experience to find the choicest tinder and kindling in the woods, for instance, but use their trusty flint and steel or bow saw to spark it into a fire so they can stay warm and boil water.

The usefulness of tools applies to threat hunting, whether you build your own team or turn to a managed service to gain 24x7 threat hunting expertise. People's knowledge is the key to successful threat detection in any situation and people are the cybersecurity heroes. However, tools can increase the effectiveness of threat hunting by extending your capabilities. One tool available to add to your threat hunting toolkit is Microsoft Defender Experts for Hunting.

Microsoft Defender Experts for Hunting assists your hunt

Threat hunting is incredibly time-consuming so using a managed service can give you 24x7 coverage with a lower cost than building a team in-house.

Consider Microsoft Defender Experts your trail guides in all your threat hunting adventures. Defender Experts for Hunting was created for customers that have a robust security operations center but want to proactively hunt threats using Microsoft Defender data. Defender Experts for Hunting is a proactive threat hunting service that goes beyond the endpoint to hunt across endpoints, Office 365, cloud applications, and identity. Our experts will investigate anything they find, then hand off contextual alert information, along with remediation instructions so you can quickly respond.

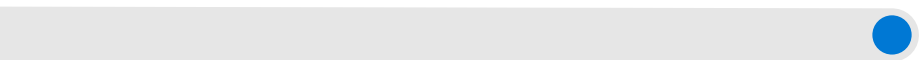
Guided by the 24 trillion threat signals Microsoft observes every day, our hunters investigate suspicious activity, like the case of vendor compromise that led to a large phishing campaign in one Microsoft customer's environment. Defender for Expert Hunting also includes one-click access within the Microsoft 365 Defender portal to Experts on Demand if you have questions about a specific incident, nation-state actor, or attack vector.

How Microsoft Defender Experts for Hunting works

Step 1:
Microsoft hunting experts investigate and analyze potential malicious activity associated with human adversaries

Step 2:
If the threat is found to be valid, analysts conduct a deep-dive investigation, gathering threat details, including scope and method of entry.

Step 3:
Defender expert notifications appear as incidents in Microsoft 365 Defender, alerting you to the threat and sharing threat details to protect your organization's endpoints, email, cloud apps, and identities.



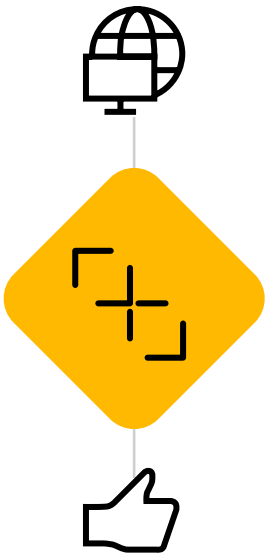
Formulate hypotheses to explain data suggesting a potential threat

Find context using artificial intelligence and data from observations

Hunt for and collect observations to support hypotheses, with the help of automated systems

Investigate and analyze the most critical potential threats first, using threat intelligence

Notify customers affected by a validated threat, with categorization based on behavior, characteristics, and impact.



Thrive in your threat hunting

In this threat hunting guide, we've offered recommendations on how to identify and investigate threats. We hope that like a wilderness guide who can ease people's experience in the wild, we have provided you with strategies you can implement for smoother threat hunting. Find out more about Microsoft's threat hunting service and visit the Microsoft Defender Experts for Hunting webpage.

Plus, collaborate with fellow hunters on community queries in the Defender Portal. Review and contribute queries on GitHub.

Happy hunting!

Threat hunting guide takeaways

Proactive threat hunting can help prepare you to address sophisticated modern threats more effectively.

Move beyond endpoints by extending the digital perimeter using XDR and following Zero Trust principles.

Commodity malware and human-operated attacks are two distinctly different types of attacks requiring different approaches.

Know the ABCs (authentication, backdoors, and communication) of threat hunting

Cyberattacks are as varied as they are insidious. Commodity malware can evolve to human-operated attacks rapidly.

Understanding common attack scenarios can help you prepare.

Building your own threat hunting program is challenging but could be useful (Hint: First study our maturity model and assess your organization's level).

Another set of eyes never hurts – consult a Defender Expert to help with your investigations

Get started

- Read how Microsoft Defender Experts for Hunting offers proactive threat hunting.
- Get details on Microsoft Defender Experts for Hunting's core features.
- Read the Microsoft Defender Experts for Hunting announcement and how to get started.
- Explore Microsoft's security research and threat intelligence efforts
- Check out our quarterly cyberthreat intelligence brief called Cyber Signals.
- Bookmark the Microsoft Security Blog to stay aware of the latest security threats.
- Learn more about the threat of ransomware as-a-service.
- Learn more about protecting your organization from ransomware
- Learn more about human operated ransomware and how to build resilience against it
- Incident response overview
- Incident response playbooks