SOPHOS
Cybersecurity delivered.

Getting Started With Threat Hunting

Practical guidance on preparing to search for and neutralize elusive cyber threats

Cyberattacks are evolving. Adversaries are increasingly turning to sophisticated and highly evasive methods to facilitate and execute their attacks. The practice of hunting for and neutralizing malicious activity has therefore become critical in the fight against these advanced threats – but it isn't easy.

In this report, we provide guidance on getting you started with threat hunting and a summary of the tools and frameworks security teams are leveraging to help them stay ahead of the latest cyber threats and rapidly respond to any potential attacks. We'll also give you the five steps IT professionals should follow to prepare for threat hunting.

A Sophos Whitepaper. August 2022

The state of cyber threats in 2022

Attacks have increased in volume, complexity, and impact

The cybersecurity challenge facing organizations continues to grow. Over the last year, 57% of organizations experienced an increase in the volume of cyberattacks, 59% saw the complexity of attacks increase, and 53% said the impact of attacks had increased. Almost three in four (72%) saw an increase in at least one of these areas.

A growing trend is an increase in supply chain attacks, such as the SolarWinds incident revealed in March 2021. Attackers had inserted modified instructions into the source code of their Orion solution that is used to manage complex networks remotely. This backdoor enabled the adversaries to access the networks of SolarWinds' customers, including several government agencies.

Ransomware is a real threat to all organizations

66% of organizations were hit by ransomware in the last year, up from 37% in 2020. This is a 78% increase over the course of a year, demonstrating that adversaries have become considerably more capable of executing attacks at scale.

The growing use of legitimate tools in cyber attacks

Adversaries are increasingly taking advantage of bootleg or pirated copies of legitimate, off-the-shelf software and free, open-source tools. Typically, these tools are designed to simulate cyberattacks to improve security but can be exploited by criminals to do the opposite.

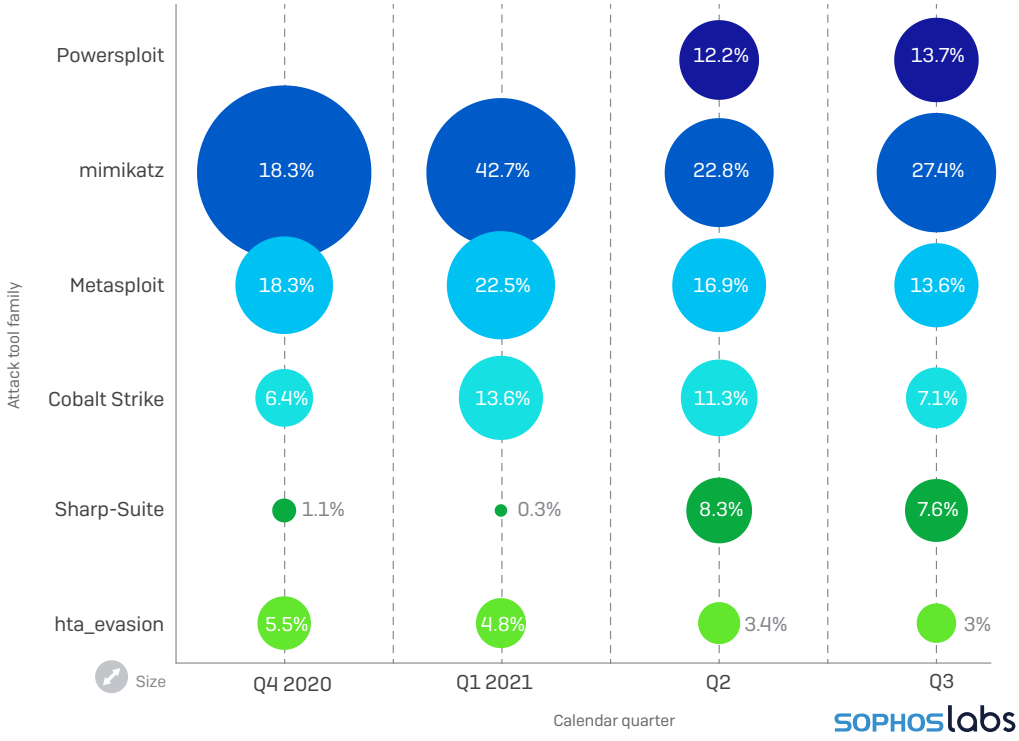
Tools like Mimikatz (used by penetration testers and malware authors alike), while not strictly commercial offerings, were used widely, appearing in nearly every hands-on-keyboard incident Sophos investigated over the past year.

Also, notably dominant (thanks to its source code being leaked in 2020) were pirated copies of Cobalt Strike (an adversary simulation software), which were not only used in ransomware attacks but also dropped as an initial payload of other malware.

[1]*The State of Ransomware 2022 - Sophos*
[2]*The State of Ransomware 2022 - Sophos*

Prevalence of top attack tools

On a per-machine basis, the most frequently encountered attack tools seen in 2020-2021



Sophos 2022 Threat Report

Cobalt Strike's 'Beacons' feature, which provides a capable backdoor to Windows machines, has meant the software has become the favored tool for cybercriminals. As such, most of the ransomware cases we've seen over the last year have involved the use of Cobalt Strike Beacons.

For a more detailed overview of the state of cyber threats today, check out the latest Sophos Threat Report.

Proactive cybersecurity practices are a must

Supply chain attacks. Software exploits. Legitimate tools. The common theme here is the nature of these approaches. They are human-led. They are highly targeted and calculated. They are evasive and non-detectable by traditional means.

Organizations must shift to more proactive cybersecurity approaches to remain ahead of the criminals. Responding to human adversaries requires a human-led approach.

Enter threat hunting.

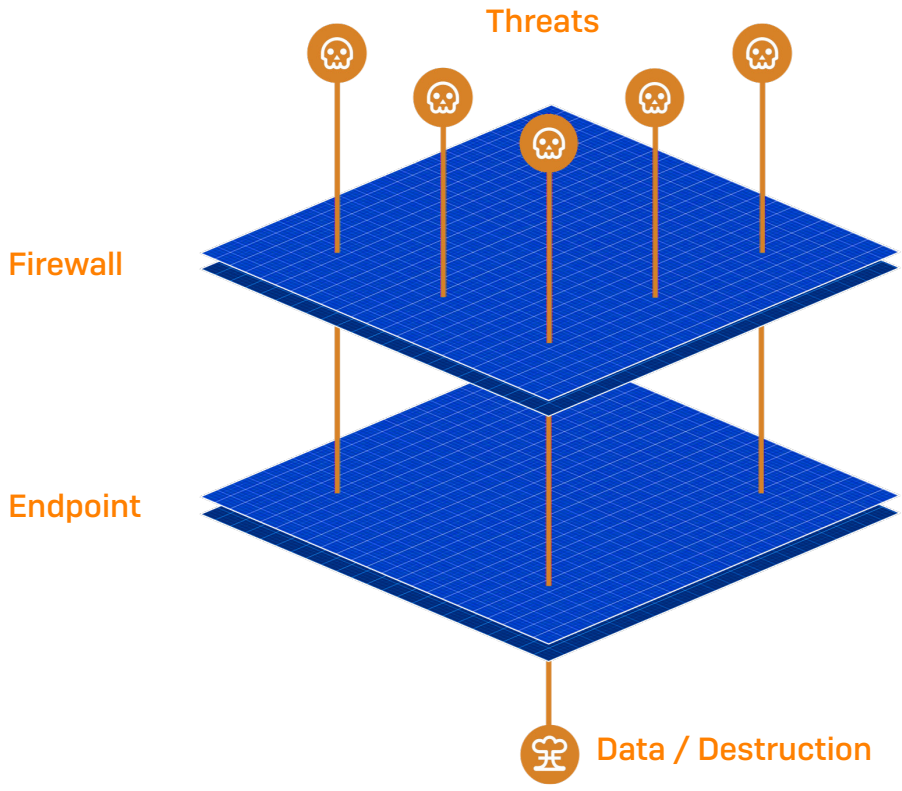
What is threat hunting?

Threat hunting is the iterative and proactive process of searching through endpoint and network telemetry to identify malicious activity, done so with the assumption that adversaries have already evaded defenses. We label it as iterative as the practice needs to adapt constantly to ensure it remains an effective method to seek and neutralize today's equally evolving cyber threats.

During a threat hunt, teams will analyze the tools, techniques, and procedures (TTPs) used by threat actors to determine the attack's stage and build intel. Once they have established this, they will take an appropriate action to neutralize the threat if necessary.

Why do we need to threat hunt?

The reasons are multiple though the overarching reason is a single truth: contrary to innumerable claims, technology alone cannot stop 100% of threats. Despite multiple layers of defenses, some threats are still sneaking their way into and compromising IT estates.



As we've already alluded to, modern threat actors are increasingly turning to adaptive and evasive approaches that are literally 'hands-on keyboard' instead of the automated and wide-scale attacks of yesteryear.

This is reflected in the findings of our threat response teams, who report a significant rise in the number of human adversaries controlling and driving attacks. This means security teams are required to hunt for the unknown to stay on the front foot while adopting the mindset that a breach has already occurred.

The threat hunting mentality

Experienced threat hunters often assume that a potential threat has already evaded defenses irrespective of where it might be in the attack chain. They adopt this mentality because it compels them to do two things.

Limit threat actor dwell time

Adopting this mindset compels teams to limit the threat actor's dwell time. The longer a hacker has inside your network, the more time they have to execute nefarious activities. Therefore, the less time we can give an adversary inside a network, the less damage they can do. Security teams are compelled to seek out threats before their impacts can be felt by assuming defenses have already been evaded.

Reduce the time to detection

Adopting this mentality also compels teams to reduce the mean time to detection. You may have multiple layers of defense in place, and the evasive threat may trigger your defense further along its attack chain. The problem is, at this point, it's too late – the damage is done as the threat has already escalated too far. By hunting for the threat, we may be able to identify weaknesses in our security that can subsequently be addressed, ultimately reducing the time to detect the same or similar threats in the future.

Who does threat hunting?

Profile of a threat hunter

Before we delve into who does threat hunting, it's essential to understand the role of a threat hunter. Threat hunting is a highly complex operation. Individuals in this space need to possess a specific and niche set of skills. That said, the typical traits required of a threat hunter are as follows:

- **Creative and curious** – looking for threats can be akin to looking for a needle in a haystack. Threat hunters can often spend days looking for threats, using numerous methods to unearth them.
- **Experience in cybersecurity** – threat hunting is one of the most advanced operations within cybersecurity. Therefore, prior experience in the field and foundational knowledge are a must.
- **Threat landscape knowledge** – understanding the latest threat trends is a must when seeking out and neutralizing unknown entities.
- **Adversarial mindset** – the ability to think like a hacker is critical in combating today's human-led approaches.
- **Technical writing ability** – threat hunters are required to log all their findings as part of the investigation process. Therefore, the ability to communicate such complex information is critical in seeing the hunt through to its conclusion.
- **Operating system (OS) and networking knowledge** – advanced working knowledge of both is essential.
- **Coding / scripting experience** – required to help threat hunters to build programs, automate tasks, parse logs, and carry out data analysis tasks to aid and progress their investigations.

Unfortunately, compounding this rare combination of competencies is a notable skills shortage in the IT sector, with 54% of IT administrators believing that even with all the tools at their disposal, cyberattacks are now too advanced for their IT team to deal with on their own . That said, where roles can be filled, we broadly see threat hunting conducted by one of two different teams.

In-house Security Operations Center (SOCs)

Where organizations choose to do threat hunting themselves, you will find them employed within the SOC. A SOC is a centralized in-house business function focusing on monitoring, detecting, investigating, and responding to cyber threats while improving the parent organization's overarching security posture. They are the go-to team within the organization regarding cybersecurity matters.

Third-Party Security Operation Providers

Many organizations are increasingly outsourcing their security operations to third-party providers. This may be due to a lack of in-house capacity (IT teams saw a 69% increase in cybersecurity workload over the last year), lack of skills, or preference for external experts for this critical 24/7 task.

Managed detection and response (MDR) providers

MDR, delivered as a fully managed service, empowers organizations with a dedicated team of security analysts hunting for lurking threats 24/7/365. In fact, "51% utilize a managed detection and response (MDR) service provider to help integrate telemetry data for threat detection and response," according to ESG Research.

MDR providers have a variety of advantages over an in-house only security operations program. The most significant advantage of them all is often experience.

The Sophos MDR team has thousands of hours of experience, having seen and dealt with everything adversaries can throw at them. They can also learn from attacks on one organization and apply them to all customers. Another benefit is scale: the Sophos MDR team can provide 24/7 support delivered by three global teams.

Managed security service providers (MSSPs)

MSSPs are employed to manage part of or all the organization's IT security operations allowing in-house teams to focus more on day-to-day tasks. MSSPs will offer threat hunting capabilities as part of a managed service. This may well include MDR services as detailed above.

Threat hunting enablers

Endpoint/extended detection and response (EDR/XDR)

For threat hunters to identify and investigate potentially malicious activities, they need inputs and investigation tools. Enter EDR and XDR. They enable hunters to quickly see suspicious detections and investigate them thoroughly.

As the name suggests, EDR provides inputs from the endpoint solution. In contrast, XDR consolidates signals from across the wider IT environment, including firewall, mobile, email, and cloud security solutions. Given that adversaries exploit every attack opportunity, the wider you cast your signal net, the better you can detect them early.

One of the biggest practical challenges with EDR/XDR solutions is noise: threat hunters get so many signals that it can be hard to see the wood from the trees. That's why it's essential to combine your EDR/XDR solution with powerful endpoint protection that stops more threats up front, enabling defenders to focus on fewer, more accurate detections.

The anatomy of threat detection and response

Threat hunting is a component of a more extensive operation – threat detection and response. At Sophos, we apply a threat detection and response framework to our hunts. This consists of five core components.

1. Prevention

Having robust and properly configured prevention technologies (such as an endpoint protection solution) in place prevents attackers from being able to penetrate your network. More importantly, it also reduces the number of security alerts that are generated on a daily or even hourly basis. With fewer alerts to wade through, the security team can better spot and focus on the signals that matter – in this case, evasive human-led adversaries.

2. Collection of security events, alerts, and detections

Data is the fuel that powers threat hunting and analysis. Without the right type, volume, and quality of signals, it is challenging for security operations teams to accurately identify potential attack indicators. Yet data without context complicates the analyst's conviction decision. Without meaningful metadata associated with the signal, the analyst will have difficulty determining if the signals are malicious or benign.

3. Prioritization of the signals that matter

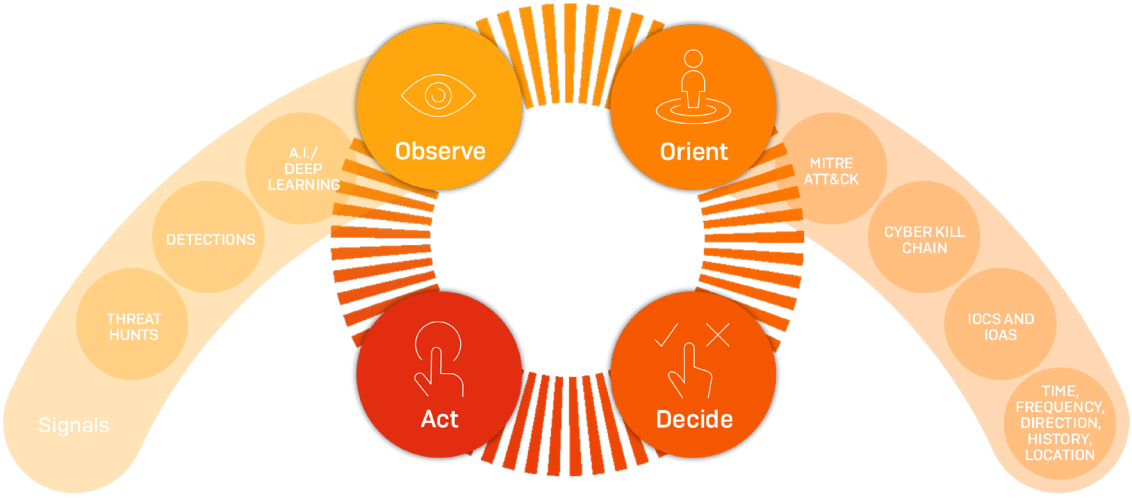
To avoid being overwhelmed by data and failing to spot the items that warrant closer investigation, you need to be able to pinpoint the alerts that matter. This is harder than it looks. The more you can improve signal-to-noise ratios by using a combination of context that only event producers can provide, together with automated and artificial intelligence, the better. Even with automation, it is not a simple process.

4. Investigation

Once you have isolated the key signals, it is time to add insight and measure what you have discovered against industry frameworks and models to build a confidence threshold in the conviction of malicious or benign behavior.

OODA Investigation Framework

Experienced security analysts often utilize a framework to guide their investigations. For example, the Sophos MDR team uses an investigative methodology known as the OODA loop. This allows them to engage in the cycle mentioned above to ensure that all findings are tested and proven:



The OODA loop is a military concept that enables our team to go through a reasoning cycle to fully understand the event and surrounding behavior. They can then build off this knowledge and employ human decision-making and intuition to conclude whether malicious activity is present within a customer environment and, based on this, can decide how to act upon it.

When applying the OODA framework, Sophos' security analysts will often perform the following steps:

- **Observe** - what do we see in this detection?
  - Observation of the potential external and internal connections related to the detection
  - Ascertaining where the detection is happening and if end users are associated with it
- **Orient** – what do we understand about this detection?
  - Gathering evidence-based data
  - Understanding the TTPs common or specific to this attack or threat actors. One such resource utilized to identify TTPs is the MITRE ATT&CK framework, which we'll expand on later in the report.
  - Gathering intelligence on indicators of attack (IOAs) and indicators of compromise (IOCs)
- **Decide** - Is this detection malicious, suspicious or benign? Is action required?
- **Act** – based on the previous steps, what will you do?
  - Mitigate - neutralize – re-loop – improve.

5. Action

This is a big one. Once you've determined that you are dealing with a threat, you need to do two things – and they are both equally important.

The first is to mitigate the immediate issue, while the second is to remember that you are probably only addressing a symptom of the attack and still need to hunt down and neutralize the root cause. The first must be done without impairing your ability to do the second.

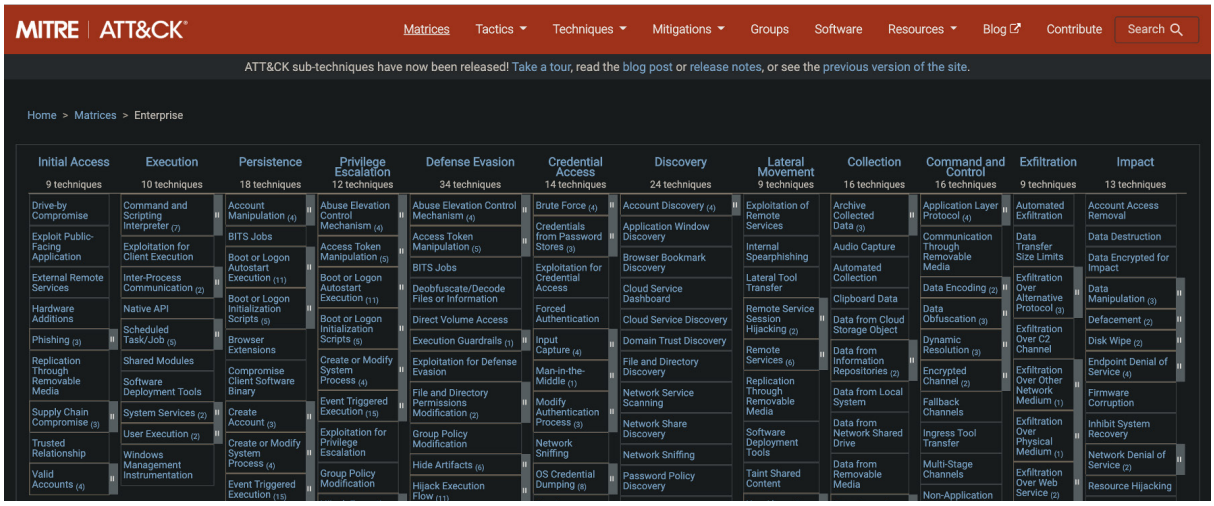
Sometimes it will be enough to quarantine a machine or disconnect it from the network, while at other times, the security team will need to go deep into a network to extract the tendrils of an attacker.

For instance, just because you've successfully blocked and removed malware from your system and stopped seeing the alert that put you onto it doesn't mean the attacker has been eliminated from your environment.

Professional threat hunters who see thousands of attacks know when and where to look deeper. They look for what else attackers are doing, have done, or might be planning to do in the network – and neutralize that too.

Classifying threats: the MITRE ATT&CK framework

A resource often used by threat hunters is the MITRE ATT&CK framework. If you've spent any amount of time in cybersecurity, you've most likely at least heard of it. Among many frameworks, MITRE is a globally accessible knowledge base of adversary TTPs based on real-world observations, and is used as a foundation for developing specific threat models and methodologies. It enables threat hunters to map attacker behaviors to a plethora of previously identified TTPs. This, in turn, allows hunters to establish where in the lifecycle the ongoing attack is. It is critical to the 'Orient' stage of the OODA framework.



You can get more detailed information on the MITRE ATT&CK framework here.

Threat hunting methods

This section will look at some commonly employed threat hunting methods. At Sophos, we often initiate hunts in two different ways.

Lead-driven threat hunts

In our organization, any detection that needs further investigation is reviewed by a human threat analyst who can apply business context and human reasoning to any situation. They will observe the behavior, consider the previously established business context, build a hypothesis, and then act on it. The hypothesis may be to actively engage with the potential incident or do some further investigatory work to further cement their knowledge on the issue at hand.

To complete the loop, the analyst will wait and review to see the results of that hypothesis and testing. If further investigation is required, then they can repeat this cycle until they have a decision. If the event has evolved into an active incident, the analyst will pivot into full response mode to actively combat the threat.

Leadless threat hunts

While lead-driven hunts require one of our sensors to detect or generate a "signal" of interest, a leadless hunt is much more organic. Although we may still be using our artificial intelligence algorithms to process the large amount of data we ingest, leadless threat hunts are nearly always helmed by a human threat analyst.

Rather than relying on that initial systematic signal to give us a heads-up that something needs to be investigated, we proactively run queries on a customer's, or multiple customers', estates. This may occur for several reasons, not limited to:

- A customer in the same industry vertical has been targeted in a particular way, and we want to perform due diligence to ensure that the same threat actors are not attempting to attack any of our other customers
- SophosLabs has informed the MDR team of a significant attack targeting customers, either in the same vertical or with similar properties
- A significant event has occurred within the security landscape, and we want to ascertain if any of our customers are affected

Case study: The ransomware hunt that unearthed a historic banking trojan

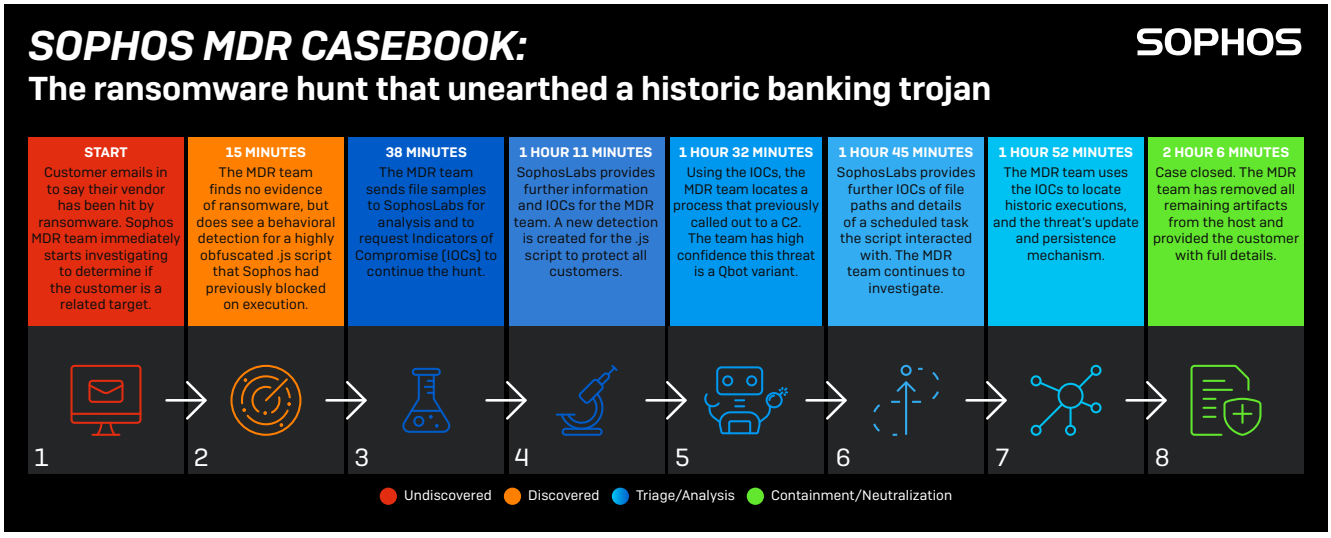
Now that we've outlined the intricacies around threat hunting, let's look at a threat hunt in action. As investigated by the Sophos MDR team, this case is a great example of how a threat hunt can uncover the unexpected. In this case, a customer got in touch to say that a vendor they worked with had been hit by ransomware, and they were worried that they might also have been infected.

The Sophos MDR team started investigating immediately, working with our experts in SophosLabs. They quickly realized there was no evidence of ransomware. At this point, some teams might have closed the case and moved on to other work. However, the Sophos MDR team continued investigating and uncovered a historic banking trojan.

The customer was able to relax knowing that they hadn't been affected by ransomware and that a historic banking malware had been fully removed – an outcome that wouldn't have come to fruition without expert intervention.

And as this story shows, while ransomware is often the threat that is front of mind, it's essential also to be alert to the attacks that prefer to hide in the shadows.

Within two hours and 6 minutes, the whole incident had been investigated and cleaned up.



For a deep dive into this case, check out the article here.

Preparing for threat hunting – five steps to support a successful outcome

You'll hopefully now have a good grasp of all things threat hunting related. However, before you can begin, it's essential to ensure your organization is best equipped to carry it out effectively.

1. Understand the maturity of your current cybersecurity operations

Before you can begin to understand potential adversaries, you need to understand the state of your current cybersecurity operations. Mapping your processes to a cybersecurity maturity model (such as the CMMC) is a great way to establish how well equipped (or not) you are to begin threat hunting. It's also a good idea to audit your security posture to determine just how susceptible to threats you might be.

2. Decide how you want to go about threat hunting

Once you've established your cyber maturity, you can then decide whether threat hunting is something you want to do in-house, fully outsource, or a combination of the two.

3. Identify technology gaps

Review your existing tools and identify what else you need to do effective threat hunting. How effective is your prevention technology? Does it have or support the threat hunting capabilities brought about by EDR/XDR?

4. Identify skills gaps

Threat hunting is complex and requires specialist skills. If you don't have the experience in-house, explore training courses to help develop the necessary skills. Also, consider working with a third-party provider to supplement your team.

5. Develop and implement an incident response plan

Before you start threat hunting, it is essential to have a fully-fledged incident response in place to ensure any response is measured and controlled. Having a well-prepared, well-understood response plan that all key parties can immediately put into action will dramatically reduce the impact of an attack on your organization.

A good incident response plan should outline protocols for preparation, detection, and reporting, triage and analysis, containment and neutralization, and post-incident activities. For tips on building an effective incident response plan, refer to our incident response guide.

For further practical guidance on preparing for and conducting threat hunting, be sure to check out the Sophos Threat Hunting Academy.

How Sophos can help

As we've already mentioned, effective threat hunting is incredibly complex, requiring next-generation technologies coupled with extensive human expertise. Fortunately, Sophos can support your threat hunting objectives irrespective of your cybersecurity maturity.

Preventing threats from breaching your network – Sophos Intercept X Endpoint

Threat hunters can only conduct their roles efficiently if they aren't inundated with security alerts. One way to achieve this is to introduce best-in-class prevention technologies so that defenders can focus on fewer, more accurate detections and streamline the subsequent investigation and response process. Enter Sophos Intercept X Endpoint.

Sophos Intercept X is the industry-leading endpoint security solution that reduces the attack surface and prevents attacks from running. Combining anti-exploit, anti-ransomware, deep learning AI, and control technology, it stops threats before they impact your systems. Intercept X uses a comprehensive, defense in-depth approach to endpoint protection rather than relying on one primary security technique.

The prevention capabilities in Sophos Intercept X endpoint protection block 99.98% of threats (AV-TEST average score Jan-November 2021). Defenders can then better focus on the suspicious signals that require human intervention.

You can learn more about or take a trial of Intercept X Endpoint here.

Conducting threat hunts yourself– Sophos XDR

Designed for security analysts working in dedicated SOC teams and IT administrators covering security and other IT responsibilities, Sophos XDR enables your team to detect, investigate, and respond to incidents across endpoint, servers, firewall, cloud workloads, email, mobile, and more.

Immediately get to the information that matters to you by choosing from a library of pre-written, customizable templates covering many different threat hunting and IT operations scenarios – or write your own. You have access to live device data, up to 90 days of on-disk data, 30 days of data stored in the Sophos Data Lake cloud repository, and an automatically-generated list of suspicious items, so you know exactly where to start.

If you would like to try out Sophos XDR to conduct your own threat hunts, Sophos gives you the tools you need for advanced threat hunting and security operations hygiene. You can either start an in-product trial (if you have a Sophos Central account) or take a trial of Sophos Intercept X, which includes XDR.

Threat hunting as a fully managed service or to supplement your team – Sophos MDR

Sopho MDR is a multifaceted, comprehensive, and award-winning MDR solution that brings the expertise and skill of the Sophos team of security analysts and their vast array of capabilities to bear on your network and cloud environments. Sophos effectively becomes an extension of your security operations, adding its vast capabilities to your own.

The Sophos MDR team of threat hunters and response experts will:

- Proactively hunt for and validate potential threats and incidents
- Use all available information to determine the scope and severity of threats
- Apply the appropriate business context for valid threats
- Initiate actions to remotely disrupt, contain, and neutralize threats
- Provide actionable advice for addressing the root cause of recurring incidents

Even if your organization has a mature security operation center, you might want a second set of eyes monitoring their environment to ensure nothing slips through the cracks. Sophos MDR brings together threat hunting and endpoint protection while providing oversight and expertise every day. Your network and cloud assets are a top priority to the Sophos network analysts and threat hunters who monitor and actively remediate and neutralize threats on your behalf.

With a good MDR service, you and your organization can sleep well knowing that there is a team of skilled experts constantly monitoring your organization, hunting threats, investigating suspicious activity, and responding to potential incidents. With the ever-growing cybersecurity threat landscape, there is peace of mind when working with a team whose entire focus is cybersecurity.

To discuss how Sophos MDR can support your organization, speak to your Sophos representative or request a callback. In the meantime, catch up on the latest MDR research and casebooks.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

22-08-08 WP-EN (PC)