DEMYSTIFYING THREAT HUNTING

F-Secure Whitepaper

F-Secure

CONTENTS

Why this whitepaper matters 3
Confusion in the marketplace 4
What threat hunting really is 6
Continuous response 7
Good threat hunting unpacked 10
The future of threat hunting 14
Conclusions 16

WHY THIS WHITEPAPER MATTERS

"Threat hunting" has become something of a buzzword in the cyber security industry, and like any other buzzword the term is often misused – it is not uncommon to see vendors renaming their traditional security operations services "threat hunting" while doing nothing to improve the outcome being delivered.

We wanted to clear up the confusion. Demystifying Threat Hunting will explain:

- What threat hunting is – and what it isn't.
- What's Continuous Response and why you need it.
- Why Continuous Response and threat hunting are both required to successfully defend against targeted attacks.
- Good threat hunting unpacked.
- The future of threat hunting.

We've also produced a short film which features our own threat hunters talking about their craft in their own words. You'll find a link to it later in the whitepaper.

1. CONFUSION IN THE MARKETPLACE

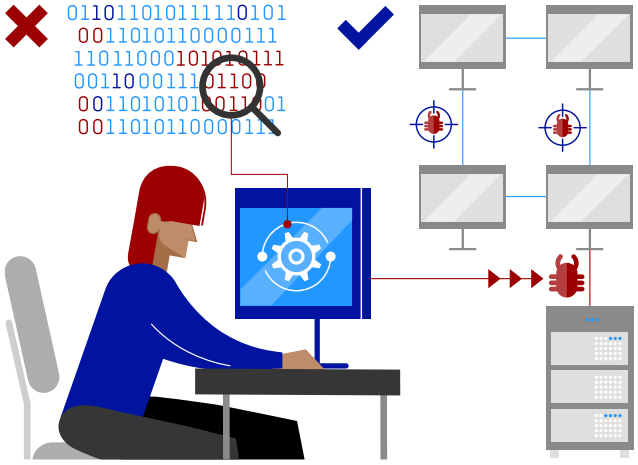
At F-Secure Countercept, we wanted to provide clarity on what threat hunting actually is, why it's important, and what is needed to be a successful practitioner of this critical skill. However, before you can do this, we first need to separate fact from fiction associated with this often misunderstood term.

Myths and misconceptions about threat hunting

1

Myth: Threat hunting is manually hunting through raw data to find an attacker.

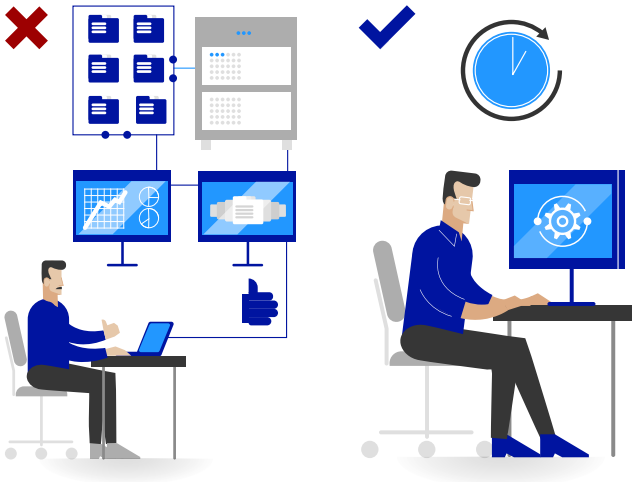
Reality: A single host will generate well over 1 million events in a day. Having someone hunt across all that data in search of multiple potential attack techniques would be a waste of time. Rather than a laborious and ineffective manual search, threat hunting is about identifying the gaps in your detection capability and developing use cases for your detection tooling that will plug those gaps before an attacker can exploit them.



2

Myth: Threat hunting is a one-time activity, e.g. a "hunt sprint" across an organization.

Reality: Attackers are always looking for new techniques that are cheaper and more effective than what they're currently using. If attackers never stop looking for new ways in, defenders can never stop looking for new ways to keep them out - by definition, this cannot be a one-time event.



3

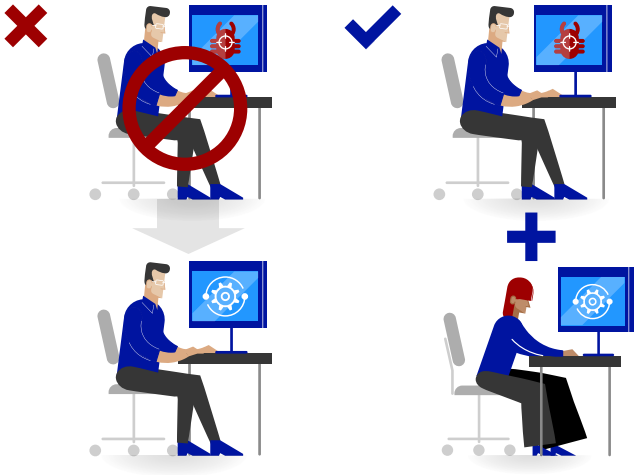
Myth: Threat hunting is the modern way for security operations centers to work.

Reality: Threat hunting is not a new and sexy methodology that security operations centers will use to replace their existing methodology - despite what their marketing may say! Threat hunting is complementary to detection & response operations rather than a replacement for them. Both are necessary to effectively defend against attackers.

4

Myth: Managed threat hunting is a replacement for Managed Detection & Response.

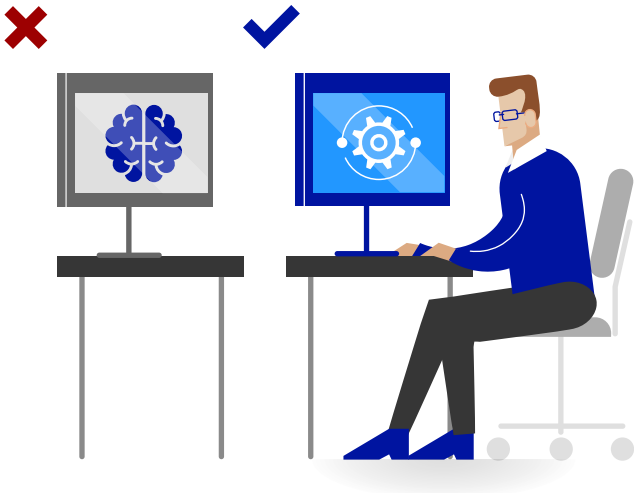
Reality: MDR is about minimizing the impact of an attack on an organization by providing a detection & response capability that the organization cannot deliver themselves. Just adding 'hunters' into a detection & response workflow doesn't change MDR into managed threat hunting. Any credible MDR vendor will employ threat hunting alongside core operations to ensure that their detection capability continues to develop and remain effective.



5

Myth: Threat hunting can be automated with artificial intelligence.

Reality: The most effective Threat Hunters are trained to think offensively, identifying gaps in detection capability that could be exploited by an attacker. Artificial Intelligence isn't capable of thinking creatively at the level required - while some security challenges can be solved with data analytics alone, threat hunting isn't one of them.



2. WHAT THREAT HUNTING REALLY IS

Threat hunting grew out of a need – to be able to defend against the range of targeted attacks that were bypassing even the most innovative of security tools. Tools and methodologies can only take you so far unless you recognize their limitations and are constantly looking to improve on their capabilities. Threat hunting is all about identifying areas that your detection capability doesn't cover, then deriving use cases that can plug those gaps. Threat hunting complements and enhances your detection capability by ensuring that gaps are discovered and dealt with before an attacker has the chance to exploit them.

WHAT IS THREAT HUNTING?

- A continuous improvement process for developing detection use cases.
- Ongoing research into attacker techniques, based on the adoption of an attacker mindset.
- An experiment in assuming compromise across an estate.
- An activity whose success is defined by the quality of the detection use cases implemented.
- A necessary component in the defense against targeted attacks.

Threat hunting allows defensive teams to identify additional data sets and sources needed to detect future advanced attacks. By developing hypotheses and simulating attacks, threat hunting builds a detection roadmap based on attack types identified by the team responsible for detection and response.

"Evolving threat landscape" is also a something of an overused phrase, but it is one that is rooted in reality – attackers are constantly looking for and developing new techniques that are more effective and cheaper than those they were using before. Defenders will not be able to compete unless they employ a methodology designed to combat the constantly evolving nature of attack techniques.

Threat hunting isn't the only component required for successfully defending against targeted attacks. It doesn't replace the need for an effective detection and response capability underpinned by a team with the right expertise and focused on using the best tools available for the job.

A detection and response team needs to have a combination of offensive understanding, investigative know-how, and response training to be effective. The methodology we developed to achieve this capability is called Continuous Response. To successfully defend against targeted attacks, both threat hunting and Continuous Response are needed. We explain this methodology in Section 3.

3. CONTINUOUS RESPONSE

What good is detection without response?

Targeted attacks – by their very nature – will bypass all your preventative controls.

Although there is much more detection-focused tooling on the market than there used to be, EDR being the primary example, most organizations still suffer from two major problems:

- They don't have enough of the right people who can investigate an alert to determine if it's genuinely malicious activity.
- They lack the understanding and know-how to respond appropriately if malicious activity is detected.

These problems are clear when you examine the data on breach response time. The time between the occurrence of a breach and its containment (also known as the breach lifecycle) grew noticeably between 2018 and 2019 [1].

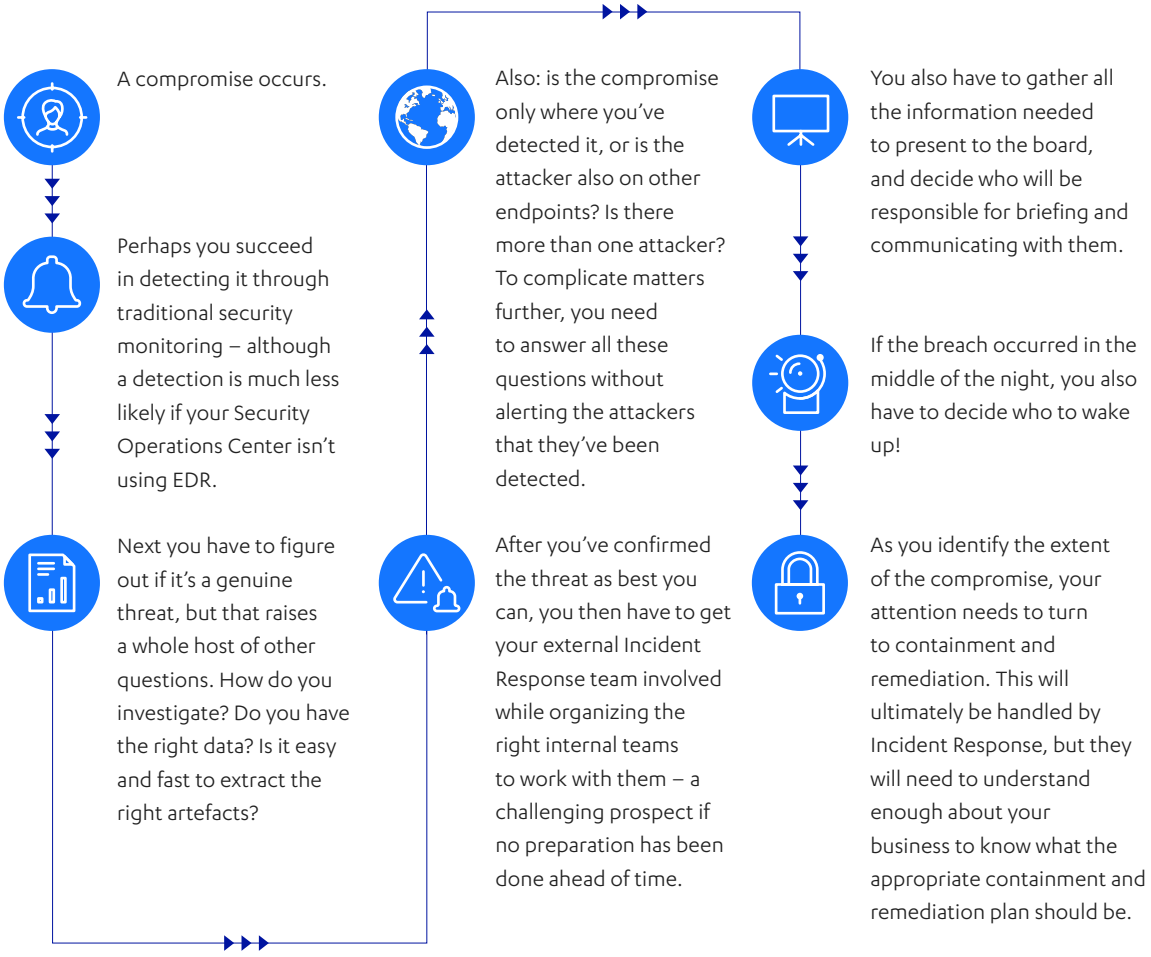
WHY DOES THE RESPONSE GAP EXIST?	
87% of targeted attacks are being executed within minutes [2]	"The time from the attacker's first action in an event chain to the initial compromise of an asset is typically measured in minutes." [2]
But are not being discovered at the same pace, with some taking 'months or more' [4]	"The average time to identify a breach in 2019 was 206 days." [5]
After discovery, slow response gives attackers more time to achieve their objective.	"The average time to contain a breach is 73 days." [6]

The time needed to contain a breach is sometimes referred to as the "response gap." In general the longer the response gap, the bigger the impact on the organization that has been attacked. At 73 days, the average response gap gives an attacker a long time to try and achieve their objective.

[1] Ponemon Cost of a Data Breach 2019
[2] 2018 Data Breach Investigations Report - Verizon
[3] Ibid
[4] Ibid
[5] Ibid
[6] Ponemon Cost of a Data Breach 2019

Why does the response gap exist?

Imagine this scenario:



All these things take time, and the potential impact of the breach is increasing continuously. A motivated attacker won't just wait around for you to organize your response.

What do you need to stay ahead? How can you detect – and respond – to minimize business impact? With Continuous Response.

The three Cs of Continuous Response

Continuous Response is our term for an approach that combines detection and response into a single methodology. When an attack is confirmed, defenders can act immediately to contain the attackers and frustrate their ability to achieve their objectives – even before a remediation plan has been put in place. Defending against sophisticated cyber-attacks requires an equal balance of detection and response. Continuous Response is all about:

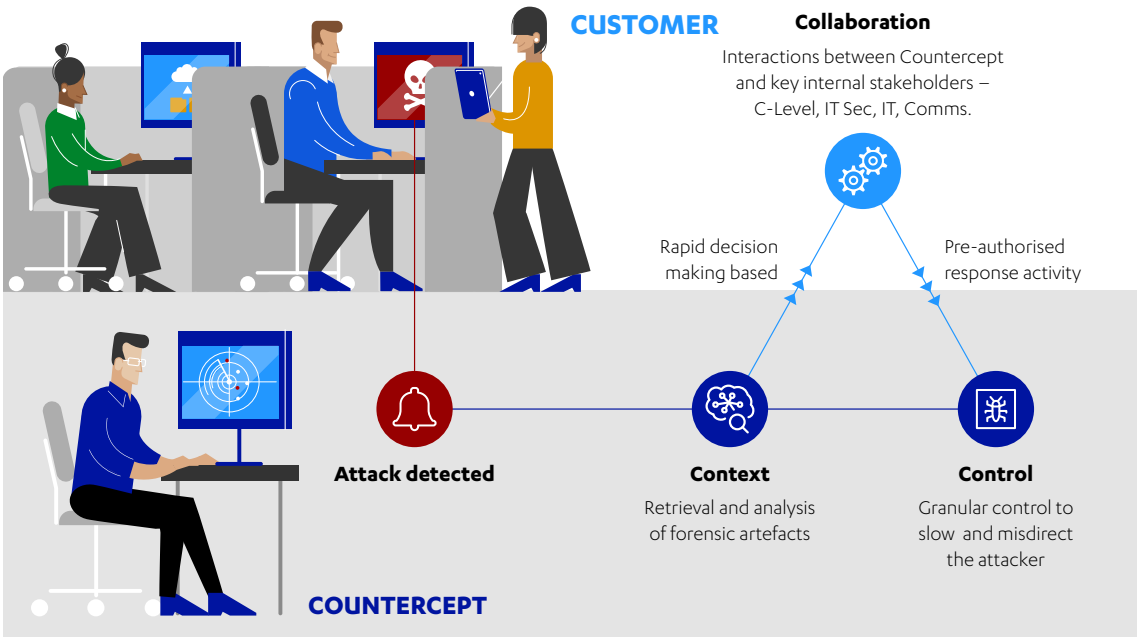
Having experts who know how to investigate suspicious activity to determine whether it is actually malicious by retrieving and analyzing artefacts. It's essential to build up your picture of the attack during the breach, not as a post-breach activity.

Being able to contain and disrupt the attacker once an attack is confirmed, until a full remediation plan has been developed and agreed. Containment and disruption is important to minimizing business impact.

Remediating the attacker's activity by killing their C2 channels, deleting whatever mechanisms they are using for persistence, and removing their foothold in the organization.

Continuous Response is a combination of Collaboration, Context, and Control. It puts the right people in the right place at the right time (Collaboration), while equipping them with the right information to make a decision (Context), and the ability to take the right action (Control).

HOW DOES CONTINUOUS RESPONSE WORK?



4. GOOD THREAT HUNTING UNPACKED

The elements of good threat hunting include cultivating an offensive mindset, giving people time to think, giving them access to the tooling and data they need, and collaboration with red teams and Incident Response teams.

Offensive mindset

Being able to think like an attacker means that blue teams don't just have to react to attack techniques that have already been seen in the wild – they can anticipate where attackers are likely to go next and develop their defensive capability first.

Being able to think like an attacker requires:

A detailed understanding of and familiarity with the techniques and attack paths that attackers are using to bypass security tools. Our team members undertake practical offensive qualifications, such as OSCP, and spend time shadowing our Targeted Attack Simulation teams.

A detailed understanding of underlying technologies, such as operating system internals, to know what can be exploited and what can be masked as normal-looking activity.

A knowledge base of attacker behaviors. The breadth and complexity of attack techniques mandates that any successful team must build up and maintain a wide body of knowledge about how attackers operate. Open-source models like MITRE ATT&CK™ are excellent starting points, which should be built up based on research and experience related to the organizations being defended.

Giving people time to think

One of the most important developments in the evolution of threat hunting has been the creation of an organizational structure that gives people time to think. This includes understanding that core detection & response operations and threat hunting should be delivered by the same team – but not expecting people to do it at the same time.

Having the same team deliver operations and continuously improve the capability that enables those operations creates a culture of mutual responsibility. For example, if the team develops a noisy rule, the same people will have to deal with the outcome and can therefore be counted on to fix it. It also vastly improves the operational effectiveness of team members as they have an intimate understanding of the underlying detections.

Having the same team deliver operations and continuously improve the capability that enables those operations creates a culture of mutual responsibility.

If threat hunting is all about looking for things that evade your detection controls, then it requires an understanding of what you can detect. With this understanding, you can then prioritize your threat hunting activities based on your weaknesses. You can also use this to demonstrate capability improvements and the effectiveness of your threat hunting activities. If success is defined as finding active threats, it will be difficult to justify the time invested in research –despite the fact that research time is essential. Success should be measured as the demonstrable improvement of your detection & response capability.

Giving people dedicated time for research and threat hunting also ensures that team members are kept engaged, challenged, and ultimately motivated by having different tasks to focus on in the role. Retention is an issue in teams responsible for delivering security operations, and ensuring that the role includes a variety of interesting tasks is vital for keeping retention high. The only downside of this approach is that such varied skills are harder to find and develop. However, this is less true for organizations that make a point of building the right culture for the job. Providing flexibility and encouraging team members to become trained in a wide variety of specialist skills also keeps engagement high and helps with attraction and retention.

Giving people dedicated time for research and threat hunting also ensures that team members are kept engaged, challenged, and ultimately motivated by having different tasks to focus on in the role.

Research needs blocks of uninterrupted time to be effective – regular context switching is not conducive to effective research. At F-Secure Countercept we structure shift patterns so that each team member has at least one day per shift pattern where they can focus exclusively on threat hunting. This ensures that all team members regularly get stretches of uninterrupted research time. By planning 25% of the team's time for threat hunting, we ensure people regularly get this uninterrupted time. As an added benefit, we have stretch capacity and backup for if operations become particularly busy.

Tooling and data

To develop new detection capability, Threat Hunters need access to raw data rather than alerts from other systems. Correlation and aggregation of other alerting has its utility, but it primarily serves to improve efficiency in analysis. To facilitate all types of analysis, API access to the data is required, along with the freedom to experiment with various data analysis techniques.

It's also important to have a flexible tech stack. Threat hunting will occasionally reveal the need for new telemetry sources or other requirements. Being able to quickly update your tech stack to facilitate the latest type of attack can be very useful.

Threat hunting can be intimidating for a newcomer to the discipline. It's important to have tooling such as Kibana that enables easy exploration and analysis of data, followed later by more complex analysis techniques using Python or similar tools. Sharing techniques and code through collaboration tooling such as Jupyter further enables team members to contribute.

Much of our intelligence goes into determining exactly what is useful to detect, rather than complex analysis techniques.

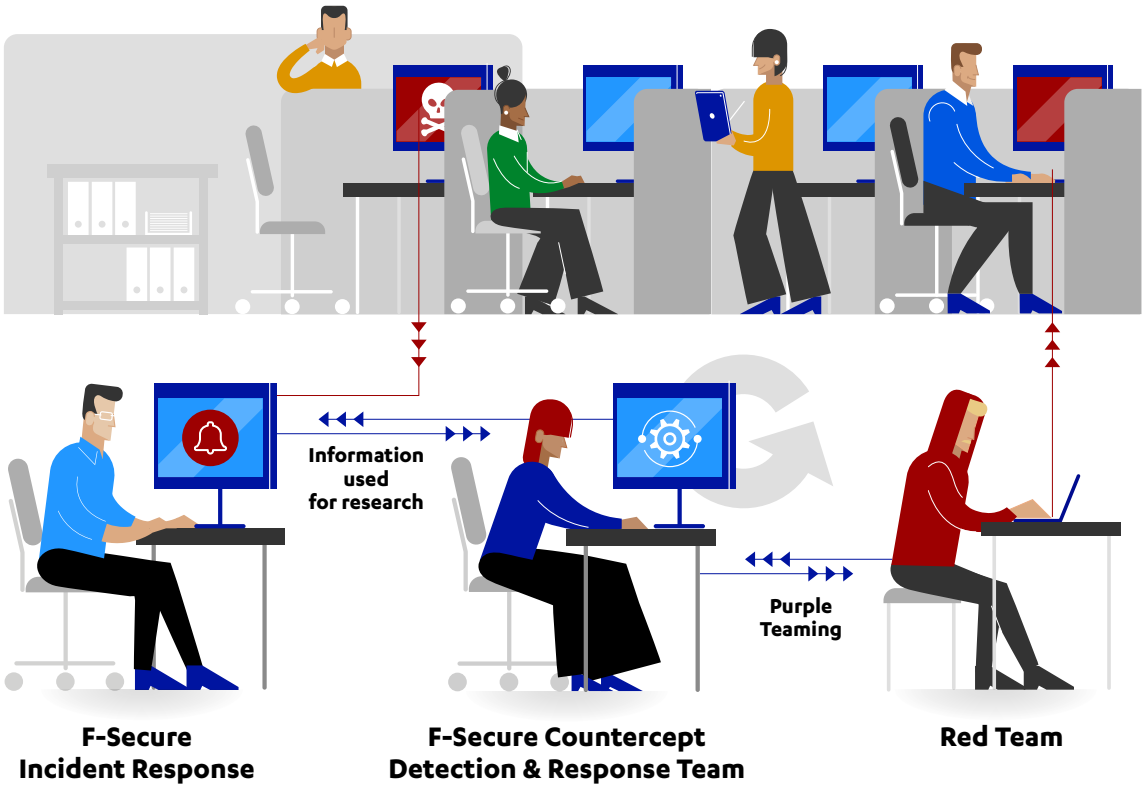
Data analysis techniques should be kept as simple as possible. Although terms like "machine learning" and "artificial intelligence" are sexy and exciting, you can go a long way, and at a much quicker pace, with simple string matching, least-frequency analysis and data tables. Much of our intelligence goes into determining exactly what is useful to detect, rather than complex analysis techniques. Of course, some scenarios call for more complex analysis. For example, User Behavior Analytics typically requires learning what is "normal" for a particular user, and machine learning is useful for this task. Such techniques should be viewed as a tool in the hunter's belt, not the answer to the overall problem.

Continuous testing is essential for good threat hunting. As you get into the habit of continuously improving your detection capability, it is important to ensure you don't break what you've already got! To achieve this we have developed a testing framework that periodically spins up virtualized infrastructure, automates pre-determined attack paths, and checks that all the expected detections are generated. Although there are many checks and balances prior to rule deployment, things occasionally slip through the cracks. Having a test that is as close to the real world as possible is invaluable.

Collaboration with red teams and incident response

The aim of the game is to defend against attackers. Competing against red teams is a great way of learning and researching; 'paper-based' research is no substitute for the real thing. Although your threat hunting team will be offensively trained, having a fresh perspective from another offensive team will help uncover blind spots and test your team outside of laboratory conditions. Good red teams do their own research as well, which ensures that blue teams are being tested against the latest capabilities. Purple team exercises can also help with this process.

IR teams learn vital information about attacker behavior from the incidents they contain and remediate. This information can provide a valuable source of insight that can be used to develop new detection capability. This is something that can be done during an incident. Rules can be developed as a compromise is being assessed in order to automate their detection, rather than having to find other compromised machines solely through investigation. This approach has already proven successful on a number of occasions.



5. THE FUTURE OF THREAT HUNTING

No one truly knows what the future may bring, but there are trends and emerging technologies that give us a clue of where threat hunting will go in the future and what needs it will serve.

What do we think the future will bring?

Moving away from the endpoint

Attackers are still most active on endpoints and therefore Threat Hunters continue to focus most of their attention there. As organizations continue to move to cloud-hosted services, working in the browser, and with modern operating systems, attackers will increase their focus on these areas. In anticipation of this trend, Threat Hunters should also begin to take a closer look at those areas as they will present gaps in existing detection capability that attackers will look to exploit.

Standardization of the term

Threat hunting within the cyber security industry can still mean a wide variety of things – this post details what we mean by the term but plenty of vendors still use it in other ways today. We expect and hope that the definition of threat hunting will become more standard in the future allowing practitioners to focus on best practices, tooling and knowledge exchange, and enabling buyers to clearly interpret the impact when the term is used.

Threat hunting goes mainstream

For organisations with appetite and budget to develop an internal capability, threat hunting, as described in this post, will become the de facto approach to attack detection capability improvement.

This will bring several benefits. Firstly, the incumbent and (un)popular analyst role will become less necessary, as Threat Hunters will be far more engaged in operations and the overall capability. Exposing present-day analysts to threat hunting should bridge the skill gap through exposure and increase staff retention.

Secondly, as organizations frame the value of threat hunting in terms of capability improvement (rather than necessarily finding threats), they can more easily justify the investment of time. Additionally, as a more defined process is being followed, that time is used more effectively.

Ideally "threat hunting" as we know it will become the de facto approach by which organizations develop their detection capability. This will be helpful for attracting and retaining blue team talent, which will in turn help push detection forward. As this occurs, we can expect threat hunting to be recognized as one of the most exciting and impactful disciplines within cyber security. More people are recognising that the practice of threat hunting continues to result in tangible improvements to a company's cyber security posture.

Improved tooling and technique development puts attackers at a disadvantage

As blue teams become as collaborative and fast-paced as red teams have become, the growing popularity of this discipline will accelerate everything from the talent involved to the capabilities of threat hunting teams. Empowered by threat hunting's continuous improvement process, blue teams will drive a shift towards more collaborative tooling and technique development specifically designed for threat hunting, forcing attackers onto the back foot.

Sharing of rule logic

One of the biggest challenges many teams face today is finding teams skilled enough to build detection logic for their organisation. Although the security industry is well practiced in sharing knowledge in human-readable forms, work is required to understand and translate this into sensible automation. Projects like Sigma have the potential to create a framework that allows for rule logic to be shared, removing or reducing the redundancy of creating rule logic over and over again at different organizations for the same attacks. Removing rule redundancy at all organisations for generic attacks (attacks on Windows endpoints, Active Directory etc.) will allow threat hunting teams to focus further down the kill chain for scenarios more specific to their organization. As endpoint technology normalises, we expect to see this kind of capability sharing as the natural extension of already popular knowledge sharing projects, such as ATT&CK.

6. CONCLUSIONS

With so many vendors using “threat hunting” as more of a buzzword than anything else, it’s no wonder the real meaning of the term has become obscured. In Demystifying Threat Hunting, we’ve covered the key myths and misconceptions about what threat hunting really is, and provided a clear definition of the term: threat hunting is the process of identifying gaps in your detection capability and developing use cases for your detection tooling that will plug those gaps before an attacker can exploit them.

We’ve also explored Continuous Response, our term for an approach that combines detection and response into a single methodology to allow defenders to contain and frustrate attacks as soon as they occur. We’ve explained that Continuous Response is an evolving discipline of constant improvement, and that threat hunting is a key feed into that loop ensuring our detection and response capabilities remain highly effective at detecting and responding to targeted attacks.

We’ve touched on the elements of good threat hunting, including the need to cultivate an offensive mindset, to collaborate with red teams and Incident Response teams, and critically, to give Threat Hunters the space and time to dedicate to research along with access to the right tooling and data – all of which is baked into F-Secure’s approach to the discipline.

Finally, we’ve shared our thoughts, observations and predictions about the future of threat hunting, giving you a window into developing trends.

Watch a short film which features our threat hunters talking about their craft in more detaill

Follow us on Twitter to get a fresh perspective on our industry

Meet one of the F-Secure Countercept team

ABOUT F-SECURE

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and innovations in machine learning. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats.

Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

f-secure.com/business | twitter.com/fsecure | linkedin.com/f-secure

F-Secure