White Paper

A Checklist for Effective Threat Hunting

Top Requirements for Cyber Analysts and Management

securityhq.com

SecurityHQ

Table of Content

Executive Summary

In our last white paper 'The Fundamentals of Threat Hunting. Hunt Like a Pro' we brought to light the fact that most organisations had a very limited understanding of what threat hunting is, and that without the right threat intelligence it is practically impossible to know what information is available across all digital platforms. Especially regarding business information and data. In fact, we concluded that most organisations are unaware of who or what is targeting them at any given time. And what organisations do know, often gets confused with other areas of detection and response.

In response, our previous paper covered some of the basics, including the answers to the following questions: What is threat hunting? Where does threat hunting fit? What is needed to start threat hunting? What triggers threat hunting? What are we hunting for? What is threat hunting skill mapping? With an ending discussion on the outputs of threat hunting.

In this paper, we take this discussion a step further to provide a checklist of key questions analysts and management must make when implementing threat detection. We do this by exploring an example strategy and hypothesis, followed by an examination on what we are hunting for, what does threat hunting look like, a look into tracking threat hunting, what are the outputs of threat hunting, and an acknowledgment of the current limitations of threat hunting publicly available.

'Threat Hunting is all about knowing the 'Unknown'. Security controls in place can be trusted to detect traditional attacks. However, Threat Hunting if performed with relevant context driven by intelligence and analysis helps to catch novel cyber-attacks. In the end, it is all about connecting the dots to have a broader picture of your network.'

- Swapnil Bohsale, Security Consultant, SecurityHQ

Key Terms

Abbreviations used in this paper include:

TTP's – Tactics, Techniques & Procedures

IOC's – Indicator of Compromise

APT – Advanced Persistent Threat

DNS- Domain Name Service

IPS – Intrusion Prevention System

EDR- Endpoint Detection & Response

Threat Hunting Outline

Threat Hunting, as mentioned in our previous paper, is a process, not a one-off activity. It requires planning, it requires ideas, and it requires attack theories. It is important that we call it a process because it is bigger than just a one-off task. Think of it as a continual loop.

This loop is used to find unidentified threats in a network, to identify current or historical attacks, breached corporate material, credentials, intellectual property and brand infringement by harvesting data available on the visible, dark, and deep web. This is done by analysing both current and historical security logs, pulling data apart and analysing the anomalies.

Threat Hunting is all about creating a plan, selecting a focus, and creating a hypothesis. Valuable data from threat hunting can come from sources such as:

- DNS Logs
- Network Proxy Logs
- Firewall Logs
- Endpoint & Server Activity Logs
- Active Directory Logs
- Email Gateway Logs
- Operating System Logs

Once the data is collected from these sources, it can be analysed, and the response can be actioned.

Key Questions for Analysts

1 Analyst Questions

Threat hunting is an active defence. Which, as The National Cyber Security Strategy 2016-2021 paper on Detecting the Unknown: A Guide to Threat Hunting argues, 'departments first need to sufficiently mature their Architecture (e.g. Vulnerability Management), Passive Defence (e.g. Technical Controls such as firewalls) and other Active Defences (e.g. Protective Monitoring), while operating a mature Intelligence capability to add value to and enable Threat Hunting.'

They go on to state that 'according to the SANS 2017 Threat Hunting Survey (7), only 35.3% of the 306 organisations surveyed (of which 14.4% were government) hunted on a continuous basis. This rose to 43.2% of the 600 organisations surveyed in the SANS 2018 Threat Hunting Survey (8). Additionally, in the 2017 survey, only 4.6% of respondents were using externally published guidance, suggesting little existed in terms of industry good practice for Threat Hunting. Structured Threat Hunting performed on a frequent basis provides an effective means of reducing risk across the organisation'.

This means that to provide structured threat hunting, a Security Operations Centre (SOC) based threat hunting capability needs to be implemented to reduce risk. Within a SOC, threat hunting needs to be conducted by a threat hunter who can proactively search for threats. SOC analysts, incident response teams and threat hunters have similar skill sets in that they must understand the threat landscape as it continually evolves for a specified industry or geography, they understand all the systems and processes and have the security operation skills to be able to know the limitations and capabilities of controls on a given network.

Once a threat hunter/ analyst is more experienced, they will naturally have skills that fit within the realms to investigate a breach at depth.

The below questions are typically asked by the analysts performing the threat hunt.

1. Do we have any of the IOCs in our environment?

2. Is the network under active attack? Say, for instance, that the analyst has been given a bunch of IOCs from threat intelligence, from research, from blogs, from authorities, they then need to question if any of these are in the environment.

3. Have we observed any suspicious TTP's in our environment? If so, what?

4. Do we know if a server was vulnerable, and do we know if that vulnerability had an exploit available? What happened on that server? Has that vulnerability ever been exploited? Has anything malicious been planted there?

'My message for companies that think they haven't been attacked is you're not looking hard enough.'- James Snook, deputy director in the office for cyber security, Government Cabinet Office, London, April 2016

Key Questions from Management

2 Management Questions

In the words of Mr Ernest Tan Choon Kiat, 'Once we escalate to management, there will be no day, no night.' This is true, as management need to ask many questions following an escalation. But it is also crucial that these questions are answered in rapid speed.

Speed is crucial, because once an attack has been detected, management need to ask the following questions to improve their processes and reduce their response time for subsequent attacks.

1. Why did we not detect the attack in the first place? Say, for instance, if we are doing threat hunting, why didn't we get that alert in the SOC to tell us about the activity?

2. How can we improve detection capabilities for similar attacks? Because we did not detect it in the first place, what can we do to improve detection the next time it happens?

3. What was the impact of that attack that was discovered through threat hunting? So, say you didn't have any detection for it, which means it could have been a new or advanced threat, you found it through threat hunting, what was the actual impact of that attack? Management needs to ask about the genuine scale of this compromise, and what to be concerned about.

If you knew a building was going to be targeted for a robbery, and it had a vulnerability like an open window, would you do nothing, or would you be proactive and find that open window, close it, stop the thief, and create better defences for future attacks?

Once the above questions are asked, better systems can be put in place to ensure the same issues do not arise and cause more issues to the business.

To do this businesses need to put in place strategies. Strategies such as the following scenarios presented.

Strategy & Hypotheses Examples

There are two key examples of high-level strategies.

1. A strategy could be, for example, for the next 6 months, you (the analyst) tell the team that you are going to focus on the detection of a particular APT of interest and their activity in the environment, and in the network. So, you might pick a single APT, and focus on their TTP's, and focus on their recent attacks. From that, you can investigate whether you are likely to be targeted by this APT or not.

2. Threat hunting as a service works when your team focus on threat hunting in a particular part of the business that is known to have poor security controls i.e., data security & insider threats. In a big environment you will have legacy systems, you will have teams that are running legacy software that cannot be touched due to stability concerns, you will have teams running operating systems that they dare not put an EDR agent on. All these things contribute.

Those are two high-level strategies.

Threat Hunting Hypothesis Behind Threat Hunting Examples

1. If users within the business have the ability to send outbound emails, then data leakage could be possible. So, threat hunting can focus on detecting sensitive data leaving the boundary to prove if sensitive data leakage has happened or not.

2. If an attacker wanted to maintain persistence on a server, one way to do that would be to modify a registry key on that servers operating system. So, the threat hunter needs to go and compare the registry values across the same servers, for example that are public facing. Then questions need to be asked. For example, are there any registry key values that are different? Does one stand out? If they are not consistent then why not? Are they running the same application? It's about knowing what an attacker could do and then proving or disproving it.

That is the strategy you approach with, and then formulate the hypothesis behind it.

Tracking Threat Hunting

Tracking threat hunting actively is hugely important to measure the proactiveness of the team, and response to threat intelligence. Inside SecurityHQ, we ensure the following elements:

1. All threat activity is tracked by the SecurityHQ ticketing platform for reporting and oversight.

2. Each threat activity task is assigned an owner who is responsible for the threat hunting activity.

Synopsis & Outputs of Threat Hunting

Threat Hunting will typically create outputs. These include the follow key points.

1. **Threat Hunt Reports -** In complex Threat Hunts it is important to produce a Threat Hunting report which can be used for historical reference and for sharing knowledge with the team.

2. **New Detection Rules -** New detection rules often come from Threat Hunting activity. If no malicious activity has been detected, detection rules are created to catch any future activity matching similar patterns of an attacker.

3. **Identify Anomalies -** There may be scenarios during a Threat Hunt when an analyst detects benign anomalies within the environment, i.e., noisy scripts and strange account behaviours.

4. **Improved Prevention -** Regardless of the outcome the output should aim to also drive improvement with regards to prevention, to stop similar attacks from happening in the future.

To learn more about Threat Hunting, Download our Datasheet.

Or, for a more direct approach, get in touch with one of our expert analysts.

Authors

Barlow, Eleanor

Content Manager, SecurityHQ

As an experienced named author and ghost writer, Eleanor specialises in researching and reporting on the latest in cyber security intelligence, developing trends and security insights. Eleanor holds a first-class degree B.A. (Hons) in English Literature, and a master's degree (M.A.) from the University of Bristol.

Hambleton, Aaron

Security Monitoring & Incident Response Lead, SecurityHQ

With 10+ years of experience in cyber security, Aaron has worked in Financial Services, Retail, Insurance, Government, and Telecommunication industries as a security consultant and incident response analyst. Aaron is a GIAC certified Defence Analyst with extensive knowledge in Security Blue Teaming, Incident Response, Cyber Security Operations, Cloud Security, and Cyber Security consultancy in an advisory capacity.

https://www.linkedin.com/company/threathunting

How Does SecurityHQ Differ?

SecurityHQ is a Global Managed Security Service Provider (MSSP) that detects, monitors & responds to cyber threats 24/7, to ensure complete visibility and protection.

The right combination of tools, skills, people, and processes is essential to manage, detect and defend your environment from all malicious activity proactively and effectively. Our mission is to provide world-class security operations, to empower our clients and partners, to integrate processes seamlessly, and act as an extension of our user's own teams to address specific risks and challenges and improve security posture.

Which is Why...

We are enabling

the security of clients across the globe in every vertical.

We are collaborating

with partners to provide enterprise grade solutions tailored to client and industry specific needs.

We are helping

businesses feel protected, by delivering **24/7** visibility, every minute of every day, 365 days a year.

We are supporting

organisations with a team of **250+** experts available on demand.

Integrity & Transparency

Our code of ethics is fundamental, not only to our business success, but to the growth of all that we value. We place the power of our SOC team into the client's hands, providing complete visibility of the digital footprint, systems and processes, specific threats, and security posture.

Incident Management Platform

Collaboration is critical for effective security operations. Our incident Management & Analytics Platform provides a single pane of glass for incident workflows, SLA management, data visualisation and document repository.

Innovation

Cyber threats are increasing, both in terms of volume and sophistication. Which means that traditional approaches need to be re-evaluated. SecurityHQ combines best-in-business technology, processes, and expert minds to provide solutions to your security needs.

Bespoke & Engineered

Every client is different. Your risks, geolocations, regulatory requirements, and processes demand a bespoke response. We provide tailored services based on clients' specific needs. Built from the foundation up, our team of expert engineers know exactly what is required.

Have a question? We would love to hear from you.

Safeguard your business, people and processes with SecurityHQ.

Reach us

sales@securityhq.com | +44 (0) 20 332 70699

Americas	+1 312 544 0538
APAC	+91 9359609941
Europe	+44 20 332 70699
Middle East	+971 4354 9535

Follow us f in 🐦 ▶