CYBERSECURITY SKILLS FOR 2021

Threat Hunting for Effective Cybersecurity

How to Protect Critical Assets Through Systematic, Proactive Threat Intelligence

Table of Contents

Each chapter is linked for easy skimming

1 Introduction to Threat Hunting Page 3

2 Prerequisites for a Threat Hunt Page 5

3 Step 1: Define Your Threat Hunt Page 7

4 Step 2: Equip Your Threat Hunt Page 8

5 Step 3: Finalize Your Threat Hunt Plan Page 9

6 Step 4: Execute the Threat Hunt Page 10

7 Step 5: Evaluate the Threat Hunt Page 12

8 Step 6: Share and Act on Your Findings Page 13

9 Conclusion Page 14

10 About Sixgill Page 15

Introduction to Threat Hunting

What is It, Who is It for, and Why?

For today's companies, cybersecurity is often an uphill battle. On the one hand, **cybersecurity spending continues to grow**, while new security technologies are constantly being developed. But on the other hand, **cyberattacks** continue to plague major businesses and organizations (and even, recently, **parts of the U.S. government**).

Between increasingly sophisticated hackers and a **legal landscape** that threatens to punish those companies that fail to adequately protect their customers' privacy rights, it's not hard to see why cybersecurity professionals are so concerned about the risks they face. Adding to the problem, many major cyberattacks are allowed to continue for an extended period before the victims discover them and take action. In fact, it now takes an average of 280 days before a data breach is detected and contained, according to **IBM**.

If even today's advanced cybersecurity technologies can't always keep companies safe from major cyberthreats (or even alert them promptly to ongoing cyberattacks), what can these companies do to gain the upper hand? One increasingly promising strategy is to add an extra, proactive layer of security through **threat hunting**.

Threat hunting is seeking evidence that a threat has begun to materialize before you have any indications that the threat has become your reality. By seeking out the highest-priority potential cyberthreats rather than waiting for evidence of them to appear, threat hunting provides a proven, systematic way to defend yourself from the risks that most concern you. Armed with the early warning of cyberattacks that threat hunting often provides, your cybersecurity team can then take action to mitigate a risk posed by threat actors.

Threat hunting is...

seeking evidence that a threat has begun to materialize before you have any indications that the threat has become your reality.

Is threat hunting a viable and worthwhile approach for your company? That depends on the risks you face and how much you have to lose. Although threat hunting is a resource-intensive undertaking, automation has made it viable for more organizations by reducing the time, expense, and skills it requires. Large, well-funded organizations facing substantial risks – such as banks, insurance companies, financial trading firms, gambling or gaming companies, large healthcare conglomerates, governments, and militaries – may have in-house threat-hunting teams. Additionally, smaller, well-funded firms with substantial risks may employ threat hunters as contractors.

Whether your company relies on threat hunting on a full-time basis, works with contractors as needed, or does not currently use this approach to cybersecurity at all, it is useful for today's cybersecurity professionals to understand what threat hunting entails and the benefits it provides. **Not only can this information help you decide whether (and when, where, and how) to turn to threat hunting, but it can shed light on the proactive tools you may have at your disposal to protect your company from cyberthreats.**

What this guide will teach you:

1

What tools and information you need before you can start planning for threat hunting

2

How to set priorities and build a threat-hunting road map

3

The six steps involved in a threat hunt and how to perform them effectively

4

How you can make the most of the information you gather through threat hunting

Prerequisites for a Threat Hunt

Information and Tools

The first piece of information you'll need when planning a threat hunt is likely to be an **inventory of your critical information assets.** In order to make sure your threat hunt is effective and efficient, you'll want to know what relevant data you have, where it is, who can access it, and which safeguards protect it.

The reality is that many companies and organizations carry out threat hunts without a full inventory of their information assets, but it is well worth your time to gather as much of this information up front as possible. The more complete your inventory is before you start, the faster and more complete your threat hunt will be.

Details to include in your inventory:

- Physical and logical topologies
- Network device information (make, model, OS version, and configuration)
- Security control information (make, model, OS version, and configuration)
- Host information (make, model, hardware configuration, and OS version and configuration – as well as the names, versions, and configurations of any applications on that host)
- Pan-host/pan-infrastructure information for hypervisors, content management systems, data interchange systems, etc. (including versions, security controls, and access lists)
- Data flow between apps and hosts for business solutions
- Access controls for all of the above
- Access lists for all of the above
- Locations, types, and formats of logs for all of the above

After you've created this inventory (to the extent feasible), your next step is selecting your most critical data assets and ranking them in order of importance. In a large and well-funded organization, this is typically done either in a risk assessment or by a risk management program.

Which assets are most important to protect? The answer varies widely from organization to organization, based on specific needs, goals, and threats. For example, one company may be most concerned with its financial accounts, while another may be more focused on protecting its intellectual property.

Using investigative tools to identify threats

In addition to knowing which data assets you need to protect, developing a threat-hunting roadmap requires you to have a sense of what threats are out there that may impact your organization. You can get a snapshot of the latest and most urgent threats to watch out for by relying on a cyberthreat intelligence feed such as Sixgill's Darkfeed, which automatically provides real-time updates on threats identified on the deep and dark web. This kind of feed can also be used in conjunction with auto-block rules, enabling you to automatically protect yourself against obvious threats in real time, without relying on a threat-hunting or IT team.

If you have enough cybersecurity resources to support a threat-hunting team, then an investigative research portal is likely a worthwhile investment for you. With a solution such as Sixgill's Investigative Portal, you can take a highly tailored approach to both searching for threats and setting up automatic alerts, based on your industry's threat landscape and the most critical assets listed in your inventory.

Creating priority intelligence requirements (PIRs)

Once you know what your key information assets are, which of them are most critical, and what threats you need to watch out for, you're ready for an analyst to create a roadmap of the most urgent threats to investigate. They should do this by generating a list of **priority intelligence requirements (PIRs)** – a set of very **specific questions** about potential **cyberthreats** that should guide your threat-hunting program. Simply put, your **list of PIRs** should lay out which specific risks you want to investigate and in what order.

With all of this information in hand, your team will be ready to start the **six steps that make up a well-organized threat hunt.**

Step 1

Define Your Threat Hunt

With your list of PIRs in hand, you're ready for an analyst to lay out **your threat hunt**. First, this involves articulating the purpose of the hunt. Why are you about to conduct a threat hunt, and which possible threat will you focus on? Keep in mind that each hunt focuses on one specific threat and answers one main question.

Next, the analyst defines the scope of the threat hunt. This process starts with identifying your assumptions about the hunt and laying out your hypothesis based on your threat intelligence.

At the heart of the hypothesis is a critical question: If the threat that you're worried about happened to you, what evidence would there be? Based on the answer to this question, the analyst can (and should) generate their hypothesis.

For example, let's say threat X uses tools that typically leave the registry key "gotcha" in location Z. If threat X happened, I would expect to find the key "gotcha" at location Z. I care about threat X on servers A, B, and C. Final hypothesis: If key "gotcha" is at Z on servers A, B, or C, I might be suffering from threat X.

Each of your hypotheses should answer a single yes/no question, so that the threat hunt will either confirm them or determine that there is no evidence. For complex threats, you may have multiple sub-hypotheses that you research answers to.

After your team articulates their hypothesis (and maybe sub-hypotheses) for each threat hunt, they can determine which elements of your environment to search.

The last component of defining a threat hunt is laying out its limitations. For this step, it is important to consider certain key questions.

Questions to consider when defining limitations:

- What timeframe will the threat hunt consider?
- What environments should it *not* consider?
- Do you have any relevant legal, regulatory, or contractual constraints?
- Do you have any technical limitations that could constrain the threat hunt?
- What is the deadline by which you need to have the threat hunt completed?

Step 2

Equip Your Threat Hunt

To make threat hunting viable on a scalable, ongoing basis, your team will need to operate with the efficiency that comes with the right technological tools. **Using the most effective digital solutions can accelerate a threat hunt by more than 20 times.**

The time to make sure you have those tools in place is before you start collecting data for a threat hunt. **You'll want to consider three types of tools here: threat intelligence sources, telemetry-based technologies, and automation solutions.**

When it comes to threat intel, there are a wide variety of tools that gather information in different ways and from different sources. Depending on your inventory of information assets and the hypothesis (or hypotheses) driving your threat hunt, you may want to use any or all of the information sources listed below.

Key tools for threat hunts:

- Solutions (including automated feeds, investigative portals, or both) offering you threat intelligence gathered from the deep and dark web
- Open-source threat intel feeds
- Web spiders
- General-purpose search engines
- Information provided by major cybersecurity vendors, such as antivirus service providers
- Government-provided resources
- Insights gathered from publicly available media, such as cybersecurity blogs

Telemetry-based tools can either alert you to potential threats or provide insight into anomalies that you're already aware of. System logs can be a rich source of information on cyberthreats, and SIEM (security information and event management) solutions offer you an automated way to sift through this data in order to draw conclusions.

To make the most of all the information you have access to – and to do so efficiently – it is critical to tap into the power of automation. A SOAR (security orchestration, automation, and response) solution can be a massive force multiplier here, using automated playbooks gathering information from disparate sources and conveniently presenting it to analysts. This accelerates the single most time-consuming step in threat hunting: just gathering the data. If you do not have a SOAR, then APIs and scripting solutions go a long way toward streamlining a threat hunt by automating tasks that would otherwise be time-consuming. Leading artificial intelligence engines can likewise use automation to cut down on the amount of work time needed for a threat hunt by identifying patterns and relationships for the analyst.

Step 3

Finalize Your Threat Hunt Plan

Having defined the threat hunt and which tools to use, you are ready to address the rest of the questions that should be answered before starting the data collection phase. These should fill in the remaining gaps in your plan.

Basic questions for completing a threat hunt plan:

- Who will conduct the threat hunt?
- How will they conduct it?
- When will they conduct it?
- Where will they conduct it?
- What resources will they use to conduct it (including the tools you have selected for the hunt)?

After answering these questions, you will want to clearly define your company or organization's change control process and any legal oversight, and how these factors will affect the threat hunt. You'll also want to lay out a schedule for the hunt.

Then comes the last step before getting into the heart of the threat hunt: the review process. **The idea here is to ensure that your plan is workable, unbiased, appropriate in light of your hypothesis and sub-hypotheses, and cost-effective.** You should involve somebody besides the analyst who made the plan here, minimizing the chances that biases compromise the plan's effectiveness and reliability.

The review process should ensure that:

- ✓ The hypothesis and plan serve your hunting objective.
- ✓ The most appropriate tools and resources have been selected to achieve your objective.
- ✓ Your result will answer the key question of the hunt.
- ✓ Your hunt will not disrupt your organization's other activities.
- ✓ You have all the necessary approvals (including internal change, stakeholder, and legal oversight, as well as approvals from any relevant third parties).

Step 4

Execute the Threat Hunt

With preparations complete, your cyberthreat analyst can start carrying out the threat hunt based on your plan.

How to execute a threat hunt:

A Collect data

How you will collect data should already be laid out in your plans, so now it's just a matter of following through. Data collection is typically the most laborious part of executing a threat hunt, especially if there are hurdles making it difficult to access all of the systems and data that your plan calls for. In this part of the process, it is especially worthwhile to use automation in order to dramatically reduce the amount of work time required.

B Process data

The second-most work-intensive part of the threat hunt (after data collection) is processing the data you've collected. This involves compiling the information so that a threat analyst will be able to examine it. Here is another great opportunity to streamline your threat hunts through automation – especially with scripting, SOAR solutions, or both. Ultimately the success of the threat hunt depends on the quality and comprehensiveness of the data gathered and processed. The more data points you have, and the more extensive the background information at your disposal, the higher the quality of your analysis will be.

C Analyze data

While much of the data collection and processing can be automated, analyzing that information is still a job for a (human) threat analyst today. Expert AI systems can help with pattern associations, particularly on open-source data. SOAR and SIEM systems can be configured to help detect and block IOCs, but require frequent retuning and reconfiguration. A professional's expertise and capabilities can really make a powerful difference here.

Professional recommendation

You want your experts spending their time on hypotheses and analysis – not maintaining and curating dark-web contacts, not negotiating access to logs and configuration data with sysadmins in your environment, and not collating data. Purchase the dark-web portals and feeds, automate the data collection and collating, and let your analyst analyze. This is how you achieve 20 times greater throughput, maximize your analyst's productivity, minimize your spend, and make proactive threat hunting commercially viable for your team.

D Draft a conclusion

The last part of executing a threat hunt is answering the questions at the heart of the threat hunt and writing a report explaining your findings. There are three basic questions your report should address:

- What is the answer to the question defined in your PIRs? (Keep in mind: Although it's a good idea to provide some explanation in the report, it's important to provide a clear "yes" or "no" to the basic question from your PIR.)
- Even if you found no evidence of a cyberattack, did you find that your organization has any vulnerabilities to cyberthreats? (If so, recommend the priority for remediation, and which stakeholders should be engaged for further discussion.)
- Did you run across any other findings of note?

Step 5

Evaluate the Threat Hunt

Evaluate your team's performance and learn actionable lessons. This is the key to continually improving your threat-hunting team, and the time to do it is after you've executed a hunt and answered the key question defined in its PIR.

Questions to consider:

- Was the chosen hypothesis appropriate and sufficiently specific for the threat hunt? (And if not, was the hypothesis too specific or too general, and what made it a poor match for this threat hunt?)
- Was the scope of the threat hunt ideal? (And if not, was the scope too wide or too narrow, and why?)
- Was the threat intelligence you received helpful, and what would have made it even better?
- If you used a threat intelligence provider's portal, was the portal sufficient? What would have made it more helpful?
- What other tools did you use? Were they sufficient? What would have made them more helpful?
- Did everyone follow your threat-hunting and associated change/notice processes? Were there any areas not addressed in your process that you had to work around? Are there any process improvements you can make for better detail, speed, accuracy, or coordination?
- Did staff perform as expected? Were there any issues with following processes? Any missing training? And is there any training that would enhance future performance?
- Did leadership have sufficient information to address leadership questions and report status throughout the effort? Did leadership communications in any way inhibit the hunt?
- Finally, for each of the above, what went WELL? What did you do right? Be sure to recognize those responsible for the successful parts.

Step 6

Share and Act on Your Findings

After receiving any necessary approvals on your conclusions, it is important to share this information within your company, so that improvements can be made for future threat hunts. It is also a good idea to share relevant findings (when possible, and only with the necessary approvals) with the third-party vendors you worked with on this threat hunt, such as threat intelligence vendors, so that they can better help you with future threat hunts.

Finally, you should act on the conclusion of your threat hunt. If you found evidence to support your hypothesis, then it is important to quickly hand your report over to your incident response team and initiate your incident response process.

If you did not find evidence to support your hypothesis, then it's worth remembering that this does not necessarily prove that your hypothesis is false – it simply shows that, based on the data you gathered, you could not confidently confirm that hypothesis. If this is the case, you should report your findings internally and then move on to your next threat hunt.

Your six steps for effective threat hunting:

1 **Define Your Threat Hunt**

2 **Equip Your Threat Hunt**

3 **Finalize Your Threat Hunt Plan**

4 **Execute The Threat Hunt**

5 **Evaluate The Threat Hunt**

6 **Share And Act On Your Findings**

Conclusion

Given the cyberthreat landscape facing today's businesses and organizations, it is not difficult to see how proactive steps such as threat hunting can help them stay safe. By searching for specific evidence of a possible cyberattack rather than waiting for that evidence to become obvious, a cybersecurity team can maximize its chances of identifying the threat relatively early. Then, this team can go to work actively mitigating the risk.

So, is threat hunting a worthwhile endeavor for your business or organization? To answer that question, you'll need to consider the threats you could face, how costly a cyberattack could be for you, and what cybersecurity resources you have available.

Although threat hunting is still no simple feat, it is getting more efficient due to the ever-advancing variety of cyberthreat intelligence and cybersecurity tools on the market. Options including scripting, APIs, SIEM tools, and especially SOAR solutions enable analysts to get more done, faster, through automation. Meanwhile, solutions like Sixgill's Darkfeed and Investigative Portal give companies and organizations easy access to relevant cyberthreat intel from the deep and dark web – allowing for faster, more comprehensive threat hunts, and relieving them from needing the skills, expertise, and time to maintain and curate dark-web sources.

In addition to using these technologies, cybersecurity teams can optimize their threat hunts by ensuring they are done systematically, with proper planning and oversight. By consistently following a sequential approach to threat hunting – with a focus on the six steps laid out in this guide – these teams can streamline their processes, ensure compliance with relevant rules and regulations, and continuously improve their approach to threat hunting.

With this combination of technology and a well-defined process, cyberthreat analysts can boost their productivity – turning a project that could take roughly 20 hours when done manually into a task that can be completed in about one hour.

This way, your company's cyberthreat analysts can adopt threat hunting on a scale large enough to make a serious contribution to your cybersecurity.

sixgill

Know What's Out There

Book a Demo

Follow Sixgill

About Sixgill

Sixgill's fully automated threat intelligence solutions help organizations fight cyber crime, detect phishing, data leaks, fraud and vulnerabilities as well as amplify incident response - in real-time. Sixgill's Investigative Portal empowers security teams with contextual and actionable alerts along with the ability to conduct real-time, covert investigations. Rich intelligence streams such as Darkfeed™ harness Sixgill's unmatched intelligence collection capabilities and deliver real-time intel into organizations' existing security systems to help proactively block threats. Current customers include enterprises, financial services, MSSPs, governments and law enforcement entities. Contact us to learn more about Sixgill's solutions for enterprises, resellers and MSSPs.