Soc strategies and best practices for hunting unknown threats

Law, Security

Security operations centers (SOCs) have evolved a long way from the days of being primarily reactive to threats to proactively hunting them down. It used to be all about taking action once a security team received an alert about a known bad behavior. Today it becomes more and more about trying to figure out what bad behavior looks like. Security analysts might recognize unknown cyber threats when they see them, but they don't always know how to characterize those threats beforehand.

In some ways, hunting unknown cyber threats is similar to a big game hunter stalking some never before seen species of prey. The hunter spots a strange pair of animal tracks and decides to follow them—not because the hunter knows what the animal is, but because the mysterious tracks are interesting and pique curiosity. The tracks might lead down a variety of diverse paths until it ultimately reveals something truly malicious or something completely benign. Similarly, with cyber threat hunting the clues you find along the way can give you an idea of the nature of threat, but you don't get a full picture until you've been able to track most of its movements and get a closer look.

Unfortunately, cyber threat hunters can easily waste a lot of valuable time and resources following false trails or hunting benign prey. Every minute a hunter spends going after false indicators of compromise or harmless event of interests, is time that could be spent hunting actual threats that are already spreading throughout the infrastructure and causing real damage. To help SOCs and cyber threat hunters be more efficient and effective in their hunt efforts, this paper outlines hunt pitfalls to avoid, as well as SOC and hunt best practices to embrace.

Essential SOC-Level Elements of a Hunt Strategy

Probably the most critical aspect of a SOC strategy is to get executive management to buy-in on the importance of cyber threat hunting. While that might seem obvious, it can’t be overlooked. Without that executive buy-in, you’ll be severely limited in your ability to put together an effective hunt team and execute on the other elements of your SOC and hunt strategies. Once you have that buy-in, you can focus on other key elements, including finding the right people for your hunt team, understanding your business and what you’re trying to protect, making sure you have the right data for an effective hunt, developing a hunt playbook, ensuring your hunt team has the necessary access and permissions within your network, and acquiring the right hunt tools.

Find the Right Hunters

The secret sauce to successful cyber threat hunting is hiring good people that can think. Even with all the buzz around machine learning, artificial intelligence is not going to remove the need for humans to make the judgment calls on what hypotheses you base your hunts on, what hunt approaches you engage, what paths you decide are worth pursuing, when do you pivot, when do you fall back to different hypotheses, and if should you keep moving forward with certain hypothesis or approach.

In terms of who to hire for your hunter or hunters, you might want a data scientist, security analyst, digital forensics expert, security engineer, or a combination of these. You might even initially hire someone less experienced or sophisticated as you explore the expansion of your staff or staff capabilities. As part of that effort, you can turn to your hunt tool provider for guidance and education on how to build a capable hunt team. That said, there’s one underlying trait you want in any hunter you hire—an intellectual curiosity to explore data and try to understand what’s happening inside that data.

Know your business

Security has become a critical element to any organization’s business strategy. That’s why both SOC analysts and hunters need to understand their organization’s business mission and objectives. They need to know what is important to the business and what it cares about. Understanding what the business cares about enables SOC analysts and hunters to gain a clear understanding of what they need to protect and why.

For example, while it’s definitely important to protect user account access credentials, what really makes those credentials important is what they grant access to. For salespeople it could be customer leads and lists. For marketing teams it might be go-to-market strategies, product roadmaps, and competitive positioning. For engineering it could be source code, blue prints, design documents, process information, invention details, and other intellectual property. In government agencies it could be any top secret or sensitive classified information, including military operations, weapon systems, defense plans, intelligence activities, technology advancements, economic development plans, and names of certain intelligence operatives.

But it’s not enough to know what needs to be protected. Analysts and hunters need to understand the potential outcomes if those assets are not protected. How will it impact the organization and individual people? Will the organization lose business? Will there be lawsuits? Will people's livelihood be put in jeopardy? Could it even put people's lives in danger? When analysts or hunters understand the implications of the theft or loss of any of these, it not only helps them understand the critical nature of protecting those assets, but it makes it easier to know where to focus their hunt efforts.

Knowing your business also helps you understand what is normal for your business. It helps you create logic and rules around what behavior or activity should be considered allowed or acceptable. You also have to know what normal looks like before you can spot abnormal. The faster you can spot abnormal, the faster you can get on the trail of suspicious threats.

Get the right data

When you know your business and what you need to protect, it also makes it easier to determine what data sets will best help you identify threats against your most critical assets. One of the pitfalls that some SOCs succumb to is the data hoarder mentality. It's the idea of collecting every piece of data simply because there's a chance you might need it someday in the future. The problem with data hoarding is that you end up with significant information overload and it becomes extremely difficult to prioritize that data in a way that allows it to provide immediate value.

Some might rationalize the data hoarder mentality with the idea that data is cheap. But everything has a price tag. Data storage has a cost and so does the manpower it takes to pull the data together and sort through it. When you have an overabundance of data, it's harder to make sense of it and really find what you’re looking for. When you’re hunting, it’s not so much about trying to find a needle in a haystack, but more like trying to find a specific needle in a giant stack of needles. Since all the needles look similar, it becomes extremely hard to determine what is unique about the one you want. You can dramatically simplify that task if you start with a smaller, more focused stack that comprises only the data sets you really need.

With data hoarding you also have the risk associated with any sensitive information you might collect and the added expense of taking steps to making sure it’s stored in a way that prevents breaches into your own storage of that information. It’s much safer and more effective from a hunt and cost perspective to prioritize and decide up front what data sets you really need to collect to enable successful hunt efforts.

The volume of data you have also impacts how much time it takes to sort and hunt through it all. With hunting there’s the concept of failing fast so you can quickly pivot from a fruitless path or an incorrect hypothesis to one that will produce desired results. How much time can you pursue a hypothesis before you decide it’s faulty and you need to pivot? Are you focused on the data sets that really can enable you to prove or disprove your hypothesis? You might end up extending a fruitless hunt much longer than you should have simply because it takes a lot of time to wade through an ocean of data that has little to do with your hypothesis and the assets you need to protect.

In addition to focusing on the right data, you need to make sure you’re getting quality data. Do you have clean data sources? Are the tools you’re using to collect your data delivering the data in a usable format? Is it being parsed correctly? Has it been correlated and aggregated in a way that enhances or impedes your hunt? Do you even have the necessary permissions to access the data needed for a successful hunt? Any questions on the quality of your data and what data you should collect need to be resolved before the actual hunt stage begins.

Adopt best practices

SOCs generally do a great a job at threat detection. They have good insights into known threats and have remediation strategies and plans in place to deal with those threats as they’re detected. Mature SOCs also have strategies and plans in place for dealing with unknown threats. It’s not so much a playbook of every single step or action that needs to happen, but rather a playbook or methodology of general best practices for initiating, executing, and ending hunts for suspected unknown threats. It’s similar to how first responders like a police force or fire department have general response procedures and best practices for the various threats they encounter. And when they encounter new threats that they’ve never seen before, they use and adapt those same best practice procedures to deal with those new threats too.

Creation of hunt playbooks and methodologies

The hunt playbook and methodologies you create need to cover a variety of elements. The playbook should answer a variety of questions, including how does your hunter develop a hypothesis for a hunt? Once the hypothesis is formed, what’s next? What approach strategy or strategies will you follow to carry out the hunt? What tools will the hunter use to assist with the hunt? What do you do when the hunt ends?

Develop hunt hypotheses

Hunters work under the assumption that their organization has already been breached. With that assumption, they work on developing hypotheses regarding the nature of that existing breach. Typically, hunters will develop several different hypotheses that they can test at the same time. As one or more theory fails, they can lead to pivots in direction or approach that allow them to successfully prove other hypotheses.

In concert with their understanding of what the business cares most about, hunters might develop their hypotheses based on a wide variety of factors, such as anomalies identified in outlier charts, unusual traffic spotted through DNS analytics visualization, alerts that haven’t received much attention, external threat intelligence, past experiences with bad actors, or simply something that appears interesting or doesn’t seem quite right.

Figure out your approach strategy

Once you have a hypothesis or multiple hypotheses, you need to decide on how you will go about proving or disproving your hypothesis. What will be your approach? Before you decide on your approach strategy, it’s best if you can first answer the following key questions that have become a critical best-practice starting point for many of the most sophisticated hunt analysts and is associated with what is known as the Diamond Model of Intrusion Analysis:

What are you hunting? Even though it sounds simplistic, the answer needs to guide your approach. The hunting process can be expensive in terms of time invested. Whenever you make the decision to see where a hunt hypothesis might lead, you risk wasting valuable time and resources. To minimize that risk you need to be able to narrow down the exact type of activity you will be hunting. Is it exploitation? Lateral movement? Exfiltration of data? Something else? That understanding will help you stay focused, and prove or disprove your hypothesis faster.

Where will I find it? When someone asks for help finding a lost item, the helper often asks the frustrating question “ Where did you have it last?” The response is often, “ If I knew that, I wouldn’t need to look for it.” Likewise, knowing the answer to this question might seem to eliminate the need for the hunt. But this question is more about narrowing the search even further. Where in all your devices on your network or in all your data, are you most likely to find that kind of activity? What data sources can you eliminate? What data sources should you focus on?

How am I going to find it? This question is more about what tools will you need for a successful hunt. Will the advanced analytics platform and dashboard visualization of a hunt tool like ArcSight Investigate be all that you need? Or will you need to write some custom Python code to do custom data manipulation on the backend to perform statistical modeling of that data? Will you need visualization software? What tools will give you the best information on what you’re hunting for and where you’re looking for it?

When are you going to find it? This question is not about predicting the future. Rather it’s about putting time limits on your hunt. Going with the assumption that you’ll look forever until you find it isn’t a good idea. An endless hunt wastes time, money, and resources that could be used for hunting something that actually delivers results. Deciding in advance on a specific amount of time that you feel will be necessary to achieve your goal and hopefully answer your hypothesis, makes it easier to end a fruitless chase, report your findings, and move onto your next hunting activity.