SECURE | ANCHOR

THREAT HUNTING

WHAT IS IT, WHO'S DOING IT, AND HOW TO GET STARTED YOURSELF

INTRODUCTION

Repeat after me...

"We are going to be compromised. We are going to be compromised. We are going to be compromised!"

In the current threat landscape, compromise is a fact of life. And you have to accept not only that you're going to be compromised, but also something that on the surface sounds much more radical... You need to accept that a compromise isn't a bad thing!

This is a key point that needs to be socialized with executives. A breach is going to happen, period. But when it does, it shouldn't be equated with a failure in security. Sometimes a breach can mean your organization failed at security, yes, but not necessarily. (This is why we need key security metrics to show that the proper security was in place.)

Here's the truth. No matter what security measures you implement, *"100% security"* simply doesn't exist.

Why? Because 100% security is 0% functionality.

As soon as functionality is added to an environment, security drops from 100%—which means preventing *"all"* attacks is an impossibility.

But it's also important to remember that the goal of security is not to prevent all attacks. The goal of security is to control the damage.

A key component of controlling the damage? Early detection. And the way to catch an attack early is by being aggressive and going on the hunt.

In other words, as a security professional, you're either hunting or being hunted... and it's up to you to choose which.

Because, as I said above, security isn't just about preventing attacks. It's about timely detection and minimizing the damage when attacks do happen. Which means you need to actively look for ongoing breaches—even ones you don't know about.

That's called threat hunting—and, increasingly, security professionals are coming to see it as a viable weapon in the war in cyberspace.

One of the reasons why organizations suffer so much damage from a breach is that they are compromised for a long time and fail to detect it. And with the probability of a breach at your organization being so very high, threat hunting is about being proactive. Instead of waiting one or two years to detect a breach, it's safer to assume that you've already been compromised—that you're in the middle of a breach right now— and go about aggressively looking for the adversary within your environment.

Threat hunting is based on that premise—the earlier you can detect an adversary the less overall damage and the less impact a breach will have.

So, let's get hunting...

WHAT IS THREAT HUNTING, AND WHY IS IT IMPORTANT?

Threat hunting is the act of aggressively tracking and eliminating cyberadversaries from your network as early as possible. It involves detecting and eliminating attackers proactively, so that you incur less damage and see a quicker return to *"business as usual."*

Implementing a threat hunting program can also provide a more accurate picture of where your organization is exposed to threats, and help you strengthen those weaknesses. If you know how an adversary is breaking into your environment, it can help you improve your defenses and stop an attack from happening again in the future.

In **previous writing** I've done on threat hunting, I identified several activities that are normally part of the process, including:

- Understanding the threat or threats you're facing
- Identifying which data and business processes could be affected
- Quickly detecting and analyzing bad behavior based on indicators of compromise (IoCs)
- Identifying activities related to IoCs and determining which systems are affected
- Taking whatever action is appropriate, such as eliminating threats, repairing systems, and identifying and remediating sources of vulnerability

Speed is of the essence, of course, because your data is at stake—if you can put a stop to an ongoing attack before too much damage has been done, you win.

Continuous hunting vs. discontinuous hunting

Continuous threat hunting aims to identify both known and unknown indicators of compromise—such as anomalous network behavior, changes to the registry, and so on.

Discontinuous or *"on-demand"* hunts have as their goal the identification of a particular type of attack or a compromise within an organization. They're usually carried out either when you suspect you might be currently under attack, or think you could be threatened in the near future.

Continuous hunts are important, but they can't catch all attacks—you may not be automatically searching, for example, for an adversary that is stealthy and utilizing a new method of compromise.

And to carry out a discontinuous or *"on-demand"* hunt, of course, you need to know what you're hunting for. This is the precise opposite of the kinds of broad network sweeps that define a continuous program.

Threat intelligence is critical to a successful hunt. The more you know and understand how an adversary operates, the more effective you will be at catching and detecting them.

You can see, then, that the best threat hunting program involves both continuous and on-demand methods.

WHO'S DOING THREAT HUNTING?

A recent SANS study (that I authored) asking about the state and maturity of threat hunting programs found some surprising answers: nearly 53% of companies surveyed were not following any particular methodology, choosing instead to run an ad hoc program they felt suited their needs.

This kind of approach can expose an organization to wasted resources, minimal value, and no real sense that systems are any more secure.

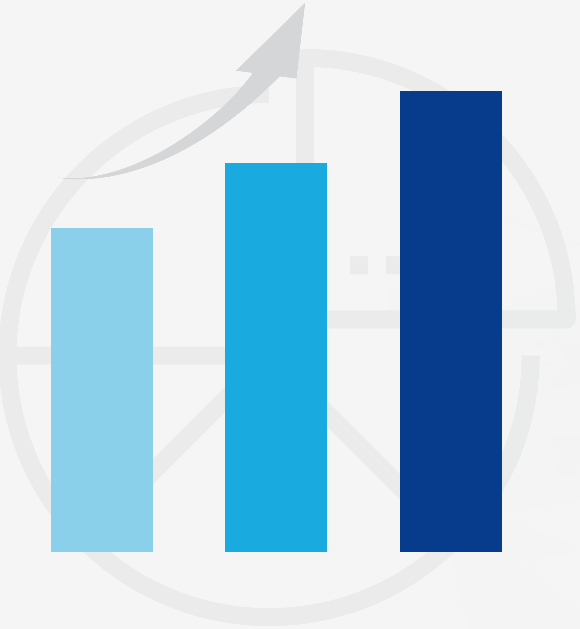
Worse, 14% of respondents weren't doing any threat hunting at all.

As far as what kind of threat hunting was taking place, 38% reported they did it continuously, and another 15% said they had at least a regular schedule. Yet more than a third—34%—said they begin to look for problems only when they have an indication or a *"hunch"* that something isn't right, and a further 12.5% said they only look when they know what they're looking for.

Finally, confidence levels throughout were low, with 88% of respondents saying they needed to improve their tools and capabilities before they felt comfortable with their threat hunting program.

If you feel you're on shaky ground, you're not alone.

Take heart, though—there are benefits to be realized. Results from the same survey show that 52% of those who have threat hunting programs in place have found threats they wouldn't have otherwise detected. 74% were able to decrease their organization's attack surface, and 59% said they were able to respond to threats more quickly and more accurately.



■ 52% of those who have threat hunting programs in place have found threats they wouldn't have otherwise detected

■ 59% said they were able to respond to threats more quickly and more accurately

■ 74% were able to decrease their organization's attack surface

HOW TO IMPLEMENT THREAT HUNTING IN YOUR ORGANIZATION

A robust threat hunting process has five steps. Below you'll find quick tips on how to handle each phase.

1. PLAN

Get ready to hunt

- Identify your most critical systems and assets. These are your biggest targets.
- Further identify which systems, users and devices are connected to those critical ones.
- Make sure that the process of using those systems creates a data trail you can analyze in an attempt to find anything out of the ordinary.
- Then monitor those systems.

Having trouble? Go back to square one and make sure you're getting detailed enough information about networks, systems, users, files, processes, and other activities.

2. DETECT

Look for game

- Search for known threats by examining indicators of compromise, attack signatures, etc.
- Don't forget about unknown threats. Start by confirming which activities are *"baseline"* and then watch for behavior that deviates from what's to be expected.

Remember, attackers often follow specific steps to avoid detection and dig deeper into your system—they'll assess systems, exploit a user or a particular endpoint, conceal themselves, establish back doors, and more.

These are IoCs that you should be able to easily notice.

3. RESPOND

Fire away

- If you notice a *"low-level"* attack in reconnaissance stage, consider what systems are being scoped and why an attacker might be interested. Check your security status—especially your patches—and educate employees about the threat. Keep an eye out for scans of web and mail servers, DNS server tampering, registry lookups or changes, and employee targeting on social media or via email.

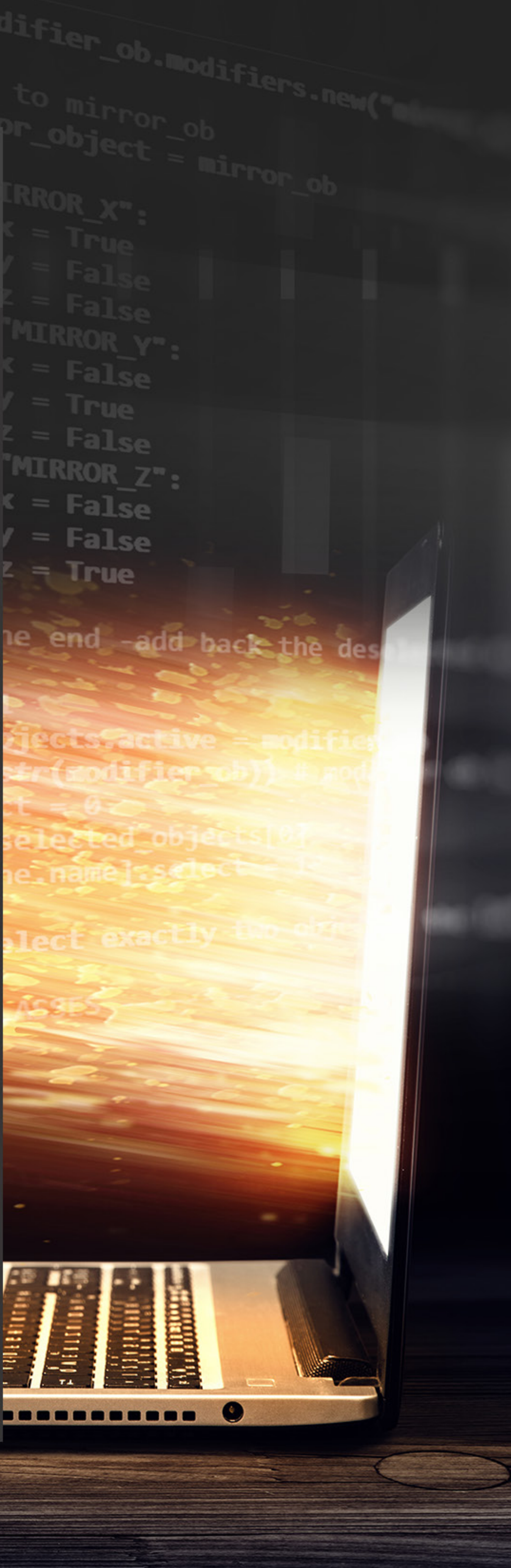
- A full-blown attack—for example, a pivot deep into your network, with an accompanying data compromise and C2 (command & control) channel opened up—requires a more stringent response, obviously. What you do or don't do at this point can have grave consequences, so while you're focusing on expelling the attackers, remember also to:

    - Track pathways and associations between the affected asset and the rest of your network and systems.

    - Determine which data—and how much of it—is under attack.

    - Determine egress points and data loss.

Finally, don't forget—another critical part of this Respond phase is reducing the time needed to fix systems and mitigate future threats.



4. MEASURE

Gauge (and report on) how well you did

- Measure your successes and failures to better inform the other stages of the process. In particular, consider these metrics:
  - Reduction in number of cyberbreaches
  - Reduction of attack surface
  - Improvement in system hardening
  - Reduction in dwell time (the period of time between when an attacker first gains unauthorized access and is finally removed from the network)
  - Increase in speed and accuracy of response
  - Measurable improvement in security of systems

By determining what works and what doesn't, you'll be able to improve your processes for *"next time."* (As a bonus, if you take the time to record metrics that demonstrate business-relevant gains, you'll have an easier job of proving your worth to the organization.)

5. PREVENT

Stay prepared

- Make threat hunting part of an unending cycle in your organization—once you detect that a system has been compromised, for example, get to the bottom of how the breach happened.

  Then use that information to prevent similar attacks in the future. When the next attack happens—and it will be *"when,"* not "if"—repeat the process.

This constant learning and fine-tuning will, over time, improve your defensive position.

And although understanding how to prevent one attack won't necessarily help you stop others, threat hunting will help you identify general weaknesses in your organization's security posture—which, to be frank, is just about the best you can hope for.

SECURE | ANCHOR

MOVING FORWARD WITH THREAT HUNTING

Quick—what was the last company you remember in the news because of a breach? (Hopefully it wasn't yours.)

It's important to remember that organizations are not in the news because they had a breach. Many companies have breaches you never hear about.

The reason why organizations are in the news is because they fail to detect a breach and the amount of damage is significant. If an organization had a breach and 1,000 records were stolen, it wouldn't be news-worthy. Add a few more zeros, though, and when you get to 100 million records, you make the news.

Controlling the damage is key—with threat hunting being a critical part of the equation. This means, of course, that whether a breach impacts your reputation depends directly on how early you catch the attack and how much you can control the damage.

Automation and tools can help here, but so can good old-fashioned expert advice. If you'd like to learn more about threat hunting and how to implement it in your organization, consider Secure Anchor Consulting. A worldwide leader in information security services for public and private enterprises, Secure Anchor Consulting has the experience and expertise to keep your personal and corporate property where it belongs: in your hands and under your control.

info@secureanchor.com	703.675.2055	www.secureanchor.com