TOP 5 THREAT HUNTING MYTHS
The cybersecurity landscape is in a constant state of change and, as many organizations have learned, it’s no longer a matter of if you’ll face a cyberattack, but when. In today’s world, attackers intentionally look normal to evade automated defenses. With the rise of ransomware and fileless attacks, it's harder than ever to protect your endpoints with confidence.

And attacks are a huge drain on company resources.

This means you’re spending almost a full year dealing with a single attack.

To prevent this, threat hunting has emerged as an essential process for organizations to preempt destructive attacks. This process is a proactive approach to cybersecurity that identifies gaps in defenses and stops attacks before they go too deep.

The people defending your organization should be your best chance at staying a step ahead of your adversaries. While it may seem aggressive to work on the “assumption of breach” — that attackers are already inside an organization’s network and are covertly monitoring and moving throughout it — the reality is that attackers may be inside a network for days, weeks and even months on end, preparing and executing attacks, without any automated defense detecting their presence. Threat hunting stops these attacks by seeking out covert indicators of compromise (IOCs) so attacks can be mitigated before the adversary can achieve their objectives.

The bottom line is this:
The adversary is hunting for your security gaps...why aren’t you?

---

1 Ponemon Institute 2018 Cost of Data Breach Study, sponsored by IBM
Unfortunately, there is a lot of confusion around threat hunting that is preventing professionals from being proactive and getting the most out of their investments. At VMware Carbon Black, we want you to be as informed as possible in order to create the best security for your organization. That’s why we’ve developed a guide to dismantle the most common myths about what threat hunting is, how it works and the value it provides.

1. "EDR IS THREAT HUNTING"
2. "THREAT HUNTING IS TOO COMPLICATED"
3. "THREAT HUNTING ISN’T WORTH MY TIME"
4. "THREAT HUNTING IS TOO EXPENSIVE"
5. "THREAT HUNTING IS JUST A FAD"
"EDR IS THREAT HUNTING"

Absolutely not.

Endpoint detection and response (EDR) is a technology piece of your security puzzle. It automates endpoint data collection, and looks for abnormalities or malicious activity, empowering responders to react as quickly as possible. EDR technology enables threat hunting, but the latter is fueled by people, not automated by a platform or solution. While the data collected by an EDR solution is often indispensable to a hunter, the actual process is a continuous, proactive one in which humans search through their environment for gaps and threats. Threat hunting is not simply installing tools and waiting for alerts, it’s humans finding evil with the help of technology and data to be able to analyze activity and artifacts. It’s not man or machine, but man and machine together that create threat hunting.

43% of security professionals say they have threat hunting capabilities today, which indicates that more and more organizations are beginning to realize its value (35% up from 2017). As a security expert, your goal should be to assemble a dynamic team that advanced tools can support but never fully replace. Your hunters can use automation to help increase the effectiveness and scale of the hunt, but threat hunting is meant to go beyond what any machine can do by itself.²

² SANS 2018 Threat Hunting Survey
MYTH

“THREAT HUNTING IS TOO COMPLICATED”

Not necessarily.

Not necessarily. The reality is, people have been hunting for malicious computer activity for as long as computers have existed. If you’re in IT, you troubleshoot all the time. You’re constantly detecting and looking into odd behavior. For example, if you saw CPU usage on an endpoint running at 100%, you’d probably want to investigate. When you threat hunt, you’re simply looking at this from a security perspective. And if you think you or your team lack the skills for this, think again. Believe it or not, the core skills needed to hunt effectively are baseline information security skills like operating systems and networking.³

Whether you know it or not, you’re probably already hunting, just without a formal process or technology to make it easier. The only difference between your current security and “threat hunting” is putting together a program with metrics for measurable success. If you use a security platform that’s built for threat hunting, you benefit from the reduced complexity attributable to automated data collection. This minimizes time-intensive incident response that forces most organizations to be reactive when an incident inevitably occurs.

It’s also important to understand that threat hunting is something that matures over time. You don’t have to start out as an expert. You don’t need to boil the ocean to threat hunt, you just need to measure success and continuously improve.

Remember, your team has the home-field advantage against the attacker. You and your team know your environment best, and you are well-positioned to find gaps. If you’re actively searching for these gaps, odds are you’ll find them long before an adversary does.

³ SANS 2018 Threat Hunting Survey
If you think threat hunting is just about finding malicious activity, think again.

Consider this: When you’re threat hunting, it’s entirely possible that you won’t find evil all the time. But what you will find more often than not are opportunities to improve your security program. Through your investigation, you may find you’re lacking critical data or access you would need in the event of an attack. You might also find gaps in your prevention that need fine-tuning to keep your environment in order.

During your hunt, you can check and tweak your security as needed to provide the best protection possible — before you need it. You don’t want the first time you find these gaps to be during a breach, because you likely won’t be able to close them quickly enough.

According to SANS research, organizations of all threat hunting maturity levels can experience measurable improvement in the security of their organizations through the process. 91% of security professionals cited improvements in the speed and accuracy of response as a result of threat hunting. These companies also saw major reductions in attack surface exposure, dwell time, time to containment and number of actual breaches. Threat hunting also cuts down the time it takes to uncover threats from months to hours, making those who do it much less likely to experience a real breach.⁴

Additionally, if your data lives in silos, it takes effort to piece things together — resulting in a drain in productivity. This is why a solution that combines endpoint security with threat hunting is ideal. If you’re using a single console, single platform and a single dataset, all of your endpoint security activities become easier. Working from a single source of truth cuts down the time and effort it takes to not only hunt for threats, but to also remediate them.

⁴ The Hunter Strikes Back: The SANS 2017 Threat Hunting Survey
MYTH 04

“THREAT HUNTING IS TOO EXPENSIVE”

It doesn't have to be.

If you want to talk about expensive...

The average total cost of a breach is $3.86 million. Breaches that take over 30 days to contain can cost companies an extra 1 million.²

In the event that you do need to respond to an incident, the fact that you've been threat hunting — and therefore have already collected and centralized all the endpoint activity data in your environment — will significantly reduce the time and money you spend responding and remediating. Additionally, many compliance requirements make it necessary to prove continuous monitoring of your environment, and the fines for not doing so can be massive. A continuously monitored environment also provides a clearer picture of the tools in use, so organizations can assess costs and make more informed decisions about the technology. The truth is that the benefits of being proactive far outweigh any costs.

“But what about the additional staff required to hunt?” you may ask. As mentioned earlier, the majority of security professionals already possess the core skills they need to hunt, and are probably already hunting. The most skilled hunters are homegrown, not hired. In fact, knowing the ins and outs of your environment gives you a huge boost over the adversary. It can actually be less beneficial to hire someone new who isn't familiar with your environment or corporate governance policies and expect them to be able to predict an attacker’s next move.

² Ponemon Institute 2018 Cost of Data Breach Study, sponsored by IBM
MYTH

05

“THREAT HUNTING IS JUST A FAD”

Not really.

Hunting for threats/gaps in security technology has always been important, even if it wasn’t labeled “threat hunting.” We’ve always found new ways to outsmart the adversary and keep our systems secure. Threat hunting programs are simply a way to measure how effective you are at doing this. It’s nothing new — proactivity has always been a strong approach.

Traditionally, it was hard to collect the right data, or use the right tools, to investigate before, during and after an attack. But now, with the development of advanced technology — like the cloud — we can. Today, threat hunting has become much easier because of the granularity of visibility that is available. These improvements are like the invention of the light bulb, places that were hidden before become illuminated and can be quickly addressed. As threats evolve, so does the technology that combats them, and so should your security processes. And the industry reflects this. In the next 24 months, 65% of SOCs expect increased investment in tools relating to threat hunting.

65% of SOCs expect increased investment in tools relating to threat hunting in the next 24 months*

---

*SANS 2018 Threat Hunting Survey
THERE ARE PLENTY OF MORE MYTHS OUT THERE ABOUT THREAT HUNTING BUT...

...at the end of the day, security professionals know that waiting until they’re notified about an attack isn’t an option.

They understand that technology is being evaded and they also know that attackers hide in alert noise. Because of this, it’s important for organizations to constantly work toward being more proactive to hunt for threats — before the threats hunt them.

To learn more about how threat hunting can benefit you, visit:

CARBONBLACK.COM/HUNT