Secureworks®

WHITE PAPER

Four Essentials for Finding a Qualified Cyber Threat Hunting Provider

Cyber threat hunting is a proactive service that not only finds indicators of compromise (IoCs), but also provides context and analysis of a breach to help prevent similar intrusions.

There are many scenarios that may compel an organization to use a cyber threat hunting service: to validate current security posture, to react to government agency notice that your network may be compromised, to give peace of mind to leadership after a competitor experiences a high profile breach, to start from a clean slate as a new CISO. Whatever your reasons, cyber threat hunting produces valuable, actionable insight into the presence of threat actors and deficiencies in the security stack. For many organizations, security has become a continuous, multi-layered quest to improve prevention while minimizing the duration and impact of the stealthy attacks that bypass even the strongest defenses.

Not all targeted threat hunting providers are created equal, but there are some proven methods for selecting one that complements your organization. Asking a potential hunting provider the right questions is crucial. The goal of these questions is to clearly understand a potential provider's threat intelligence capabilities and access to specialized technology. The ultimate goal is to find a provider that delivers a high confidence value as to determining if your environment has been breached.

Cyber threat hunting is not simply deploying an endpoint solution and assuming it will solve all your problems. Threat hunting requires security professionals who possess highly specialized background and skills to effectively seek out and identify advanced adversaries by stringing together a series of events, interpreting patterns and building context around an attack. When engaging a cyber threat hunting provider, organizations above all seek to gain a high confidence value on whether or not their organization has been compromised and next steps of remediation.

There are four essentials required for an effective cyber threat hunting engagement. But like any great recipe, the secret is in the unique way they combine and work together. Every cyber threat hunting provider should have four primary capabilities that include:

Deep direct experience with advanced adversaries and varied tactics

Sweeping visibility into threatened environments

Access to ongoing, active research driven by field engagements

The ability to correlate data from many vantage points and cohesively analyze it

Secureworks®

Pitting Experience Against Advanced Threat Actors

When it comes to targeted threats, it may not be enough to follow standard intrusion detection procedures. Motivated adversaries anticipate standard security measures and they train to bypass these measures. This is where security researchers with direct experience combating these threat actors are invaluable. Security, unlike other areas of IT, is uniquely strategic in nature. Like chess, each move is part of a larger orchestrated series designed to develop positions or exploit weaknesses; moves and countermoves are made in anticipation of the opponent's next play.

A security provider should have a team of analysts that observe threat actors' strategies and have been performing intensive inspections in a variety of environments for many years. In addition to familiarity with the security operations of multiple industries and different-sized organizations, you want a cyber threat hunting team that has firsthand experience with a range of adversaries who use a full spectrum of tactics to achieve their goals. The more distinctive attack features and obfuscation techniques a cyber threat hunter has seen, the less likely an advanced threat actor can avoid detection.

Finding a Cyber Threat Hunter with Sweeping Visibility

Cyber threat hunting requires the broadest possible visibility into threat environments, industries, geographies and even security stacks. Ideally, a provider has access to a large, active base of customers from which to draw ongoing attack indicators and intelligence. This works to the fullest when combined with pure threat research and intelligence developed by a dedicated security research team.

With customer threat telemetry and original security intelligence, a threat hunter gains powerful insight into:

behaviors exhibited by threat actors

types of malware targeting various environments

alerts that are being triggered

success rates of various forms of response procedures

Why is this important? Cyber threat hunters with wide visibility can correlate the characteristics of known threat tactics with new activity for better diagnostic precision. For example, when an organized cyber-criminal group tries to make a clean break with one element of its attack toolchain, a knowledgeable cyber threat hunter can look for activity associated with the group based on its remaining operational signatures.

Using Active Threat Research from Field Engagements

Nothing is more effective than letting adversaries inform you. A cyber threat hunting provider uniquely benefits from threat research produced by field engagements. Cyber threat hunting proactively looks for threat indicators and identifies any security gaps accordingly. If an intrusion is confirmed, a targeted threat response provides rapid containment and eviction of sophisticated cyber threats, minimizing the duration and impact of an information security breach.

Ask a potential provider if their experts also perform cyber threat response, and how findings are used to educate and inform future cyber threat hunting engagements. If a researcher encounters new malware or a novel intrusion or evasion technique in a response engagement, how does the researcher consolidate the information, and develop and share the countermeasures with the rest of the research team so that the knowledge is leveraged with other engagements in a way that benefits all customers?

10 Questions to Ask a Hunting Provider

1. What direct experiences do your cyber threat hunting professionals have with observing and combatting advanced threat actors?
2. How many cyber threat hunting and advanced response engagements do you perform annually?
3. What experience do you have with different attack techniques?
4. What resources do you have to provide wide visibility across the threat landscape?
5. How are findings used to educate and inform future cyber threat hunting engagements?
6. What advanced tools or capabilities do you use to hunt?
7. How do you collect, correlate and analyze data from network security sensors, log data and endpoints?
8. How does hunting activity correlate to advanced response should something be found?
9. How do you understand and prevent reentry?
10. How do you monitor the underground hacker market for new tools, tactics and targets for threat actors?

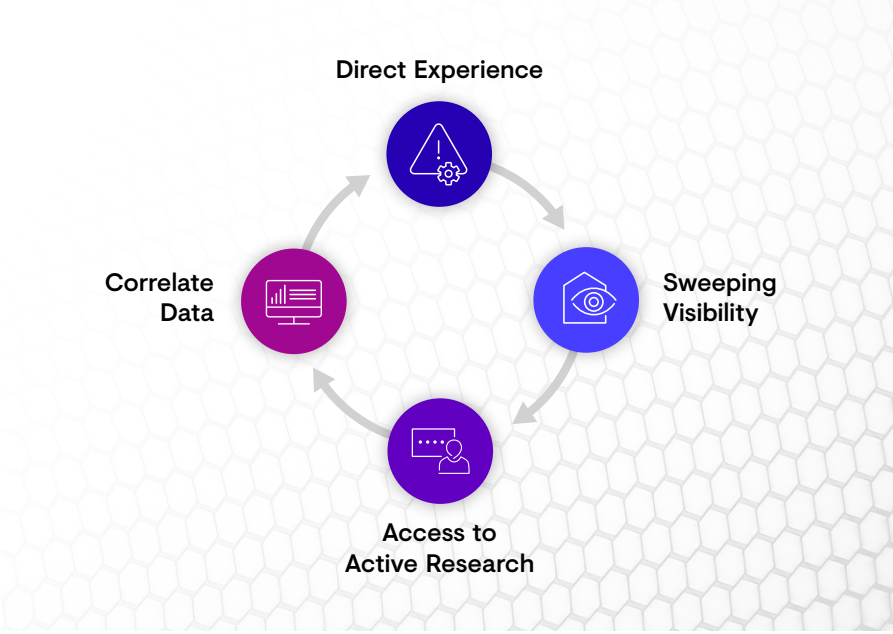
Combining and Analyzing Data from Multiple Vantage Points on the Network

Many targeted threats could be prevented if organizations knew what indicators to look for. The ability to combine threat data from multiple sources and analyze it intelligently provides the most complete coverage of advanced, targeted threats. Find out if a cyber threat hunter provider has the ability to collect, correlate and analyze data from network security sensors, log data and endpoints.

This should include a flexible platform to interrogate a system's file and registry settings, process launch patterns, process memory and encoding schemes. A cyber threat hunter should be able to identify things that are not suspicious on their own, but when seen in full context can be indications of compromise.

Putting it All Together — a Recipe for Dynamic Cyber Threat Hunting

Without the help of a trained eye, advanced persistent threats and other malware can hide unnoticed in the file system and several other areas of your network. The best cyber threat hunters have broad visibility into the threat landscape beyond your network boundaries, research from field-driven engagements and powerful correlation to find indications of sophisticated, stealthy compromise. Such a partnership will increase your confidence in system integrity and data confidentiality, and lends guidance on information security architecture, instrumentation and controls to strengthen the environment against further intrusions. Most importantly, targeted cyber threat hunting will reduce the duration and impact of a breach — preventing damage, ensuring the adversary is unable to reenter the environment in the future and allowing you to focus on your core business.



Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of customers, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our customers a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp