sqrrl

CYBER THREAT HUNTING: WHAT SECURITY EXECUTIVES NEED TO KNOW

Using proactive techniques to detect security threats

THE BIG LESSON LEARNED

Each week seems to bring the disclosure of a massive new data breach—from the theft of personal information for 21.5 million former and current government employees in the U.S. Office of Personnel Management breach to the exposure of information on over 10 million individuals at Excellus BlueCross BlueShield. It's time to admit that many enterprises and government organizations are losing the security battle, especially against targeted cyber-attacks.

The biggest lesson to be learned from these breaches is that today's advanced threats require a far more proactive strategy than ever before. Security teams cannot operate solely in firefighting mode, responding to alerts of potential threats. Today's cybercriminal can evade traditional defenses, compromising an infrastructure within minutes or hours. By the time your company uncovers the intruder—often weeks or months later—confidential data or intellectual property has likely already been compromised or even exfiltrated.

To detect more threats, more quickly, your security team needs to proactively and regularly hunt for cyber threats. More importantly, hunting should not be an *ad hoc* activity. Rather, it should be a critical component of the strategy for protecting your company's digital assets and confidential information.

If you're a CISO, information security manager, or member of the enterprise security team, read on to understand why cyber threat hunting is imperative today, how it works, and how you can make hunting as effective as possible to stop advanced threats and prevent serious damage to your company.

THE LONG BREACH:

The number of months from initial breach to discovery

18 MONTHS	C&K Systems
20 MONTHS	Excellus BlueCross BlueShield
12 MONTHS	Trump Hotel Collection
11 MONTHS	U.S. Office of Personnel Management
6 MONTHS	Home Depot
9 MONTHS	Anthem Inc.

WHAT IS
CYBER THREAT HUNTING?

When even large companies with well-funded security teams experience massive data breaches, it signals that a major shift is needed in the approach to defending against advanced threats. That's why smart organizations are engaging in cyber threat hunting.

Let's start by defining what cyber threat hunting is:

Cyber threat hunting is the practice of searching proactively and iteratively through a network or data set to detect and isolate advanced threats that evade automated solutions.

Unlike waiting for an alert from a traditional security solution, such as intrusion detection systems (IDSs) and security information and event management (SIEMs), to surface a potential threat, hunting for cyber threats lets your security team be proactive to identify threats sooner.

Most organizations already hunt in more of an ad hoc way through log analysis while others may be more committed to hunting, but lack sophisticated tools to collate and analyze large amounts of data to identify the digital footprints of an attacker. Regardless of your team's level of maturity when it comes to hunting, now is the time to formalize a plan of action for conducting successful hunting trips.

8 REASONS

YOUR TEAM SHOULD MAKE HUNTING A TOP PRIORITY

1 Targeted Attacks Are Effective

2 Attackers Have Become Extremely Fast

3 Network Complexity Is Growing

4 Information Assets Are More Valuable Than Ever

5 Losses From Cyber Attacks Can Be Devastating

6 The C-Suite Is Paying Attention

7 You Don’t Need To Start Over With New Security Systems

8 Your Team Is Probably Already Doing It

1. Targeted Attacks Are Effective

Bad actors continue to breach company infrastructure with highly-targeted attacks, using spearphishing to gain a foothold within a network. Verizon found that 23 percent of recipients open phishing messages and 11 percent click on attachments.[1] Symantec reported that bad actors are increasingly using stolen credentials to access corporate networks and then leveraging tools, such as those for network administration, that generate legitimate network activity instead of using malware so as to avoid detection.[2] Targeted attacks often evade traditional, automated defenses making them difficult to detect and defend against.

2. Attackers Have Become Extremely Fast

Today attackers can gain a foothold in a matter of hours. Verizon's 2015 Data Breach Investigation Report cites that in 60 percent of the cases, attackers are able to compromise an organization within minutes. What's the percentage of organizations that detected the threats in days or less? Sadly, it's less than 25 percent.[3] To uncover threats faster, you need a proactive hunting approach to detect stealthy attackers who have evaded your automated defense systems.

3. Network Complexity Is Growing

Cloud computing, mobility, and bring-your-own-device trends make it difficult to have the visibility you need to keep your network secure. Research from the Enterprise Strategy Group shows that 79 percent of enterprise security professionals believe that network security has become more difficult and a virtually equal percentage (80 percent) believe that endpoint security management and operations are more difficult as well.[4] Firewalls, IPSs, email security gateways, data loss prevention systems, and other countermeasures were designed for networks that were physically bound to specific locations. As networks have become more complex, it's become more difficult to make sense of all the data being collected and spot anomalous activity using automated defense systems.

4. Information Assets Are More Valuable Than Ever

Companies today are built on data. Intangible asset value at S&P 500 companies grew to an average of 84 percent by January 2015, compared to 32 percent in 1985.[5] Corporate holdings of data and other intangible assets, such as patents, trademarks and copyrights, could be worth more than $8 trillion.[6] In a CapGemini survey, 61 percent of respondents acknowledge that big data is now a driver of revenues in its own right and is becoming as valuable to their businesses as their existing products and services.[7] Hunting helps you protect those assets more effectively.

5. Losses From Cyber Attacks Can Be Devastating

The Verizon 2015 Data Breach Investigations Report estimated the average loss for a breach of 1,000 records to be between $52,000 and $87,000. A breach affecting 10 million records has a forecasted average loss between $2.1 million and $5.2 million.[8] While enterprises are loathe to publicly divulge the true impact of substantial breaches, there's no doubt that both hard and soft costs, including brand damage, mitigation costs, litigation costs, loss of shareholder value, and potential noncompliance penalties, can be enormous. Hunting helps you detect and mitigate threats to protect your business from breaches and the ensuing losses.

6. The C-Suite Is Paying Attention

In the wake of the multitude of highly publicized breaches over the past several years, IT security has suddenly become a business issue at even the C-suite and board levels. In a PwC survey, nearly 87 percent of U.S. CEOs say they are extremely concerned or somewhat concerned about cyber threats and a lack of data security.[9] CISOs are under increasing pressure to show that their organizations are more effectively protecting the company's digital assets. Hunting gives you a proactive way to scale up security efforts.

7. You Don't Need To Start Over With New Security Systems

In a Ponemon survey, 46 percent of respondents say the IT security budget increased significantly (15 percent of respondents) or increased (31 percent of respondents) in the past two years.[10] If your enterprise is like most, you have a significant investment in security solutions. The good news is that cyber threat hunting actually complements your existing investments in security software and skillsets, while letting you also maximize the value of those systems by feeding the intelligence you derive from hunting back into them to create a persistent defense.

8. Your Team Is Probably Already Doing It

Your security team may not call it hunting yet, but chances are good that they are searching for threats already. For instance, your team may be analyzing log files, using stacking to investigate data sets, or matching threat intelligence feeds with data. While their activities may not be formalized and might not use all the right data or tools, they are already moving in the right direction.

WHY YOU NEED HUNTING

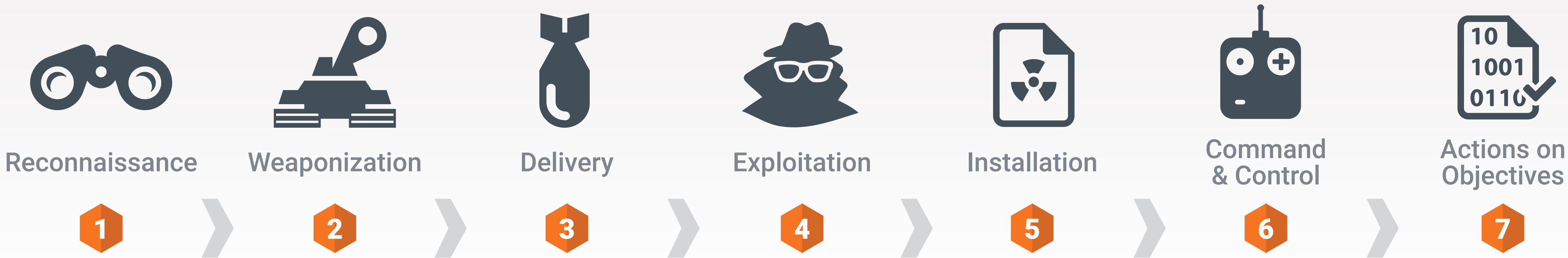
TO COMPLEMENT YOUR TRADITIONAL DEFENSES

The 2014 Verizon Data Breach Investigation Report showed that less than 1 percent of successful advanced threat attacks are spotted by SIEM systems.[11] That's a clear sign that traditional defenses are simply no match for today's adversaries.

Today's adversaries use advanced techniques to pass through perimeter defenses, ignoring detection technologies. Once in your environment, the attacker can persist for long periods of time by moving laterally across the network and compromising as many systems as possible. Using seemingly legitimate actions, the attacker can then exfiltrate sensitive data or intellectual property at will.

Unlike most traditional solutions which focus on one or two steps in the attack chain, hunting can counter an adversary at almost any stage of an attack. The datasets used to hunt might include operating system events, netflow data, application logs, and other relevant data collected by your security systems. By analyzing the data and following the digital footprints of the attacker, hunters can focus on disrupting the adversary's attack before he or she can achieve their goal.

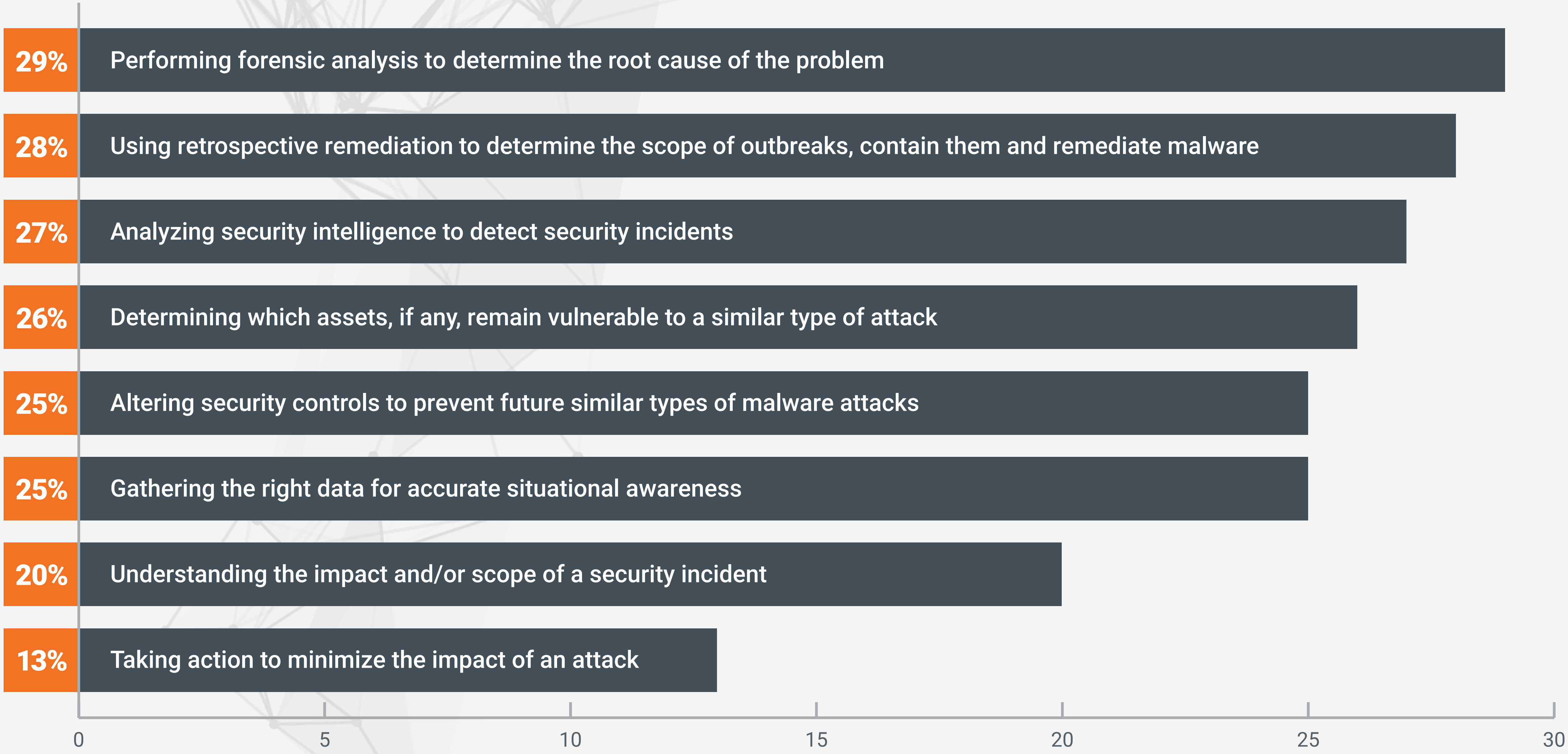
CYBER THREAT KILL CHAIN



WHERE COMPANIES ARE WEAKEST

IN INCIDENT DETECTION/RESPONSE

(AND WHERE HUNTING CAN HELP)



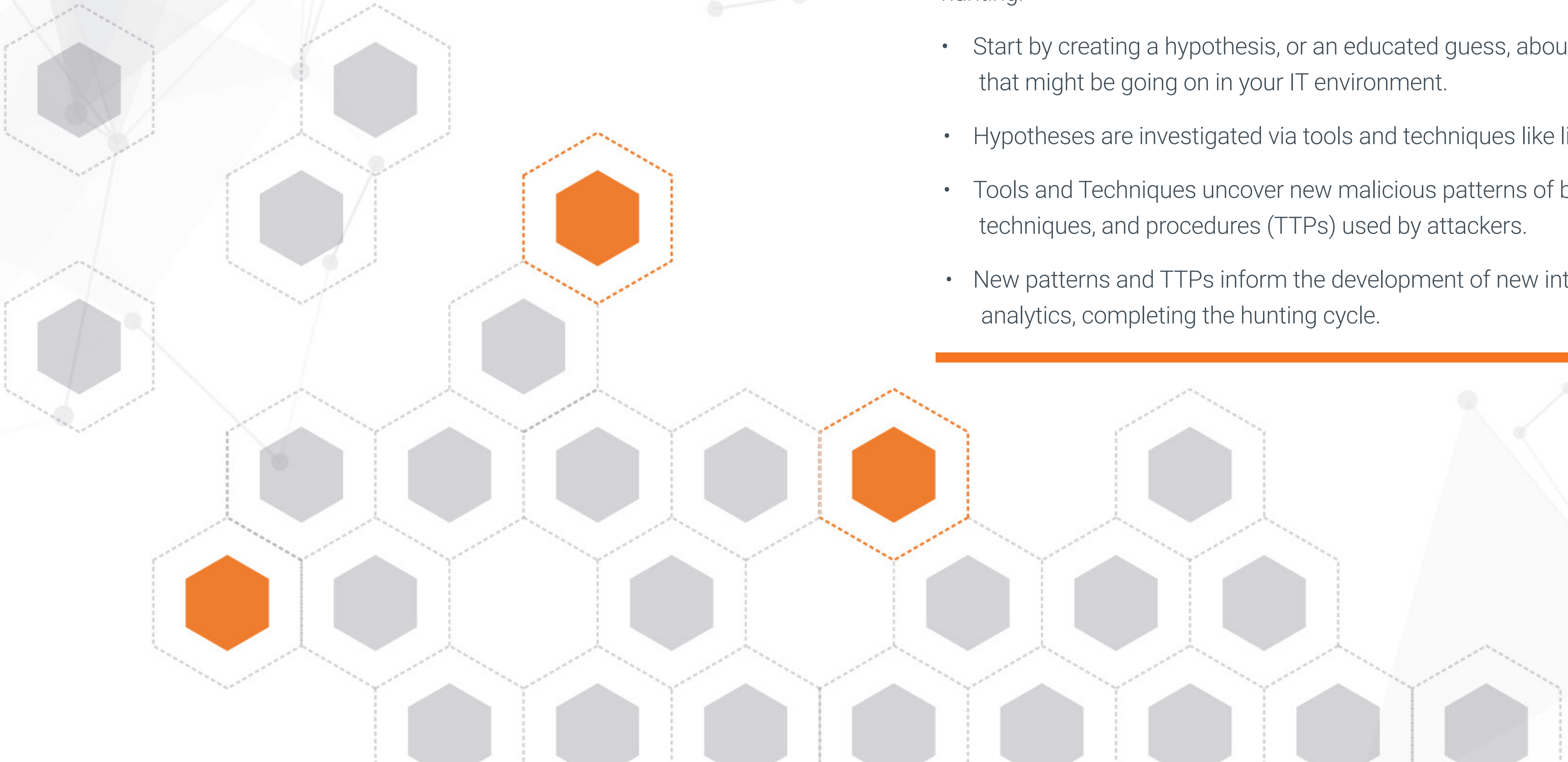
Source: Enterprise Strategy Group, May 2015.

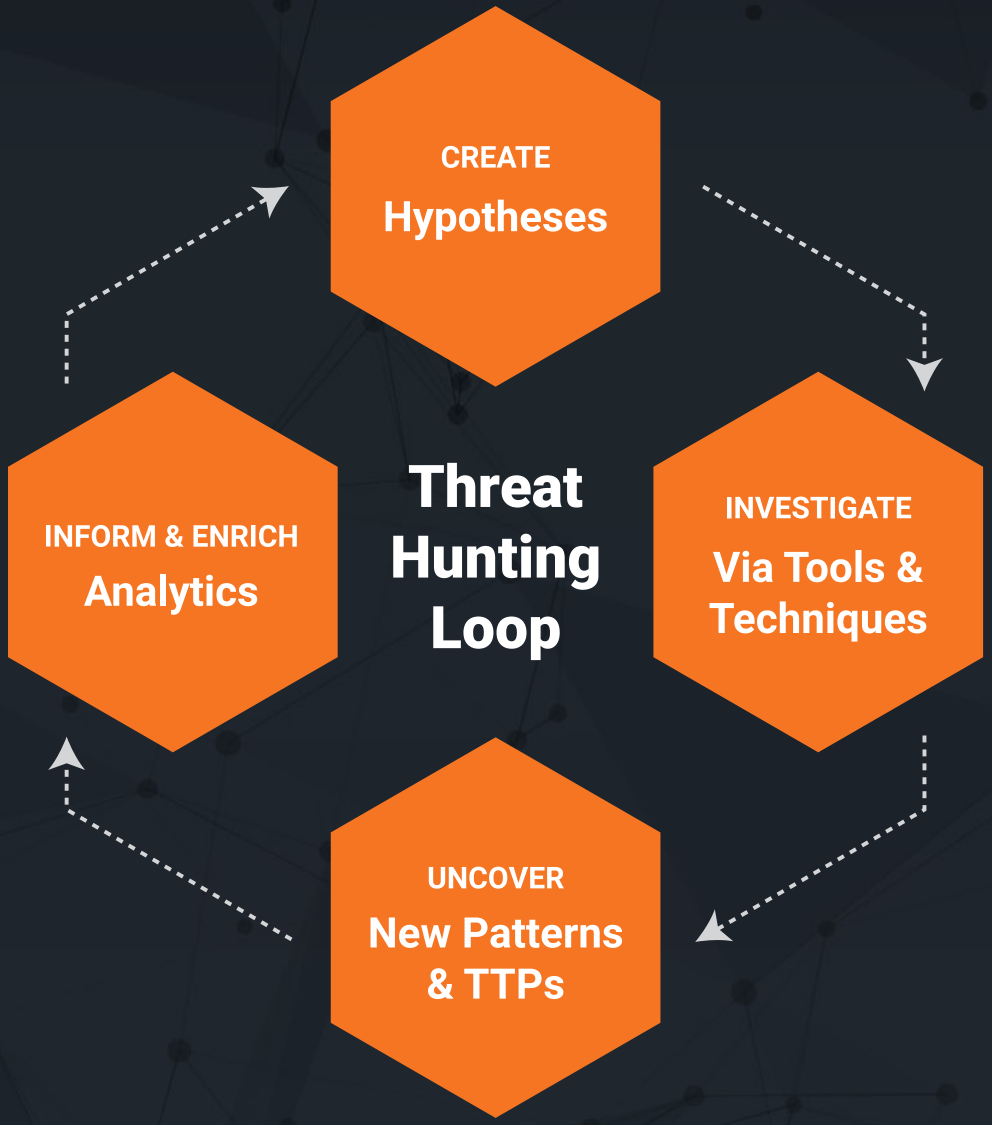
THE FORMAL HUNTING PROCESS

Cyber threat hunting is a relatively new security approach for many organizations. Until recently, most security teams relied on traditional, reactive responses to alerts and notifications, typically only analyzing data sets after a breach had been discovered as a part of forensic investigations and mitigation efforts.

Hunting is a proactive and iterative approach to security. To avoid one-off, potentially ineffective "hunting trips," it's important for your team to implement a formal cyber hunting process. The following four stages make up a model process for successful hunting.

- Start by creating a hypothesis, or an educated guess, about some type of activity that might be going on in your IT environment.
- Hypotheses are investigated via tools and techniques like linked data search.
- Tools and Techniques uncover new malicious patterns of behavior and tactics, techniques, and procedures (TTPs) used by attackers.
- New patterns and TTPs inform the development of new intelligence and analytics, completing the hunting cycle.





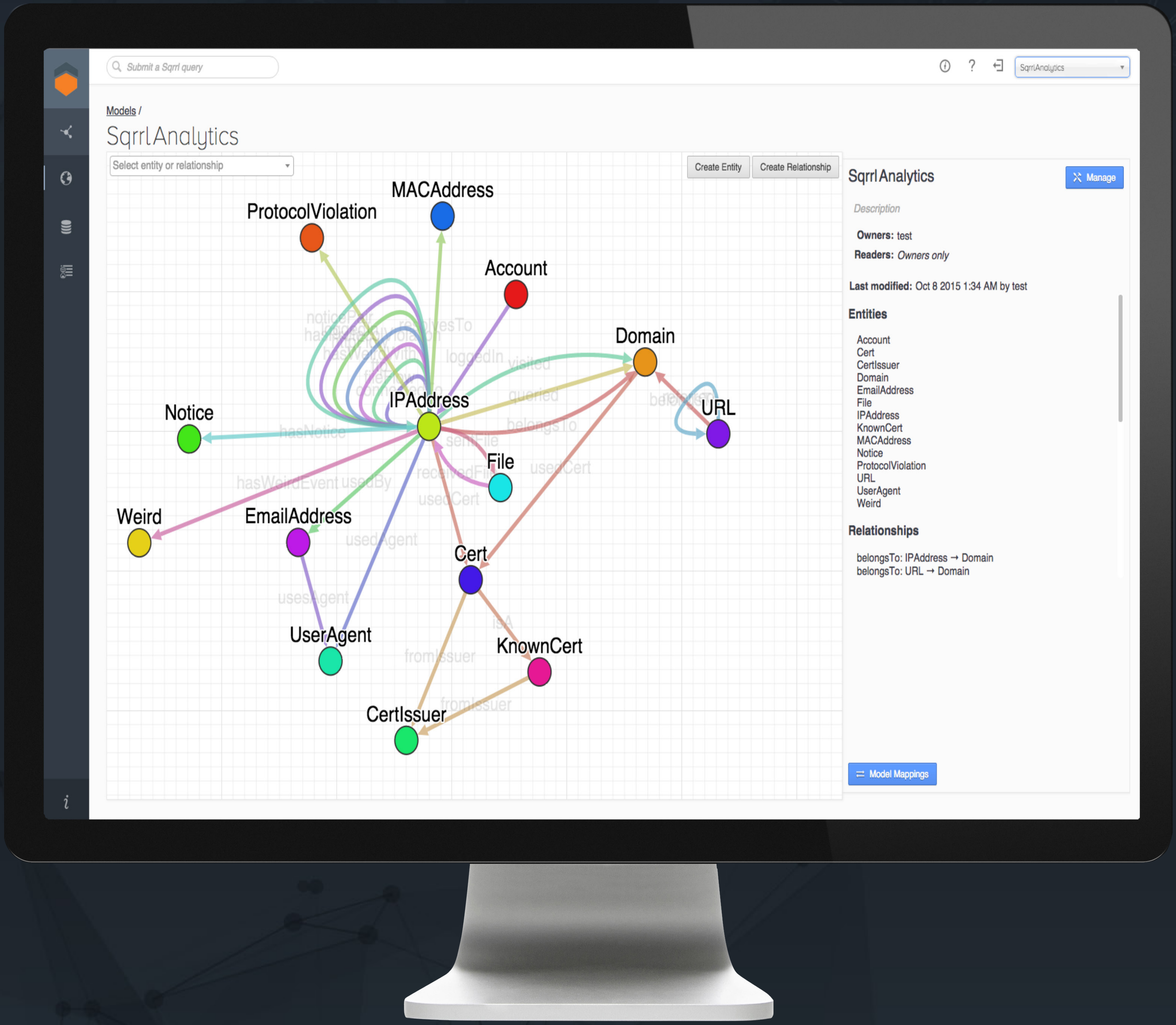
FOUR STAGES
OF CYBER THREAT HUNTING

1 **A hunt starts with creating a hypothesis, or an educated guess, about some type of activity that might be going on in your IT environment.** An example of a hypothesis could be that users who have recently traveled abroad are at elevated risk of being targeted by state-sponsored threat actors, so you might begin your hunt by investigating their accounts or machines. Hypotheses are typically formulated by analysts based on any number of factors, including friendly and threat intelligence.

2 **Hypotheses are investigated via various tools and techniques, including Linked Data Search and visualization.** Effective tools will leverage both raw and linked data analysis techniques such as visualization, statistical analysis or machine learning to fuse disparate cybersecurity datasets. Linked Data Analysis is particularly effective at laying out the data necessary to address the hypotheses in an understandable way, and so is a critical component for a hunting platform. There are many techniques you might use to find bad guys, and no single one is always "right"; the best one often depends on what you are trying to find.

3 **Tools and techniques uncover new malicious patterns of behavior and adversary TTPs.** This is a critical part of the hunting cycle. An example of this process could be that a previous investigation revealed a user account behaving anomalously, sending an unusually high amount of outbound traffic. After conducting a Linked Data investigation, it is discovered that the user's account was initially compromised via an exploit targeting a third party service provider of the organization. New hypotheses and analytics are developed to specifically discover other user accounts affiliated with similar third party service providers.

4 **Lastly, successful hunts form the basis for informing and enriching automated analytics.** Don't waste your team's time doing the same hunts over and over. Once you find a technique that works to bring threats to light, automate it so that your team can continue to focus on the next new hunt. Information from hunts can be used to improve existing detection mechanisms. You might uncover info that leads to new threat intel or even create some friendly intelligence. The more you know about your own network, the better you can defend it, so it makes sense to try to record and leverage new findings as you encounter them on your hunts.



SqrrlAnalytics

Description

Owners: test

Readers: *Owners only*

Last modified: Oct 8 2015 1:34 AM by test

Entities

Account
Cert
CertIssuer
Domain
EmailAddress
File
IPAddress
KnownCert
MACAddress
Notice
ProtocolViolation
URL
UserAgent
Weird

Relationships

belongsTo: IPAddress → Domain
belongsTo: URL → Domain

LINKED DATA:

WHY IT IS ESSENTIAL FOR HUNTING

Linked data was coined by Sir Tim Berners-Lee, director of the World Wide Web Consortium (W3C) and inventor of the web. Linked data seeks to make data more useful, by organizing it in such a way that it allows for semantic queries— queries that are contextual in nature and provide meaning to the things they describe.

Linked data search focuses on fusing disparate cybersecurity datasets into a common ontology so that they can be more easily searched and discovered. Linked data also adds weights and directionality to the relationships between assets, users, and devices, which can be leveraged for more powerful search and analytics to discover malicious patterns during hunting trips.

HOW TO HUNT MORE EFFECTIVELY

While companies can use manual techniques to hunt for cyber threats, automating as much of the hunt as possible dramatically increases scalability and effectiveness of the hunt. Automation also enables less experienced hunters to become hunting experts more quickly.

There are four core capabilities that your team needs for cyber threat hunting success:

- Big data
- Linked data model
- Advanced data analysis and algorithms
- Data visualization

1. Big Data

Because hunting is a data-driven process, it's critical to collect large amounts of data for analysis. You should be collecting logs from each of the three major security data domains (network, endpoint, and application). Authentication logs for operating systems and applications are a good place to start, as are some of the more common types of network transactions, such as HTTP server and proxy logs and netflow records. Emails and employee data, including human resources information and access privileges, can also be useful to detect internal threats and anomalies. To house and use big data efficiently, you should plan to use a big data platform such as Apache Hadoop.

3. Advanced Data Analysis And Algorithms

You need a smart and effective way of making sense of all the data you're collecting. Modern machine learning and statistical tools have the potential to multiply the effectiveness of a hunter's powers by automating common tasks such as producing activity summaries or finding anomalous entities in a dataset. Hunters need tools that implement data science techniques without requiring the users to be data scientists.

2. Linked Data Model

Unless Sherlock Holmes is on your security team, it's nearly impossible for your staff to organize and understand relationships between entities and across datasets in their heads. A linked data model is required to visually connect every entity to other entities that relate to it. Analysis of linked data gives hunters a way to quickly identify important assets, actors, and events relevant to their organizations, accentuating the natural connections between them and providing contextual perspective.

4. Data Visualization

Advanced visualizations provide compact representations of complex, dense datasets and give your hunters a more intuitive understanding of what's going on by the shape, size, color, or other attributes of the data. In particular, graph visualizations condense large amounts of data into simple-to-understand, contextual representations, saving analysts valuable time that they don't have to spend pouring over text and log files.

CYBER THREAT HUNTING: HOW READY ARE YOU?

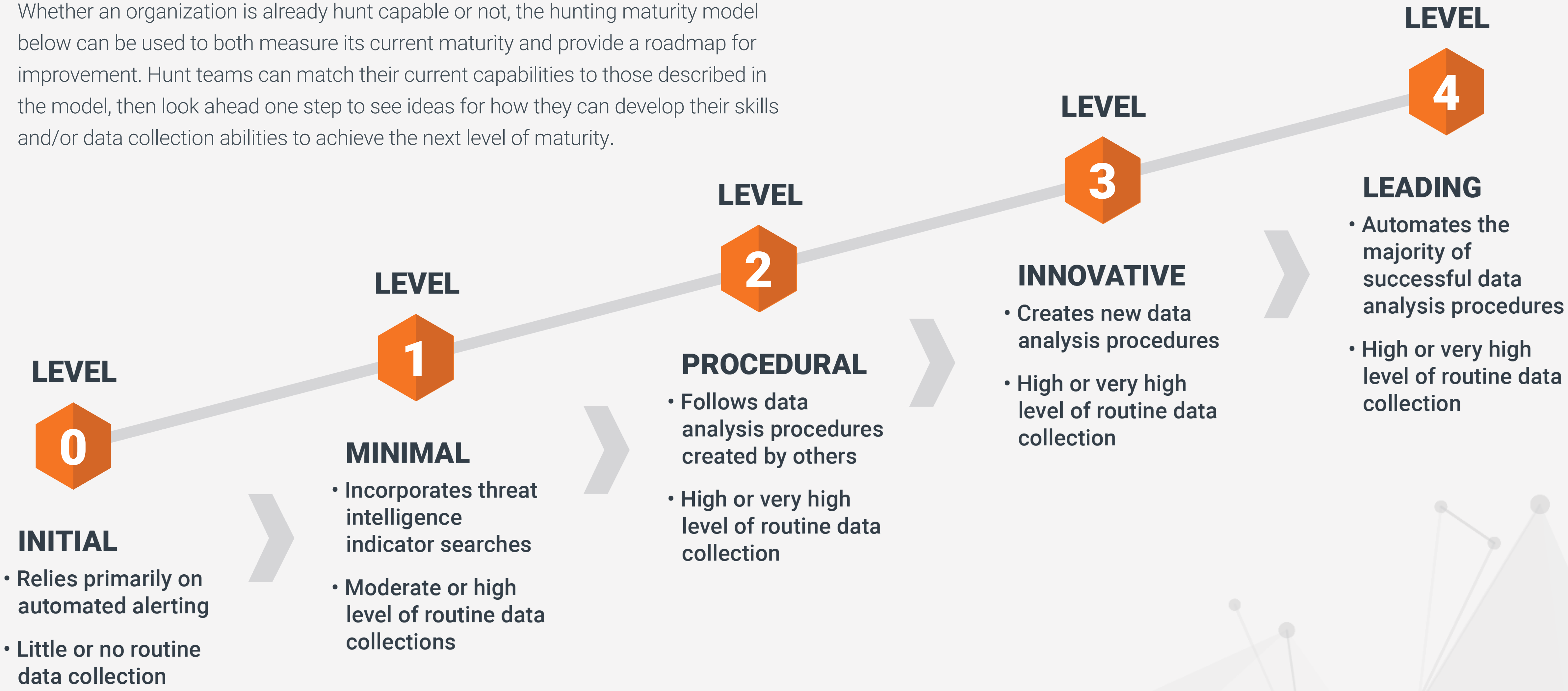
There are three factors to consider when judging your organization’s hunting ability and its maturity when it comes to hunting: the quality of the data collected for hunting, the tools used to access and analyze the data, and the skills of the analysts using the data and tools to find security incidents.

Of these factors, analysts’ skills are the most important because they use them to turn data into detections. The quality of the data that your organization routinely collects from the IT environment is also a strong factor in determining the hunting maturity level of your organization. The more data (and the more different types of data) you provide to expert hunters, the more results they will find. Finally, the toolsets you use will shape the style of your hunt and what kinds of hunting techniques you can use

Executives and managers that hear that their organization needs to “get a hunt team” may be convinced that an active detection strategy is the right move, and yet still be confused about how to describe what a hunt team’s capability should actually be. The hunting maturity model below is a tool to help an organization gauge where it stands on the hunting trail.

HUNTING MATURITY MODEL

Whether an organization is already hunt capable or not, the hunting maturity model below can be used to both measure its current maturity and provide a roadmap for improvement. Hunt teams can match their current capabilities to those described in the model, then look ahead one step to see ideas for how they can develop their skills and/or data collection abilities to achieve the next level of maturity.



LEVEL 0

INITIAL

- Relies primarily on automated alerting
- Little or no routine data collection

LEVEL 1

MINIMAL

- Incorporates threat intelligence indicator searches
- Moderate or high level of routine data collections

LEVEL 2

PROCEDURAL

- Follows data analysis procedures created by others
- High or very high level of routine data collection

LEVEL 3

INNOVATIVE

- Creates new data analysis procedures
- High or very high level of routine data collection

LEVEL 4

LEADING

- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

QUESTIONS TO ASK

YOUR SECURITY TEAM ABOUT HUNTING

Is your organization already conducting cyber threat hunting trips? Is it a regular activity? Now's the time to find out. Here are some questions you should ask your security team to help you understand the current role and maturity of hunting in your organization.

1 Are members of the security team actively hunting today? How many hunters do you have?

2 How often do they hunt?

3 What results have they seen?

4 Are they feeding the results back into the security ecosystem?

5 What challenges are they experiencing?

6 Do they have the data they need?

7 What tools do they need to be more effective?

8 Are they repeating the same hunts over and over, or is there any automation involved?

IF YOUR TEAM IS NOT YET HUNTING:

9 What methodology or techniques does your team use today to identify threats that traditional security tools might miss?

10 What barriers are keeping the security team from proactively hunting on a regular basis?

LEARN MORE

Check out the following resources to learn more about cyber threat hunting:

—Sqrrl's Hunting Site Page

—Webinar on Hunting by David Bianco

—Sqrrl Enterprise Product Paper

—Linked Data White Paper

—Sqrrl Enterprise TestDrive VM

—Cyber Hunting Use Case

SOURCES

[1] *2015 Data Breach Investigations Report,* Verizon, 2015, http://www.verizonenterprise.com/DBIR/2015/.

[2] *Internet Security Threat Report, Volume 20,* Symantec, April 2015, http://www.symantec.com/security_response/publications/threatreport.jsp.

[3] *2015 Data Breach Investigations Report,* Verizon.

[4] *ESG Research Report, "Network Security Trends in the Era of Cloud and Mobile Computing,"* ESG, August 2014.

[5] *Annual Study of Intangible Asset Market Value from Ocean Tomo, LLC,* Ocean Tomo, March 5, 2015, http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/

[6] *Vipal Monga, "The Big Mystery: What's Big Data Really Worth?"* The Wall Street Journal, October 12, 2014, http://www.wsj.com/articles/whats-all-that-data-worth-1413157156

[7] *Big and Fast Data: The Rise of Insight-Driven Business,* Capgemini, March 10, 2015, https://www.capgemini.com/resources/big-fast-data-the-rise-of-insight-driven-business

[8] *2015 Data Breach Investigations Report,* Verizon, 2015, http://www.verizonenterprise.com/DBIR/2015/

[9] *PwC 2015 US CEO Survey,* PwC, 2015, http://www.pwc.com/us/en/ceo-survey.html

[10] *2015 Global Study on IT Security Spending & Investments,* Ponemon Institute, May 2015, http://www.secureworks.com/resources/articles/featured_articles/report-global-it-security-spending-investments

[11] *2014 Data Breach Investigations Report,* Verizon, 2014, http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf

sqrrl

ABOUT SQRRL

Sqrrl is the security intelligence company that enables organizations to target, hunt, and disrupt advanced cyber threats. Sqrrl's Linked Data Analysis approach uses visual, contextual and computational tools to detect and investigate malicious behavior. This enables analysts to reveal patterns and anomalies hidden within massive security datasets. Sqrrl finds threats that traditional detection tools miss, because it focuses on uncovering an adversary's Tactics, Techniques, and Procedures (TTPs) instead of relying only on simple indicators of compromise. Sqrrl's Big Data architecture leverages Hadoop, link analysis, machine learning, data-centric security, and advanced graph visualization technology. Learn more at **www.sqrrl.com.**