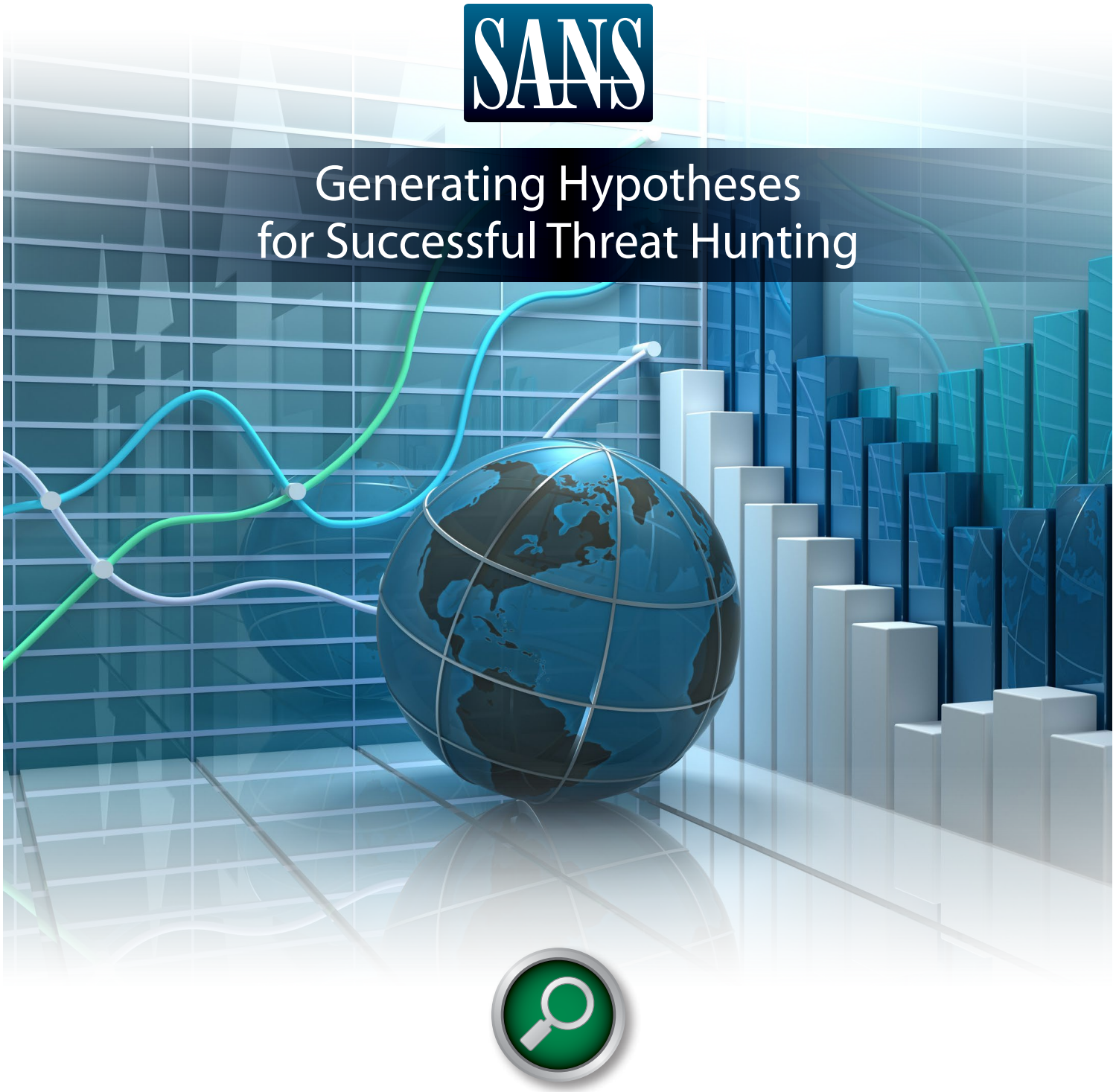
SANS | GIAC CERTIFICATIONS

WHITE PAPER

Generating Hypotheses for Successful Threat Hunting

Robert M. Lee and David Bianco



Generating Hypotheses for Successful Threat Hunting

A SANS Analyst Whitepaper

Written by Robert M. Lee and David Bianco

August 2016

Introduction

OBSERVATIONS

Observations can come from many places. They may have occurred in the past and might be instilled in the analyst as experience and knowledge, or they may be of external stimuli from understanding either the environment or the adversary activity codified as friendly or threat intelligence.

HYPOTHESES

There are two key components to generating hunting hypotheses: They are based on observations, and they must be testable.

Threat hunting is a proactive and iterative approach to detecting threats. On the Sliding Scale of Cyber Security,[1] hunting falls under the active defense category because it is performed primarily by a human analyst. Although threat hunters should rely heavily on automation and machine assistance, the process itself cannot be fully automated nor can any product perform hunting for an analyst. One of the human's key contributions to any hunt is the initial conception of what threat the analyst would like to hunt and how he or she might find that type of malicious activity in the environment. We typically refer to this initial conception as the hunt's *hypothesis*, but it is really just a statement about the hunter's testable ideas of what threats might be in the environment and how to go about finding them.

There are two key components to generating hunting hypotheses. First, an analyst's ability to create hypotheses is derived from observations. An observation could be as simple as noticing a particular event that "just doesn't seem right" or something more complicated, such as a supposition about ongoing threat actor activity in the environment based on a combination of past experience with the actor and external threat intelligence.

The second concept to understand is that hypotheses must be testable. That is, they must be something you have at least a chance of finding in the data to which you have access. Good hunts depend on the hunter's ability to know what data and technologies are required to test the hypotheses. To fully test hypotheses also requires the right analysis tools and techniques that can simultaneously take advantage of information from the environment as well as about likely adversaries. A good threat-hunting platform supports analysts in generating hypotheses and reduces barriers to testing those hypotheses by providing ready access to the data and tools needed to perform the tests.

There are three typical types of hypotheses, although any given hypothesis may combine elements from different types. Hypotheses may be derived from these sources:

- Friendly or threat intelligence
- Situational awareness
- Domain expertise

This guide explores these three types of hypotheses and outlines how and when to formulate them.

[1] "The Sliding Scale of Cyber Security," August 2015, www.sans.org/reading-room/whitepapers/analyst/sliding-scale-cyber-security-36240

Intelligence-Driven Hypotheses

The concept of intelligence-driven defense has entered mainstream cyber security, with awareness of threat intelligence, the use of indicators of compromise (IOCs) and knowledge of adversary tactics, techniques and procedures (TTPs). A hypothesis cannot be created by tools; by its nature, hypothesis generation is a very human process. However, intelligence can serve as a basis for the questions an analyst asks that lead to the formation of hypotheses.

Intelligence-Driven Hypothesis Example

If an adversary has been observed using specific command and control (C2) IP addresses in malware, these indicators may be documented in the form of an IOC. These IOCs should lead an analyst to form a hypothesis pertaining to their use and the locations in which they may be found in the defender's environment.

For example, "I know that LANKY JAGUAR tends to send its phishing messages from infrastructure hosted in Brazil. Therefore, if it is phishing my users, I should be able to examine my incoming email logs to find messages where the geolocation of the sender's IP is in Brazil."

INTELLIGENCE

Intelligence is usable knowledge generated from information. It can be generated about friendly forces (*friendly intelligence*) or about adversaries (*threat intelligence*).

Even if IOC searches do not lead directly to generating a hypothesis, they may still result in the discovery of alerts and log entries that the hunter can then prioritize for investigation. The results of the search may spark a hypothesis as the hunter begins to ask questions about the data and what sort of adversary activity they might represent. In this case, even if the initial IOC did not result in a hypothesis being created, the results of the IOC search did.

There are many ways IOCs can lead an analyst to ask questions pertaining to their use, including:

- The locations in which defenders might be able to find the IOCs in their environment
- The ways an adversary might be obfuscating them
- Overlap between C2 servers and multiple adversary intrusions or campaigns
- How the adversary is acquiring C2 servers and what that says about adversary sophistication

Hunters must note where the IOCs come from, not only in terms of trusted sources, but also in terms of the phase of the kill chain involved.[2] IOCs related to the "Reconnaissance" phase will help analysts form hypotheses that may be entirely different from hypotheses they might generate about IOCs during the "Exploitation" or "Installation" phases.

[2] "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

TAKEAWAY:

Avoid over-reliance on IOCs. If you try to generate a hypothesis that requires analysis of all data in a feed or every IOC in an intelligence report, you can become overloaded with low-quality matches. Instead, use IOCs for quick wins, then work to understand adversary TTPs.

Hunters should be careful about relying too much on IOCs. In the industry today there are many threat data feeds that lack the context to make them true indicators. If an analyst tries to generate a hypothesis that requires every piece of data in a feed or every IOC in an intelligence report to be analyzed, the analyst will be quickly overloaded with low-quality matches. Bad indicators may still lead to data discovery, but the high number of false positives usually waste analyst time. Utilize IOCs for quick wins, but attempt to move up the Pyramid of Pain to understand adversary TTPs.[3]

Good IOCs, however, often lead to the discovery of additional high-quality indicators. The same is true for good hunting and good hunting hypotheses. Don't think of hypothesis generation as a static process. You can use many of the hypotheses created on a hunt later, even if there is not enough time to fully explore them initially.

Good intelligence-driven hypothesis generation takes into consideration assessments of the geopolitical and threat landscapes and seeks to combine low-confidence alerts and indicators with additional information to help determine their usefulness. Threat hunters should use refined and contextualized threat intelligence to stimulate hypotheses that initiate a hunt. Intelligence-driven hypotheses can lead to some of the quickest discoveries in an environment, but analysts still must understand the environment in which they operate.

Returning to Hypotheses for Future Hunts

Hypothesis generation is not a static process. Consider this example. While investigating activity, a threat hunter generates two hypotheses:

1. The adversary maintains persistence in the system through modification of a registry key.
2. The adversary is maintaining persistence through a rootkit in the graphics card's memory.

Outcome: The threat hunter decides that the modification of a registry key is far more likely and that investigating it would require less time and resources; she pursues this hypothesis. It turns out to be correct. Instead of discarding the hypothesis about the graphics card rootkit, she documents it and explores the technology that would be required to test her hypothesis for future hunting trips.

[3] http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Situational Awareness

Situational awareness requires visibility into and understanding of networked environments and their individual elements so that analysts can understand their dynamic nature with respect to time and change. In short, defenders must understand their environment and be able to identify when it changes in some significant way. Having this situational awareness allows analysts to create hypotheses about the type of adversary activity that could occur in their environments.

Situational Awareness in the Physical World

Situational awareness in the physical world is defined as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future."[4] This concept can be found in military warfare discussions both in U.S. Marine Corps doctrine and in the OODA Loop by Col. (USAF) John Boyd.[5] The key points around knowing the environment and identifying changes with respect to time are especially applicable to threat hunting in the digital domain.

Situational awareness allows defenders to focus on the most important assets and information. This focus on the resources vital to an organization's mission is identified as *Crown Jewels Analysis* (CJA).[6] Armed with this type of knowledge, a defender can ask questions that lead to hypotheses about what an adversary might be looking for upon entering the network. This can lead the hunter to think about the most useful types of data to collect in the environment (and the locations from which it should be collected) to be able to begin hunting for types of adversary activity that might be especially important to detect.

Crown Jewels Analysis (CJA) Process

Preparing for CJA requires organizations to do the following:

- Identify the organization's core missions.
- Map the mission to the assets and information upon which it relies.
- Discover and document the resources on the network.
- Construct attack graphs.
  - Determine dependencies on other systems or information.
  - Analyze potential attack paths for the assets and their interconnections.
  - Rate any potential vulnerabilities according to severity.

This type of analysis allows hunters to prioritize their efforts to protect their most tempting targets by generating hypotheses about the threats that could impact the organization the most.

[4] M.R. Endsley, "Design and Evaluation for Situation Awareness Enhancement" in the Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 32, no. 2 (1988): 97-101.

[5] John Boyd, "The Essence of Winning and Losing" (1995)

[6] www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis

TAKEAWAY:

Take advantage of automation, especially dashboarding, reporting and risk scoring to stay abreast of changes in infrastructure, software and vulnerabilities.

A threat hunter that understands the assets and software in the network can exclude hypotheses that center on technologies or data that are not found within the environment. It is important to be open-minded but to avoid spending too much time on hypotheses that cannot lead to successful hunts.

To assist in keeping abreast of the rapidly changing infrastructure, software and vulnerabilities, a threat hunter should take advantage of automation, especially in the areas of dashboarding, reporting and risk scoring. It is a waste of an analyst's time to manually observe and document all the assets and data flows in an environment. Taking such an approach will prevent an analyst from getting the time or mental clarity to focus on generating hypotheses.

Situational awareness should not be confined to purely technical aspects, either. People, processes and business requirements are also critical parts of an organization's threat landscape. Failing to account for these factors often makes defense more difficult. Consider them in conjunction with the technical assets and resources to maximize your defensive home field advantages.

Situational Awareness Hypothesis Example

An analyst decides to look past the tactical level of intelligence by considering strategic challenges in the organization. To do this he first looks at non-technical influences on the organization. The analyst receives information that the company is going to acquire a new company. The new company is located in a different part of the world, and its infrastructure will become connected to the new parent company's networks. The analyst knows that the parent company will also inherit the acquired company's assets, data and vulnerabilities.

The hunter generates the hypothesis that the connection points between these two companies' networks will be abused by threat actors that have, potentially, already compromised the acquired company. In an effort to test this hypothesis, the analyst sets up additional monitoring to treat the data flowing in and out of the new network connections as suspect.

Domain Expertise

In any aspect of analysis there will always be a role for analyst experience. Different analysts bring different experiences, backgrounds and skills to the hunt, all of which influence the hypotheses they generate.

In addition to domain expertise, a hunter's previous hunts and engagements with adversaries influence later hypotheses, even for unrelated threats in new environments. Analysts should seek to not only develop their skills through these encounters, but also document lessons learned and knowledge gained from previous hunts. Further, hunters should share this documentation with their teams and keep it available as training materials and knowledge resources for newer analysts. Such practices allow the team to function and develop together.

Domain Expertise Hypothesis Example

A threat hunter knows how border gateway protocols are intended to work and has previously seen threat actors manipulate these Internet backbone protocols before. This leads the analyst to generate the hypothesis that national-level adversaries may be manipulating Internet routing to steal proprietary information from his organization without having to compromise the organization's network. Testing this hypothesis requires the organization to look outward from its network and to build trust relationships with its Internet service provider and research groups focusing on these threats.

A hunter with good domain expertise has the prerequisite knowledge about both the environment and the threats affecting the organization to ask questions of the data presented to generate hypotheses. In many ways, domain expertise is the combination of situational awareness and intelligence-driven understanding in a historical context. The situational awareness and intelligence previously derived is no longer immediately relevant, but the knowledge of it has shaped who the threat hunter is today. Both types of information help mold the hunter's ability to ask good questions and generate good hypotheses.

CLASSIC INTELLIGENCE ANALYSIS VS. TECHNICAL SKILLS

Just as a government analyst in a Russian linguist position should be able to speak Russian, so should a technical analyst strive to be a master of his or her domain. Knowledge of protocols and network routing, files and host-based information, and security tools and analytics are all important areas of expertise for an analyst to develop.

TAKEAWAY:

Be aware of biases rooted in past experience that may cause you to prejudge a situation. Unchecked, biases can lead to making poor threat-hunting decisions.

Experience often comes with an unwanted side effect: bias.[7] Hunters must be mindful of biases and other bad analytic habits that might influence them to prejudge a situation they may have picked up. For example, if an analyst has only ever worked in a government setting focusing on Chinese-based threats, she may find that her domain expertise has introduced biases that influence her to generate hypotheses primarily relating to the threats she has faced previously. Unchecked, bias can lead to defensive attitudes regarding sharing threat data and poor analytical conclusions, and it may force an analyst to continue working on a threat even when the threat is no longer active in the environment.[8]

Analysts often rely on models and analytical frameworks to help structure data to reveal patterns despite their biases. One such model is the Diamond Model of Intrusion Analysis, which requires hunters to structure the data they find into the categories of adversary, infrastructure, capability and victim.[9] Models are a method of structuring data for analysis and are not representative of a perfect approach to every situation. Threat hunters who take full advantage of their domain expertise also understand its limitations and how to defeat cognitive biases.

Different Environments Call for Different Knowledge

It can be a good thing to investigate the launch of a new command shell or the creation of a new user account. However, in different environments, domain expertise can dictate how quickly the hunter should search for these types of activities and the amount of emphasis they deserve. As an example, in an enterprise IT environment these events may not be abnormal. In most industrial control system (ICS) environments, though, both of those activities would be highly suspect because the environments are typically much more restricted. A typical ICS environment repeats the same set of activities over and over, be it building cars or keeping the power grid running. A typical corporate IT environment is much more flexible and has users taking different actions each day, depending on a combination of individual whim and changing business needs. Hypotheses developed for one type of environment do not always apply equally to others. Domain expertise is not only useful for generating hypotheses, but also for recognizing these potential differences.

[7] For an excellent discussion on analytical biases, see Chris Sanders' 2014 BSides August presentation, "Defeating Cognitive Bias and Developing Analytic Technique," www.youtube.com/watch?v=VHeSsvM1x78

[8] www.activeresponse.org/the-darker-side-of-threat-intelligence-cyber-stockholm-syndrome

[9] www.activeresponse.org/the-diamond-model

The best way to proceed with hypothesis generation is the combination of the three different types of hypotheses. Intelligence combined with situational awareness and the domain expertise of the analyst will yield hypotheses that are more likely to be successful at discovering threats in the environment. This process should be guided by formal models such as the Hunting Maturity Model.[10]

Contrasting the Maturity of Hypotheses

Not all hypotheses are good hypotheses. The following example illustrates the difference in maturity of hypotheses between novice hunters and more experienced hunters who use a combination of intelligence, situational awareness and domain expertise.

A hunter identifies an IOC alert on a new file that has run on the domain controller in one of the organization's business units. The hunter generates the hypothesis that this new file will be found on domain controllers in other business units as well and sets out to test each domain controller independently.

In contrast, a more experienced hunter also knows from Crown Jewels Analysis that the research and development network's data is the most important to the organization. From intelligence reporting the hunter also knows a new threat group has been stealing proprietary research information from similar organizations and the group is known to use malware similar to that found on the domain controller. This hunter, therefore, generates a hypothesis that the IOC is one of multiple files the adversary is using and that sensitive research documents are the adversary's goal and will likely be exfiltrated off of the network via encrypted communications.

Good hypothesis creation requires technology that can support the process of answering questions that the analyst asks. Hypotheses must be testable. If hypotheses are not testable because they are not grounded in reality, then analysts should re-evaluate how they are generating and prioritizing hypotheses. However, if the hypotheses are not testable because of a lack of data or analytic tools, then there is a technology issue that should be remediated as soon as possible. Analysts cannot rely on automation alone, but they should demand automation of any type of hunting platform. In essence, platform support is key to a threat hunter's process.

[10] http://detect-respond.blogspot.com/2015/10/a-simple-hunting-maturity-model.html

Do Your Tools Enable You?

One way to determine whether there is a problem in an organization's security architecture is to check tools against analyst hypotheses. If an analyst can generate a reasonable hypothesis that cannot be answered using the tools in the organization, then there is a technology issue. If the question cannot be answered because of the lack of appropriate data, then there may be a collection issue. Likewise, if the analysts cannot generate hypotheses to test, they may be demonstrating an effect of bias or inexperience.[11] Train your analysts in technical courses, but be sure to include structured analytical training[12] or introduce them to community resources maintained by other hunters, such as The ThreatHunting Project,[13] as a starting point.

Automation empowers hunters to make hunting a repeatable and sustainable process in the organization. Technology also helps lower the barriers keeping organizations from hunting today. There simply are not enough analysts with significant domain expertise to counter all the threats observed today. It is empowering of threat hunters with the appropriate platforms that bolsters intelligence-driven– and situational awareness–based hypotheses. Through this process these threat hunters will also become better analysts, gaining valuable domain expertise over time. Successful hunting trips help build more successful hunters.

Ultimately, hypothesis generation is only the first step to discovering adversaries. Hunters must be careful not to focus so long on hypothesis generation that it limits the time and opportunity to begin investigating. Good hypotheses lead to good hunts, but defenders must not be timid about initiating a hunt and jumping into testing their hypothesess through tools and techniques. Failing is often part of the process, and it encourages better practices. In reality, many hunting trips result in no new activity being detected simply because that activity is not present. Hunting is meant to be an agile process, and even "failed" hunts can result in increased security. Hunters should never be hesitant to try new things just because they think they may not succeed. Threats are evolving in the ways they gain access to environments, but threat hunters who take full advantage of their tools, data sets and analytic skills can out-innovate them.

[11] http://chrissanders.org/2016/05/how-analysts-approach-investigations

[12] Consider the SANS FOR578 "Cyber Threat Intelligence" course to facilitate structured analytical training and help develop better analysts. To learn more, go to www.sans.org/course/cyber-threat-intelligence

[13] www.threathunting.net

About the Authors

Robert M. Lee, a SANS certified instructor and author of the "ICS Active Defense and Incident Response" and "Cyber Threat Intelligence" courses, is the founder and CEO of Dragos, a critical infrastructure cyber security company, where he focuses on control system traffic analysis, incident response and threat intelligence research. He has performed defense, intelligence and attack missions in various government organizations, including the establishment of a first-of-its-kind ICS/SCADA cyber threat intelligence and intrusion analysis mission. Author of *SCADA and Me* and a nonresident National Cyber Security Fellow at New America, focusing on critical infrastructure cyber security policy issues, Robert was named EnergySec's 2015 Energy Sector Security Professional of the Year.

David Bianco is an active member of the threat-hunting community, speaking and writing on such subjects as incident detection and response, threat intelligence, and threat hunting. He is a regular presenter at SANS events, the maintainer of the ThreatHunting Project (www.threathunting.net) and a member of the MLSec Project (www.mlsecproject.org). David currently serves as the lead security technologist at Sqrrl. Prior to joining Sqrrl, he led the hunt team at Mandiant, helping to develop and prototype innovative approaches to detect and respond to network attacks. He also helped to build an intelligence-driven detection and response program for General Electric (GE-CIRT).