HUNTING AND RESPONDING
TO INDUSTRIAL INTRUSIONS

DRAGOS

"Hunting and Responding to Industrial Intrusions", Dragos, Inc., Hanover, MD, 1 March 2018

TABLE OF CONTENTS

DRAGOS

A YEAR IN HUNTING AND RESPONDING

2017

2017 has shown that industrial attacks are being commoditized through new malware with real-world impacts to reliability and safety.

The ICS community needs to mature from a reactive to a proactive position with mature detection capabilites and established hunting programs.

The mission of the Dragos Threat Operations Center (TOC) is to defend industrial envrionments through hunting, developing behavioral analytics and assisting organizations respond to ICS threats. The TOC is made up of industry veterans focused on defending critical infrastructure around the globe.

This Year-in-Review offers a summary of lessons-learned and TOC recommendations from work through 2017.

Ben Miller
Director of Threat Operations Center | Dragos, Inc.

HUNTING AND RESPONDING

TO INDUSTRIAL INTRUSIONS

The industrial control systems' (ICS) threat landscape is largely unknown due to limitations in collection and analysis of ICS-specific adversary activity. However, research throughout 2017 drastically increased the community's understanding that industrial networks are being widely targeted.

Prior to 2017, only a few adversary campaigns had been known to specifically target ICS and there were only three publicly known malware families that had functionality tailored toward ICS: STUXNET, HAVEX, and BLACKENERGY 2. Of those malware families, only one had caused disruption in industrial networks By the close of 2017 the MIMICS[1] research project identified census-like metrics on infections in industrial networks, six adversary campaigns were well documented to target industrial networks, and two new families of malware were identified both causing disruption in ICS networks: CRASHOVERRIDE and TRISIS.[2,3] Hunting for new threats while preparing to respond to them once discovered is vital to industrial network security especially given that lack of historical knowledge on ICS threats.

The Dragos Threat Operations Center (TOC) was built to respond to industrial intrusions, proactively hunt for adversaries in industrial environments, and train a new generation of industrial security professionals to have the capability to do the same. Throughout 2017, the TOC assisted clients to improve their ICS network security through the generation of threat-based scenarios, active threat hunting, and policy and program review with a focus on incident response preparation. The Dragos team understands no single solution solves all problems and works with customers to determine their specific needs, concerns, and requirements. Dragos recognizes contributing what works and what does not work is critical to a strong and robust community. This whitepaper is a synopsis of lessons learned from the field over the course of 2017.

[1] 'MIMICS research as presented by Power Magazine' http://www.powermag.com/malware-in-modern-ics-understanding-impact-while-avoiding-hype/

[2] 'For a deeper understanding of the ICS threat landscape and the aforementioned adversary activity groups and malware read 2017 In Review: Threat Activity Groups paper by the Dragos, Inc. intelligence team' | https://dragos.com/yearinreview/2017

[3] To read the CRASHOVERRIDE paper see: https://www.dragos.com/blog/crashoverride/index.html and to read the TRISIS paper see https://www.dragos.com/blog/trisis/index.html

CURRENT STATE

This year Dragos assisted clients in the following verticals: manufacturing, petrochemical, electric power (including transmission and distribution grids and generation such as hydroelectric, solar, wind farms, nuclear, gas turbine, and coal), and water (including wastewater and distribution). Through engagements in 2017, there was one constant: ICS owners care about network security and are actively working to improve network protections. The predispositions between IT and OT security are shrinking and teams are working in tandem, cooperation, and helping each other. In addition, numerous clients expanded their Security Operation Centers (SOC)[4] to include IT, OT, and physical security. There is also a growing trend for ICS dedicated SOC focuses which the Dragos team supports given the focus of SOCs on specific mission tasking.

Many ICS vendors have shown a strong motivation to improve through partnerships and contributing resources to security enhancements. Dedicated teams have been established to improve existing devices and implement better security in future products. Obscurity is no longer a best practice and Dragos has worked with several manufacturers focused on long-term solutions.

Most importantly, the positive changes Dragos has seen through 2017 have been organic and driven by those that make up the ICS industry. Government regulations serve a purpose but are no longer the primary motivation. Asset owners are actively working towards network security, getting support directly from vendors, and sharing information among sector peers. Dragos assesses this is the greatest avenue to change and is proud to be a part of it.

[4] For Insights into ICS SOCs read our paper:
https://www.dragos.com/media/Dragos-Insights-into-Building-an-ICS-Security-Operations-Center.pdf

MOST COMMONLY OBSERVED INFECTION VECTORS

A popular narrative in the ICS community is that phishing emails and external media are responsible for the significant portion of the infections in industrial networks.[5] However, there is an inherent collection bias with that narrative; i.e. security teams collect in the IT networks and see more phishing emails from their security efforts than communications such as VPNs directly into the operations networks. As the community increases its visibility into industrial networks more defensible metrics and understanding of the infections vectors will come to light.

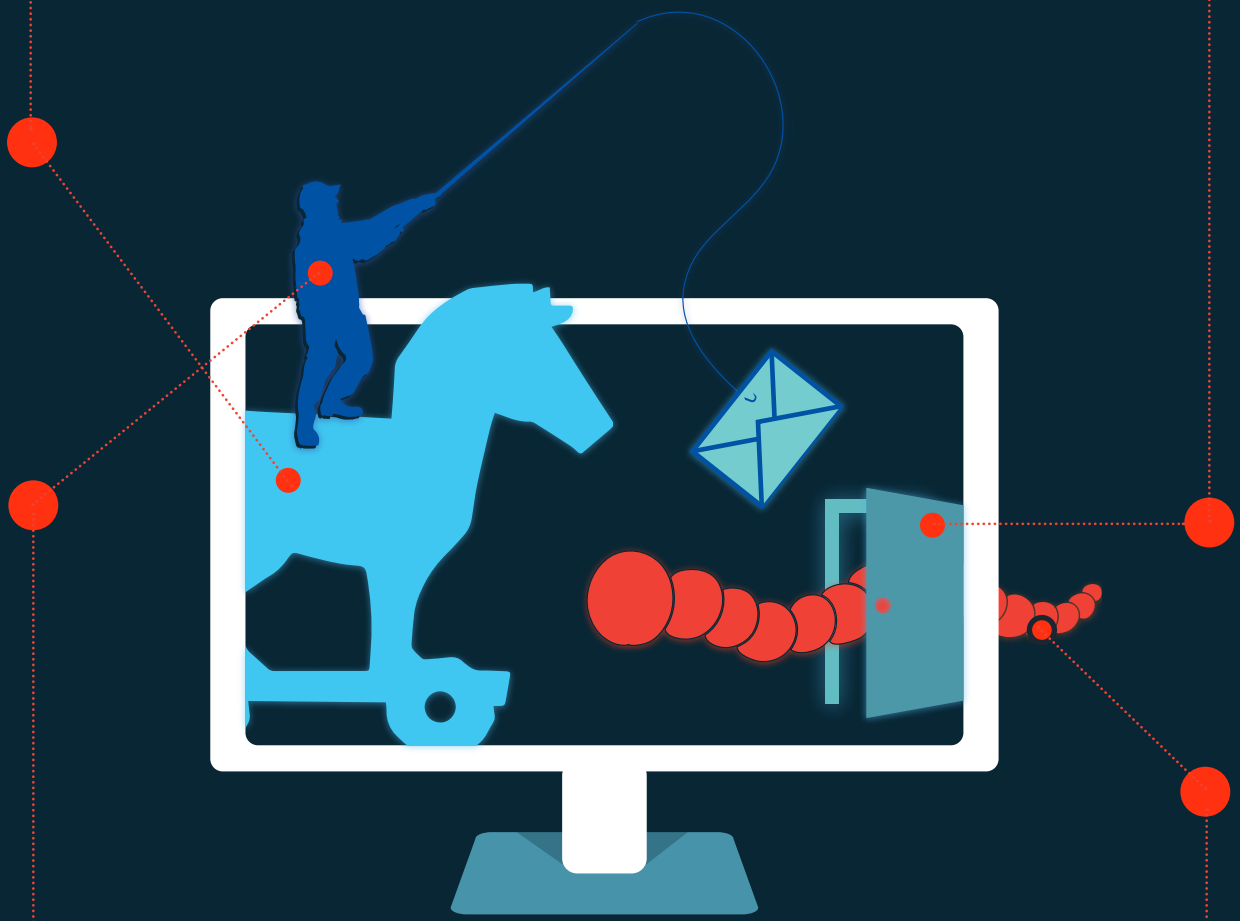
In the Dragos TOC's engagements the most common infection vector was external connections. External connections include external VPN connections to vendors and third-parties as well as partners. The next most common infection vectors are trojanized software such as those exchanged on removable media as well as those downloaded from compromised websites, followed by internal connections that connect facilities together especially those with large footprints such as global operations, and lastly phishing emails. Though these represent the most common they are not the only infection vectors nor does commonality dictate impact. As an example, there were numerous incidents this year at companies where internal connections were not their most common infection vectors but they were the most impactful for those companies with multiple operations impacts recorded.

The recommendation to the ICS security community is to consider the collection bias that can form, assess and address the most common infection vectors including external and internal connections instead of just phishing, and understand the risk of each infection vector posed to the organization instead of fixating only on the most common. It is a best-practice to take a few focused goals for this next year such as additional collection, detection, and response efforts on highlighted infection vectors. Focus on making a few significant changes in the right direction instead of trying to address everything by a small amount.

[5] This narrative originally emerged from good research by the ICS-CERT into their most commonly reported incidents. What was never reinforced publicly though was that the ICS-CERT was not getting those reporting from asset owners but more than 90% of reporting was coming from government audiences who could see the phishing emails being delivered to ICS sites based off their collection.

Interconnectivity with IT systems can provide adversaries access to the ICS environment. Many of these connections are not owned or managed by IT. Instead, third-party partners and vendors deploy and manage their own solutions for connecting to their devices.

Trojanized software, including legitimate installers, travel via removable storage and legitimate network file transfers such as SMB, FTP, HTTP etc. as well as those downloaded from websites.



Facilities can be directly linked to each other allowing for self-propagating malware to quickly spread or an adversary to gain uncontested access across a fleet of facilities.

Phishing continues to be the most common infection vector to an enterprise network. From there, attackers have demonstrated the ability to move into the industrial environment as highlighted by the Ukraine 2015 electric distribution attacks.

POTENTIAL FOR IMPROVEMENT

Although each client is different with unique environments and specific needs, Dragos' TOC has compiled the most common shortfalls and following observations from engagements through 2017. Dragos recommends the ICS community review these notes in relation to their own environment to identify areas of potential improvement.

SUCCESS IS CONTINGENT ON VISIBILITY

Visibility is required to properly scope, prioritize, and validate security controls. Without proper visibility, it is more difficult to identify what needs protecting and what controls would return the best investment. The timeline to triage, scope, and respond to any incident is directly correlated to the visibility available during the time of analysis. Retention of this data may be driven by federal requirements depending on the type of networks monitored. Each organization should also identify its own requirements for network monitoring, data types gathered, and retention.

NOTE FROM THE FIELD

The most common shortfall witnessed through Dragos' hunting engagements is organizations' lack of visibility into the ICS networks. Health monitoring and reporting of ICS devices have always been of concern although segmentation has led the industry to believe consistent monitoring of ICS network traffic for cybersecurity is not a priority. It is common for ICS networks to have connectivity through the IT network as well as direct access through vendor connections to the internet. This connectivity increases the threat surface and justifies mitigation techniques.

Gaining this visibility in an industrial environment can be challenging. Teams often don't know where to start and default to generating an asset inventory. It's absolutely important to know what assets are in your environment (and how they behave), but that's the first step and not the last step. What has proven successful and recommended by Dragos is the generation of a Collection Management Framework (CMF).

The Collection Management Framework is essentially an analysis of what questions need answering and what data sources one has available to answer those questions. These data sources range from internal sources (authentication logs) to vendors (advisories and notifications). The minimum questions the CMF will answer are:

1. What blind spots exist in my environment that limit my situational awareness?
2. Do I have strong coverage to detect and respond to phases of the ICS Kill Cyber Chain?
3. How far back into the past can I investigate?

This challenge of visibility is new in industrial environments. To break down this challenge, consider that there are three primary classifications of visibility; host, network, and industrial.

HOST VISIBILITY

Host data provides a view of system behaviors. When host logging is extensive and widely deployed, analysis efforts are streamlined because a full forensic effort is not required for every device. Remote triage of focused data types reduces several of the resources required during an IR event. The host data available is contingent on the host's platform, operating system, or firmware. Resources required for retention of that data may also be contributing factors.

In many ICS networks, hosts are not able to run a separate software agent or contracts limit what additional software can be deployed. In these instances, routine but manual baselining of host data can be done. Also, network traffic offers a variety of ways to identify host and asset information wherever possible.

For any system running a version of Windows, a minimum of network connections, process hierarchy, and (when possible) process launch arguments should be collected. This can be done by leveraging built-in operating system commands, such as WMI or PowerShell. Once the data is gathered locally, it should be transferred to a centralized collection server for aggregation and processing. There are solutions that leverage both an agent and the local OS, such as NXLog, where commands through the OS are responsible for collecting the data and the agent is responsible for transmission back to the server. The time deviation for gathering logs, user vs kernel credentials, and data types gathered will need to be reviewed and tested prior to any deployment.

PRO TIP

While a host agent is ideal for capturing local events and logs, this isn't always practical for ICS devices. Consider leveraging network traffic for host categorization when a host agent is not available. Comparisons of IPs against asset inventories and OS classification through network traffic can often provide data on host behaviors without requiring a full agent.

NETWORK VISIBILITY

A network collection capability is required for investigation and determines the success of any incident response (IR) effort. Passive collection will avoid potential impacts to critical systems as there is nothing inline to cause service delays or actively modify the packets. There are multiple methodologies available for traffic monitoring; the traffic can be parsed for behavioral analytics and then truncated, portions of the network traffic can be retained while benign traffic is truncated, or full packet capture can be retained. By using a hybrid approach of analysis upon ingest and truncating, an organization can refine the deployment for targeted threats while optimizing efficiency.

Depending on traffic load and retention requirements, all ingress/egress traffic to each subnet should be captured at a minimum. As resources allow, internal traffic should also be captured. Depending on the network design, capturing all internal lateral traffic may not be practical or provide a positive return on investment. In these cases, an organization will need to review each ICS network to determine what lateral data can be captured and whether the analysis of that data will provide increased security.

PRO TIP

Consider parsing all data from egress/ingress points to your ICS network first. While monitoring internal traffic should be an end goal, parsing all traffic traversing the border can provide immediate value. There are open source tools (bro, snort, etc.) that parse this traffic and offer customizations to refine what logs are stored.

INDUSTRIAL VISIBILITY

There is a range of data available to a security organization that is often missed as valuable in hunting and response activities. These can be vital when building a response timeline, understanding impacts to an event, root cause analysis, and developing a solid baseline of typical behaviors of how the industrial process works. Unfortunately, there is no concrete data source but instead is variable on the software and devices. Ultimately, application and device logging activity does exist and can be used to develop a baseline or retroactive level of understanding. In addition, historian data can also serve as an important tool when developing forensics timelines and understanding effects of an attack.

PRO TIP

Knowing the controls and specific vendors with a footprint on your network should be an initial priority. This inventory can be referenced when creating IR procedures and facilitate analysis of host behaviors and network traffic.

PREPARATION IS A MUST

Every security incident, whether it be a physical or cyber event, is often a high-stress situation that requires a calm demeanor and authoritative decision making. IR efforts are dynamic, requiring agility to adapt to the threat. ICS networks, however, are static; change control and thorough testing preclude implementation. On these networks, changes do not need to be substantial to have a snowball effect resulting in physical damage, harm to others, or lasting effects that exacerbate the original issue. The best prevention against making the wrong decision is preparation.

NOTE FROM THE FIELD

Through customer engagements, Dragos has identified most cybersecurity IR procedures to be focused on compliance and largely not tailored to a particular facility. These plans may fulfill regulatory requirements but don't facilitate the organization during an IR effort. An incident cannot be remedied through hap-hazard decisions based on limited information.

Control operators have procedures for responding to foreseeable plant issues. Often crafted from multiple contributors when the environment is calm, these procedures are in place to define workflows and avoid mistakes. The ICS industry has seen evidence that skilled threat actors are now actively targeting their networks and cybersecurity is an active threat. IR plans should be in place to guide a responder during cybersecurity events as well. These plans should account for roles, responsibilities, approvals, and accountabilities (R2A2's) for all interested partings, account for regulatory requirements, define an escalation procedure, and protect responders from making small changes that result in large negative impacts.

IR procedures exist to provide responders with guidance and authorization. If an action is completed by a responder, this should correspond to guidance on the IR plan. The responder should have the authority and feel protected to make these decisions as they are based on the IR procedures and not made at the sole discretion of the analyst. These documented actions need prior testing to ensure they are justified and don't introduce additional risk. Also, many emergency response teams are centralized and far removed from the industrial facilities day-to-day. Some centralized teams will have liaisons at a particular facility to serve as the 'infield response' but often these are in name only and the individuals lack the training and experience during an incident response scenario. Ideally, this staff is instead dedicated to the mission of securing the facility and has the understanding of the particular facility in addition to detection, proactive hunting, and incident response training and experience.

Finally, procedures change over the course of time and need revising. Not only due to internal changes but external. For example, many US-based firms have procedures around notification to the United States Industrial Control System Computer Emergency Response Team (US ICS-CERT). However, in 2017 this team was disbanded and its mission aggregated throughout the US National Communications Cybersecurity Integration Center (NCCIC).

NOTE FROM THE FIELD

Dragos has seen a lack of testing and validation for security controls as well as procedures. Changes in staffing, network topology, and deployed controls mean procedures should be updated as well. Guidance and procedure are only of value if it can be executed as intended.

PERIODIC TESTING

The threat landscape for digital attacks against ICS networks is growing rapidly and attackers are crafting innovative ways to compromise ICS networks. Security controls and practices must mature. Although ICS network operations are essentially static, response to an incident may change based on threat actor Tools, Tactics, and Procedures (TTPs) or IR resources available. Extensive testing should be completed while drafting IR plans to validate the procedures address the threat, don't increase risk, and facilitate the return to operation as quickly as possible. Additionally, periodic testing is required to maintain current procedures and account for any changes in staffing or on the network.

NOTE FROM THE FIELD

Dragos has seen a lack of testing and validation for security controls as well as procedures. Changes in staffing, network topology, and deployed controls mean procedures should be updated as well. Guidance and procedure are only of value if it can be executed as intended.

Tabletop exercises are proven methods for validating procedures. Each exercise should have participation from all associated parties and senior management. Actions defined in the IR procedures should be followed whenever possible to validate the guidance. By working through each step, shortfalls and areas of improvement, such as a lack of resources or training, are more easily identified.

Many firms have a strong drill and exercise culture driven by safety and reliability but not necessarily cybersecurity. Finding and leveraging those internal resources can be extremely valuable. There are also external resources available for drafting, testing, and validating IR procedures. Depending on your organization's sector, the U.S. federal government hosts biannual exercises, such as GridEx, to support industry. There are multiple vendors, including Dragos, that can facilitate these efforts as well.

INGEST INTELLIGENCE FOR THREAT MODELING

Receiving intelligence reports is only of value if that intelligence can be transferred into action. Interpreting threat advisories requires a special skillset. Too often analysts focus on low-level indicators (IPs, domains, file signatures) and do not consider threat behaviors. Dragos has been successful in changing the discussion from a brittle indicator-based approach into creating understanding via threat modeling of activity groups targeting specific sectors or clients. For this service, the TOC reviews known adversaries in relation to clients' mission statements and existing security controls to assign a risk score. This risk score can then be compared with acceptable tolerance levels and leveraged to improve security controls.

NOTE FROM THE FIELD

Too many organizations establish threat intelligence groups that focus entirely on low-level indicators. Intelligence reporting should be translated into direct risk and actionable protections for the receiving party. Threat modeling and attack scenarios can facilitate this effort and help organizations identify gaps in protection and detection capabilities.

Threat modeling is a valuable tool to legitimize and validate an organization's risk to attack scenarios. Threat models created specifically for an organization's assets and controls considered help communicate the current state of risk as well as justify additional resources as needed. Adversary TTPs don't change often so if done correctly, each model's relevancy can extend through a specific campaign.

CONTINUING EDUCATION

There exists a shortage of ICS cybersecurity experts. Fortunately, the community understands this deficiency and is actively working towards more training opportunities. In some cases, Dragos has been contracted to provide shadowing and education through assessments as a means of knowledge transfer. The community is motivated to learn, which is the primary driver to change.

NOTE FROM THE FIELD

It is clear the industry is hungry for more knowledge in ICS protections. A hands-on training seminar is now offered at the Dragos headquarters. This class has been overwhelmingly popular as it provides students with physical gear for testing. The TOC is also frequently contracted to provide on-site training. Efforts from educational institutions and asset owners will help elevate the entire communities' knowledge base.

More training organizations are offering ICS-specific cybersecurity seminars. SANS and government outreach programs have proven successful as the community is thirsty for knowledge. The motivation has been proven and the resources required to reduce the existing knowledge gap are increasing.

CALL TO ARMS

The community mindset of securing ICS has historically focused on protection. Protection is not enough; attackers have demonstrated an ability to navigate beyond any set of particular static defenses into an industrial environment. Once that is obtained the attacker has uncontested access to launch an ICS attack of their choice. Defenders are required to consider security controls can fail and alerts may be overlooked. This dedication to active defense reverses the odds from the attacker to the defender. A strong defense requires an active understanding of both the environment and threat.

Dragos has created a methodology for implementing a hunting program. This effort can comprise dedicated full-time employees or be project-based and routine. Aside from the local resources available to each organization, Dragos' recommends the following methodology be followed to ensure the hunting efforts are targeted and within scope.

INDUSTRIAL HUNTING

Hunting is proactively seeking threats in an environment and recognizing that defenses are fallible—simply waiting for an alert, alarm, or notification is not enough. It is inherently reliant on a human; adding the cognitive layer to the already existing security controls and security automation.

THE VALUE OF HUNTING IS BEYOND FINDING AN ACTIVE THREAT

The value of the hunt is in the journey and communicating what often is seen as the intangibles of the hunt. While the hunt may have zero threat findings it will nearly always discover misconfigurations, unexpected configurations, and gaps in knowledge. Each of these should be fed back into the overall security program to improve the security posture. Secondly, the skillset used and developed in hunting is also used in intrusion analysis and forensics. This strengthens the staff to respond and understand an attack when it does matter. Finally, the goal of a hunt is to automate some or all aspects of the hunt. Over time this automation will grow to strengthen defenses and free up time for staff to focus on other areas.

THE GREATEST RISK TO A HUNT IS INCONCLUSIVE DATA

Generating a hypothesis is a cornerstone of threat hunting. Fundamentally it is a statement that can be tested. Hypotheses apply structure to serve as 'true north' for the analyst to stay focused on the key deliverable. It also serves as a straightforward way to communicate WHAT the hunt is focused on as a good hypothesis is immediately obvious. Hypotheses should generally follow the SMART principles: Specific, Measurable, Actionable, Realistic and Time-bounded. A vague hypothesis such as "An APT is using zero days against my network" is theoretically provable but realistically not. Instead, a hypothesis of "An Adversary has remote access into the energy management system (EMS) network." Without proper structure and planning, the hunt may be a failure because the data simply doesn't exist to adequately hunt. This is also demoralizing and can deter the willingness of the hunter or management to continue.

Hunting is often described as generating an objective hypothesis - "An adversary has access to an HMI and is exfiltrating screenshots." Little else exists to guide an individual or team to have a successful hunt. This lack of information and tools creates an effect where only sophisticated teams of defenders can approach hunting.

SMASH - Systematic Methodology and Attributes for Successful Hunting - is our tool to plan, and communicate that plan, to others. It can help in determining the likelihood of success. SMASH can be a 5-minute exercise by a seasoned hunter who has a high degree of understanding of her environment or it can span across several meetings of multiple stakeholders. The level of structure built by the hunter isn't important; SMASH isn't made to add overhead but instead to prevent assumptions. The most important part of any planning is to have a concrete understanding of if you have the data available to test your hypothesis. If you do not, then you risk having an inconclusive or failed hunt.

ACTIVE DEFENSE REQUIRES ACTIVE ENVIRONMENTAL UNDERSTANDING

You cannot defend an environment you do not understand. Learning the industrial process and facility is important to develop a concept of how the devices hosts and networks are designed, configured, and operating. This environmental understanding gives a grounding to the hunt to have basic assumptions of what should and should not be seen. Based on prior experience, this allows the team to formulate hypothesis and validators that can be used throughout the hunt.

START WITH WHAT YOU HAVE

Hunting can be an abstract term that can be difficult to understand as each hunt can be wildly different. One may consist of an hour of log reviews while another may require several weeks' worth of manual collection of data followed by days or weeks' worth of analysis. This wide range of options produces ambiguity when it should instead generate interest. It gives ultimate flexibility for a low resource or low visibility environment to start with a low level of investment.

Often, particularly in industrial environments, a question of what maturity of technology or staff is needed for hunting is asked. Non-intuitively, a less mature environment has the most to gain from hunting (with the caveat of needing with management support).

This is because hunting is more than simply looking for threats and then stopping. It's also about identifying gaps in visibility, security controls, and team knowledge and, most importantly, refactoring this knowledge back into the environment. Hopefully, not every hunt will find an adversary dwelling in a defender's infrastructure. It will, however, likely find gaps in visibility, controls, and knowledge. When iteratively improving the environment through hunting you are improving your team's capability, fine-tuning the overall security plans and planning and automating improvements to reduce complexity and convert some of the cognitive requirements into automation.

It's compelling to think that cognitive/automation balance is a finite set and we as a community can move to an all-automation or infinitesimal level of cognitive needs. Unfortunately, security is not a static field but a competition to a living and adaptable adversary and we can't automate our jobs away. The challenge of hunting is to speed up how fast we can learn from and defend our environments.

This is where management buy-in is a requirement. Generating an ever-growing backlog of improvements that go unimplemented is demoralizing and takes away from the significant value threat hunting brings: iterative and regulator improvement to security improvements of existing technologies rather than annual capital spending and 5-year plans.

That's not to say a formal hunting program is needed. A one-person team or small team with authority and access to hunt, then, is in a good position to begin. If that first hunt, formal or informal, does not result in some tactical iterative improvement, then that may be the ultimate measure a security program is not yet ready for internally-led hunting. In this case, external service providers may or may not help in demonstrating and kick-starting hunt program values, as it is typical (and unfortunate) for a third-party outcome to generate more visibility to decision makers—particularly auxiliary decision makers who are important for future buy-in and success.

CONCLUSION

As Dragos' engagements have increased and our intelligence team has created coverage around industrial environments it has become shockingly clear that adversaries see opportunity in targeting, accessing and potentially attacking industrial environments. The challenge in going forward is not in finding misconfigurations, anomalies, and trojanized software but in rapidly creating a strong defense against human threats.

In many respects, these industrial environments are or can be architected to have strong defenses but that alone isn't enough to stop an attack. Humans who actively defend ICS networks through proactive and dynamic measures, such as hunting and developing behavioral analytics, are needed. Fortunately, the community is motivated and pursuing positive change, and Dragos is proud to be part of it.

2018 is the year the community will be challenged in how they respond to intrusions in industrial environments with the lack of visibility needed to understand the environment in enough detail to detect and stop an attack. Each organization should focus on the basic parsing of ingress/egress traffic as a means of identifying threats, as well as establishing an initial asset identification. As the community gains this maturity, proactive methods of seeking out the adversary and iteratively improving defenses will follow suit.

DRAGOS

DRAGOS, INC.

www.dragos.com

1745 DORSEY ROAD
HANOVER, MD 21076 USA
EMAIL: INFO@DRAGOS.COM