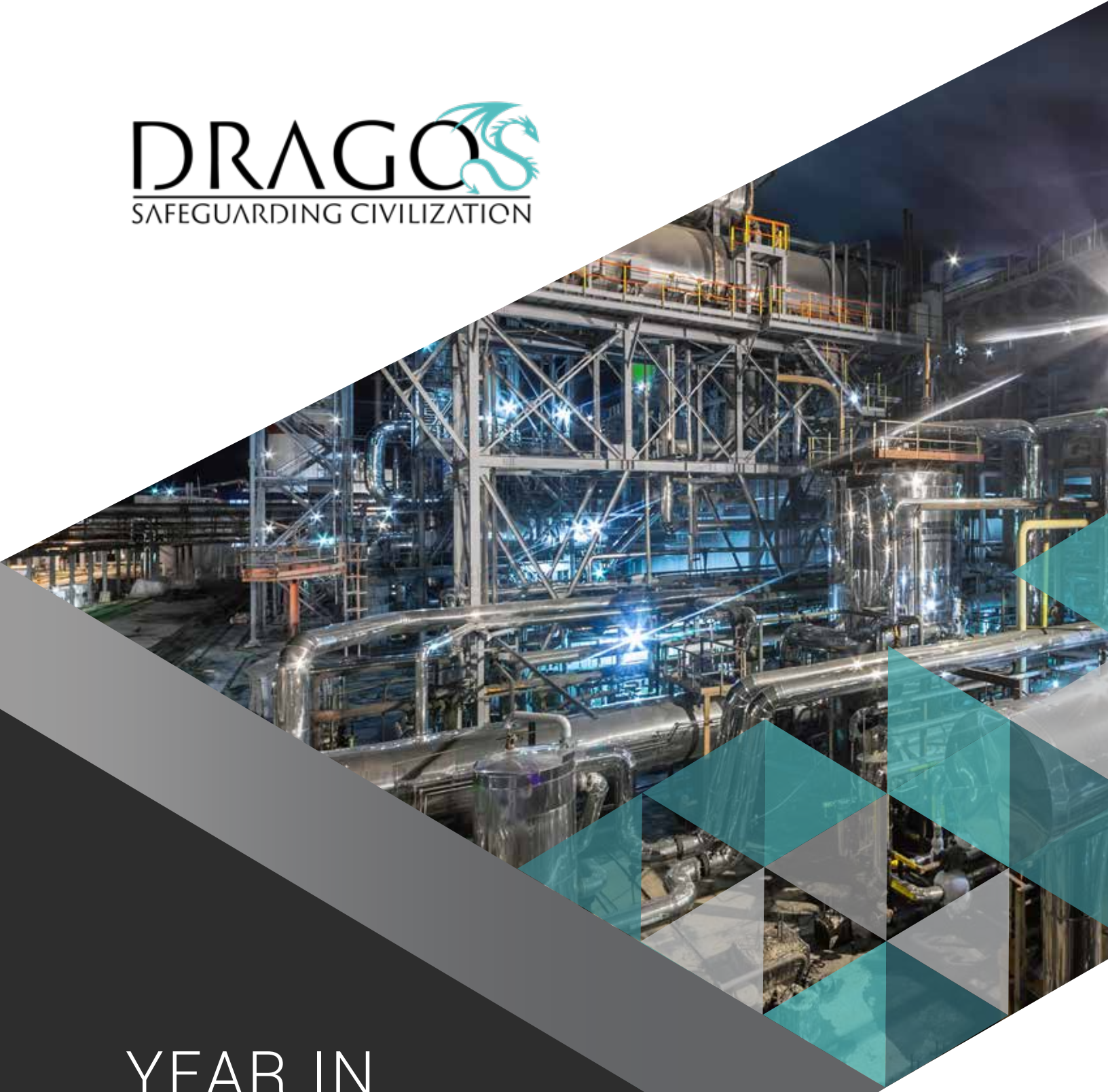
DRAGOS

SAFEGUARDING CIVILIZATION



YEAR IN REVIEW

2018

LESSONS LEARNED FROM THREAT HUNTING & RESPONDING TO INDUSTRIAL INTRUSIONS

The Dragos Threat Operations Center (TOC) provides a synopsis of lessons learned in 2018 while proactively hunting for adversaries in industrial environments and responding to industrial intrusions among oil and gas, electric, advanced manufacturing, water, mining, and transportation industries.

DRAGOS

CONTENTS

1 EXECUTIVE SUMMARY

2 PROBLEM STATEMENT

3 2018 SOURCE DATASET: SERVICE SUMMARY

4 CLIENT ENGAGEMENT OBSERVATIONS

5 CALL TO ARMS

6 CONCLUSION

EXECUTIVE SUMMARY

The Dragos Threat Operations Center (TOC) team provides client-facing services to the industrial control systems (ICS) community. Our team supports Dragos' mission of safeguarding civilization by working directly with ICS organizations to improve their protection, detection, and response capabilities through various proactive and responsive services, including: threat assessments, threat hunting engagements, tabletop exercises, incident response retainers, and ICS training.

Regardless of the service or engagement type, Dragos strives to collaborate with ICS asset owners to understand their unique challenges and considerations. Through these collaborative engagements, the TOC gains visibility into industry trends, shared challenges, and common improvement strategies. By sharing this information with the ICS community, our goal is to inspire productive discussion and facilitate improvements for all ICS organizations.

Rather than summarizing response engagements–similar to a common breach investigation report–this paper examines Dragos' customer engagements throughout 2018 to evaluate changes in the industry and discuss actions organizations can take to increase their networks' defensibility.

Dragos understands the market for ICS security vendors is growing and asset owners are looking for assistance when prioritizing actions to improve network security. In addition to the Call to Arms identified in this paper, Dragos reviewed the recently published NIST Cyber Security Framework and identified controls offering the greatest return on investment to industrial networks.[1] Organizations are taking the security of their control networks seriously and want to improve protection and detection capabilities. Dragos is focused on identifying practical approaches to facilitate these improvements.

1. NIST released a new version of their Cybersecurity Framework in April 2018. While this document maps several of the described controls to ISO/IEC 27001 (Table 2: Framework Core), there is no direct mapping to industrial control networks. Dragos is releasing a paper which interprets the original framework and translates recommendations a digestible plan addressing industrial networks.

PROBLEM STATEMENT: ICS NETWORKS MUST BE DEFENSIBLE

Problem Statement: ICS Networks Must be Defensible

Evolution of the threat landscape has forced industrial organizations to prepare for threats ranging from opportunistic ransomware to activity groups armed with the knowledge and tools to launch attacks against their processes. In response to these threats, industrial organizations have established requirements to build defensible networks, improve the security posture of existing networks, and arm analysts with resources to investigate alerts.

Asset owners are creating new security programs or extending existing programs further into their industrial environments. Some asset owners have begun mapping enterprise security programs into industrial environments without adapting them to their unique characteristics; the devices and technologies are unique and so should be the approaches. Applying specific IT solutions laterally to these networks will not result in a defensible organization, because the underlying infrastructure, devices, and data are not consistent.

For an ICS environment to be considered defensible, organizations must:
1. Develop a defense-in-depth strategy that enables the safety of the facility. Preventative controls should limit access to the facility without hampering the resilience or operation of the facility.
2. Have visibility and situational awareness beyond monitoring network traffic or keeping an asset inventory. Adding ICS security-centric knowledge to ongoing communications and assets facilitates an understanding of their roles and their importance to the overall industrial process.
3. Have staff and trained resources to actively monitor and understand behaviors (good and bad) occurring across facilities.

2018 SOURCE DATASET: SERVICE SUMMARY

2018 Source Dataset: Service Summary

Listed below are the six core service offerings the TOC provides, including the goal, lifecycle approach, and breakdown of service.

SERVICE	TARGET	PROACTIVE / RESPONSIVE	DESCRIPTION
Assessment	What is on the Network?	Proactive	Primary types: Architecture & Penetration Testing - Reviews network architecture, security controls, policies & procedures, identifies weaknesses/ provides areas of improvement - Assesses device or network security controls through active testing and execution of code
Incident Response	Is the Network Under Attack?	Proactive (Retainer) & Responsive (Rapid Response)	IR retainers & rapid response
Managed Detection & Response	Is the Network Under Attack?	Proactive & Responsive	Analysts continually perform periodic triage and hunting of network traffic via remote access to an implementation of the Dragos Platform
Tabletop Exercises	How do I Respond to Threats or Compromise?	Proactive	Dragos' TOC and intelligence teams design custom scenarios based on legitimate threats within client's vertical--includes multiple business units
ThreatView	What is on the Network? Is the Network Under Attack?	Proactive	Dragos applies custom threat behavior analytics--based on first-hand experience and intelligence of current activity groups--to proactively hunt for and identify adversary tradecraft
Training	How do I Respond to Threats or Compromise?	Proactive	Dragos' TOC generates content for the 5-day ICS training course, hosted quarterly at Dragos' headquarters

CLIENT ENGAGEMENT OBSERVATIONS

The following data correlations are focused on engagement types that involve work within client spaces: assessments, incident response (IR), managed detection and response (MDR), tabletop exercises, and ThreatView.

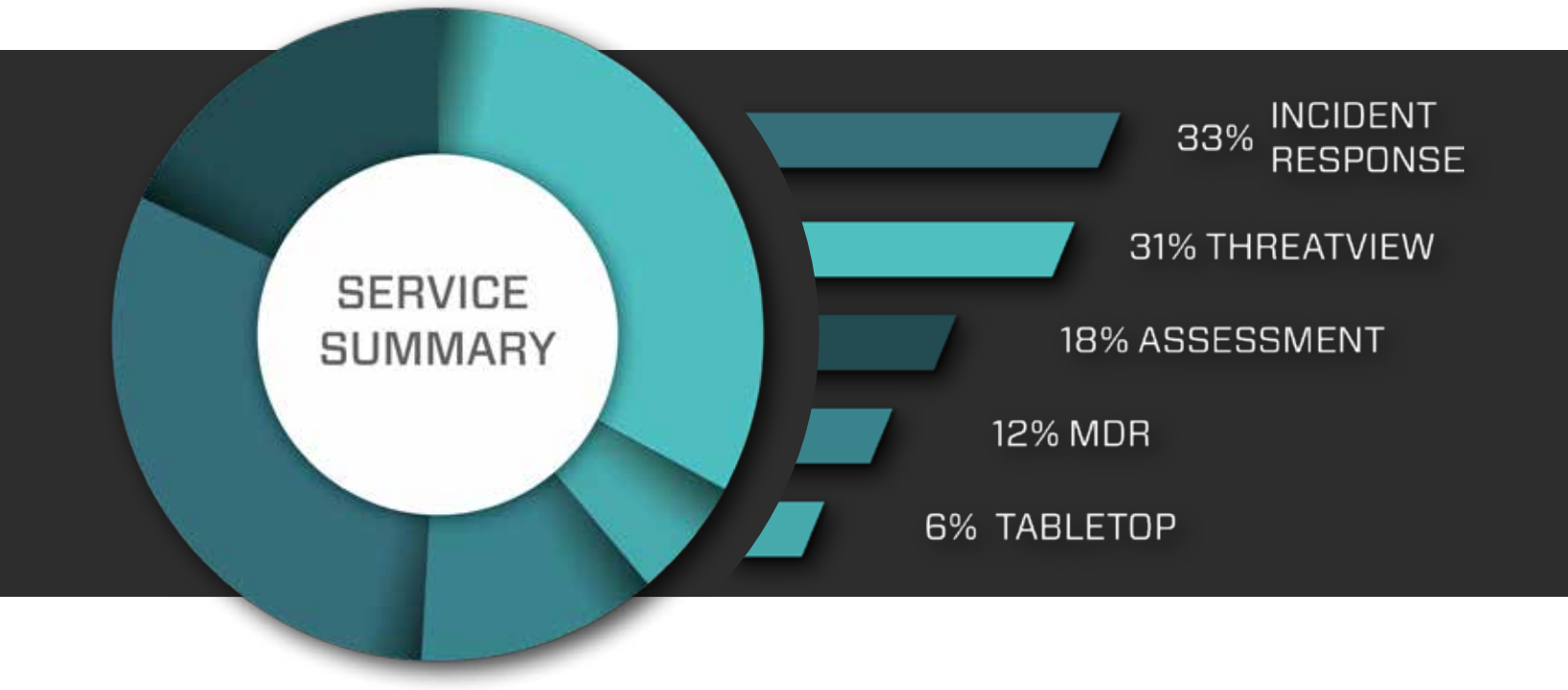
ENGAGEMENT DISBURSEMENT

VERTICAL DISTRIBUTION

PROACTIVE VS. RESPONSIVE

PROACTIVE OBSERVATIONS

RESPONSIVE OBSERVATIONS



Engagement Disbursement

Approximately 33% of the Dragos TOC engagements in 2018 were IR, including active incident handling and acquired retainers. The second largest category was ThreatView (31%), followed by assessments (18%), MDR (12%), and tabletop exercises (6%).

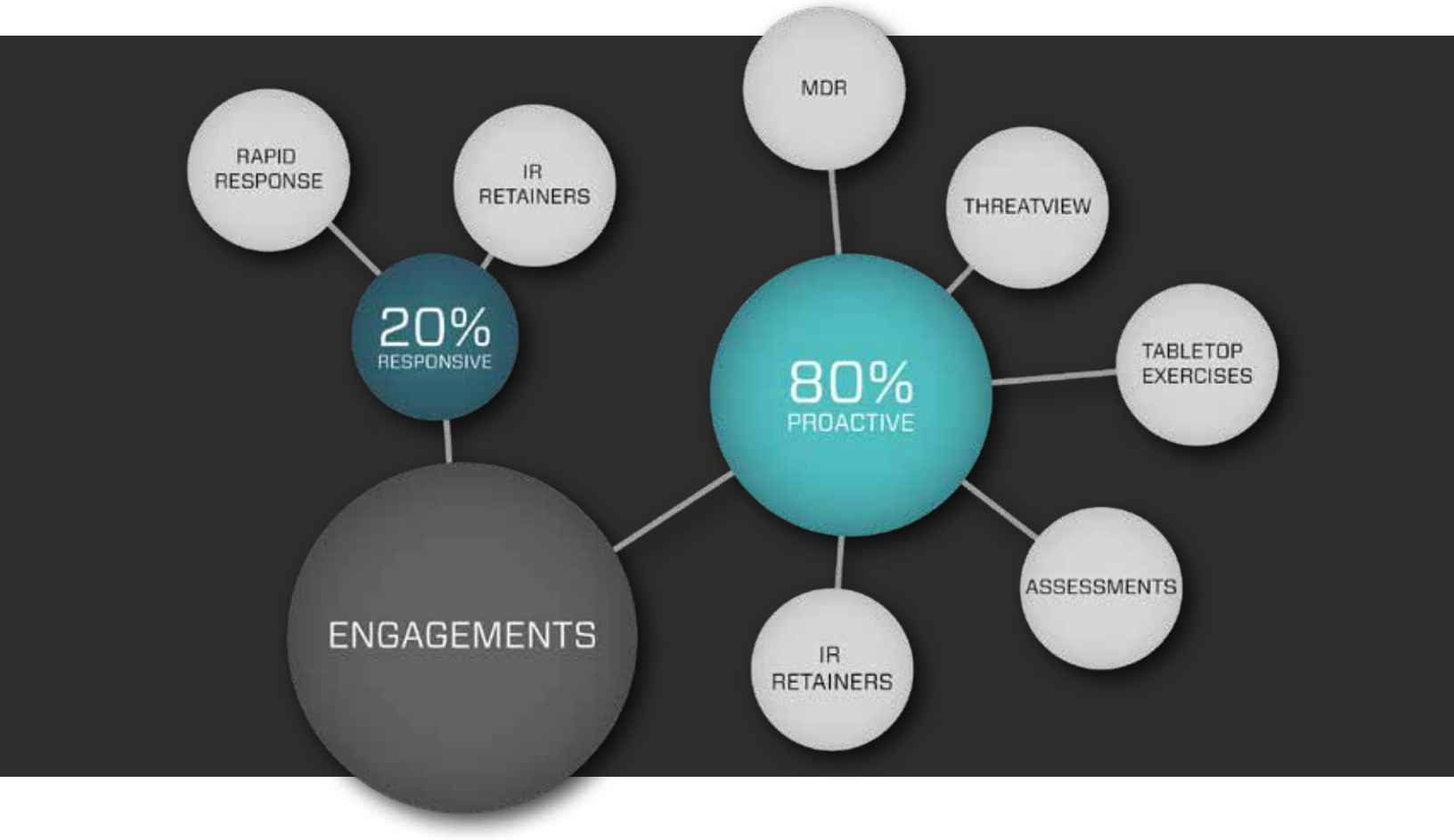
The majority of our engagements were in response to our clients requesting help to gain an understanding of their industrial environments and to identify active threats through threat hunting. Our second most requested engagements stemmed from our clients wanting to be better prepared to handle incidents and respond to active intrusions. These engagements concentrated on handling an event either through practice or confirmed compromise.

Vertical Distribution

The primary verticals Dragos engaged with throughout 2018 were focused on energy (oil, gas, electric, transmission, generation, management, and renewables). This sector accounted for 56% of all engagements. The remaining 44% was equally split between engineering and production of chemical, biomedical, and pharmaceutical products; manufacturing; transportation and shipping; water utilities and wastewater treatment. No vertical was limited to a specific engagement type or technical focus (network vs device).

It is evident smaller communities exist throughout the larger ICS community; these may be based on region, vertical, or shared assets. Upon completion of a project, other providers within the same sector would contact Dragos for similar services. While not unexpected, this demonstrates that trust is crucial; organizations are looking for assistance, but welcoming a third party to evaluate the network(s) is still highly scrutinized. A promising conclusion is that communication and data sharing is taking place within each sector. Organizations are leveraging trusted relationships with peers to better the industry.

Of note, multiple clients were device or service vendors. Engagements in this space included advising on projects, assessments of hosting platforms (firmware updates), and device penetration testing. This is an encouraging message for the industry: motivation from vendors to secure devices and protocols is increasing. The vendors Dragos performed work for are not business partners, but independent organizations that are focused on improving the security of their devices and protocols.



Proactive vs. Responsive

Approximately 20% of engagements were responsive (rapid response and IR retainers leveraged for an incident). These engagements were launched due to suspicion or confirmation an active engagement was underway and response assistance was requested. The remaining 80% were proactive (ThreatView, assessments, tabletop exercises, MDR, and IR retainers that were not leveraged for an incident). These engagements were launched with no indication or prior suspicion the network was compromised.

The graphic above validates the threat of ICS network compromise, while also showing industries' proactive stance and desire to improve. Proactive engagements were launched with no indication or prior suspicion the network was compromised. Reactive engagements were launched due to suspicion or confirmation an active engagement was underway and response assistance was requested.

Proactive Observations

One of the most encouraging revelations was the scope at which companies are considering improvements to security. Several clients requested assistance in designing the "utopian network," which puts security and defensibility at the forefront of the strategy. The approach of crafting a network's workflow, components, and architecture without limitation, then refining the roadmap based on available resources proved to be very useful. Once completed, the roadmap for future growth and enhancements was already in place and had been communicated to stakeholders as part of the previous project.

Several client requests were focused on understanding existing network architecture, current security posture, or identifying where additional investments should be made (assessments and ThreatView making up 52% of all engagements). These clients understood network defensibility was a priority and requested assistance in identifying where improvements should be made. Navigating possible improvements to these complicated networks is not straight forward. Taking into account their current security postures, several organizations requested assistance prioritizing which actions offered the largest return on investment. Understanding each network security team has finite resources and using a third party to assist prioritization can help ensure the roadmap is appropriate for the organization's current challenges. Furthermore, with the convergence of IT and OT, more collaboration between teams is occurring and infrastructure is increasingly shared between them, data is aggregated and shared between network segments, and there is more potential for monitoring; these capture points, however, may only offer partial visibility and can be complicated with other traffic types.

Customer questions were focused on visibility: What data is important? Where should data be gathered from? What capture points are advantageous? Each answer is unique to the network's design, data, and threat landscape. Dragos believes consistent monitoring of the network with technology focused on adversary tradecraft and in-depth asset classification are primary capabilities organizations should strive for as a part of their ICS cybersecurity solutions. These capabilities are best achieved through both technical and personal means.

Responsive Observations

IR engagements were not focused on a specific vertical or industry. Incident response involving a domain-wide compromise is never a quick process, and being successful requires a methodical approach. As with any other large effort where failure can result in large financial or health consequences, planning and preparation are crucial to success.

37% of IR engagements involved an initial vector dating over 365 days, while all other engagements were either inconclusive or detected and contained by facility teams and Dragos as they occurred.

In 2017, Dragos reported the original infection vector to ICS attacks remained unknown;[2] in 2018, this is still the case. One primary challenge for IR on industrial networks is performing root cause analysis (RCA), partially because a common vector into the ICS network is through the associated business or IT networks. An external adversary may not have knowledge about the network topology and must discover or create an access method to the ICS segments. Finding this pivot point can take time, so the adversary may exist in the IT network for several weeks or months prior to pivoting into the OT network. RCA in these instances requires larger data retention and resources for investigation. RCA faces several additional challenges, as network traffic logging in ICS networks is generally not verbose, and visibility to lateral movement can be insufficient. Unfortunately, internal politics and team organization can also delay investigative efforts.

A key advantage defenders have over adversaries is a pre-understanding about the network. Performing IR without directly leveraging all available knowledge would avoid this advantage, which is why it is important for external teams to work directly with internal network teams. There is no standard organizational structure for IR using consulting services; Dragos has led response efforts and reported findings directly to organizations' boards, as well as supported investigations reporting to network managers. Workflows are usually contingent on local resources available, and success is not focused on one reporting hierarchy over another. More importantly, organizational and external resources need to collaborate to maximize efficiency. No one understands a network better than those challenged with the continued operation and security of the devices. Dragos firmly believes our role in each engagement is working with the asset owners to improve the network's defensibility--this is especially important during incident response.

Multiple IR engagements were initiated without confirmation that an adversary was present or that a cyber attack took place. Device failure, equipment malfunction, or other odd activity were enough justification for some organizations to bring in IR services, secure external advisors, or initiate IR contracts. A trend has developed where ruling out cyber as a potential cause for unexpected behavior is a top priority. 25% of our IR engagements were focused on determining if a specific embedded device was trustworthy or had been modified in order to rule out cyber as a cause. If multiple devices fail within close succession of each other, organizations desire ruling out adversary activity in parallel to restoring services. Potential consequences are boundless, and the threat landscape has demonstrated these concerns are legitimate.

2. Common infection vectors to ICS networks were discussed in the Dragos Hunting and Responding to Industrial Intrusions paper, which summarizes engagements through 2017.
This paper can be found here: https://dragos.com/media/2017-Review-Hunting-and-Responding-to-Industrial-Intrusions.pdf

CALL TO ARMS

MEASURE VISIBILITY THROUGH A COLLECTION MANAGEMENT FRAMEWORK

FORMALIZE HUNTING PROCEDURES

PREPARING INTERNALLY FOR INCIDENT HANDLING

Call to Arms

Resources are finite in every organization. With the growth of the ICS security industry and increased awareness of threats, organizations often need help determining where to dedicate network security resources. To identify action items organizations should focus on, consider the initial 3 questions mentioned in the opening of this paper: What is on my network? Is my network under attack? How do I respond to threats or compromise?

As new companies enter the ICS cybersecurity market and the market grows, there will continue to be more offerings of technologies and tools. Dragos, while a product company, understands not all organizations are interested in deploying new technology, and we're focused on identifying actions that increase preparedness and require no resources other than time. As a company mission, we are focused on educating the community on practical actions that are available to everyone.

Measure Visibility Through a Collection Management Framework

Several ICS networks mature over time while being extended to adopt new functionalities and support additional devices. Retroactively identifying everything on the network can require a substantial effort. To tackle this problem, Dragos recommends creating a Collection Management Framework (CMF).

A CMF measures visibility by allowing analysts to quickly see what is on the network and, more specifically, what data is available to facilitate triage. While a CMF should be built out through a formal process, it can start with humble beginnings and does not require purchased resources. Guidance on approaching a CMF has previously been released by Dragos and is available for reference.[3]

3. Dragos has released material to define a Collection Management Framework, discuss the creation of a CMF, and examine multiple use cases. These documents and webinar can be found here: https://www.youtube.com/watch?v=fpvJl5pn4bA&feature=youtu.be

Formalize Hunting Procedures

"Threat hunting" continues to gain popularity as buzzwords for network security. Organizations are dedicating resources to hunting, while the term remains nebulous. At its core, threat hunting is proactively looking for signs of compromise without relying on alerts from existing security controls. Threat hunting has the potential to detect a compromise, identify vulnerabilities, and help analysts discover existing configurations that can be refined to improve protection and detection.

Formalized hunting procedures help ensure maximum return on the resources used. Multiple organizations have released whitepapers and blogs discussing hunting tactics. Dragos has released papers on formalizing the process to understand initial goals and calculate return.[4]

4. Dragos' whitepaper A Practical Model for Conducting Threat Hunting defines a formal model for conducting threat hunting and standing up a dedicated hunting program. This paper can be found here: https://www.sans.org/reading-room/whitepapers/threathunting/practical-model-conducting-cyber-threat-hunting-38710

Preparing Internally for Incident Handling

The ultimate goal in IR planning should be a comprehensive response plan that includes all business units and forensic capability across organizations' implementation of the Purdue Model. Under ideal circumstances, all resources to investigate a compromise through RCA would be readily available; however, this is rarely the case, and RCA may not be possible, given multiple variables. Consistent monitoring for adversary behavior across ingress, egress, and lateral traffic remains the single best strategic and tactical action organizations can take to facilitate detection and investigation of compromise. In addition to establishing a CMF to expedite evidence collection, Dragos has presented additional actions that can aid in the IR process.[5]

Continual testing through hands-on exercises and tabletop exercises should also be considered to challenge and improve existing plans and procedures. To get the most return on investment during tabletop exercises, efforts should be taken to generate realistic scenarios involving logical adversary tactics. When conducting tabletop exercises with doomsday scenarios or disjointed techniques, practical approaches are lost, and the measure of success can feel out of reach. When possible, involving multiple business units in tabletop exercises allows each individual unit understand the hand-off points between teams.

5. Dragos presented on the primary goals of incident handling and actions an organization should do to prepare for incident handling in "IR: Learning as you go is Expensive" at CS3STHLM, 2018.
That presentation can be found here: https://www.youtube.com/watch?v=qYMCh51aHJ0&feature=youtu.be

CONCLUSION

The industrial cybersecurity industry is evolving and continuing to mature. More ICS-specific attacks were discovered in 2018, and several public storylines centered on doomsday narratives; however, it is important to realize that understanding the ICS network facilitates all aspects of protection, detection, and response. Dragos' engagement types throughout 2018 demonstrate that the industry is focused on hunting for adversary tradecraft, but is also focused on increasing knowledge of their own networks--which is just as important.

The allocation of engagement types also demonstrates a wide gap in maturity. Dragos does not view this as a negative finding; we are encouraged by the increasing number of organizations aiming to strengthen defensibility. Each network has peculiarities for consideration, but the fundamental challenges facing all asset owners and vendors are not that different. Concerns from small utilities are echoed by large organizations and even vendors. Communities are sharing information about what works and what doesn't. Overall, verticals are getting better, networks are becoming more defensible, and Dragos believes continued collaboration is how we maintain this momentum.