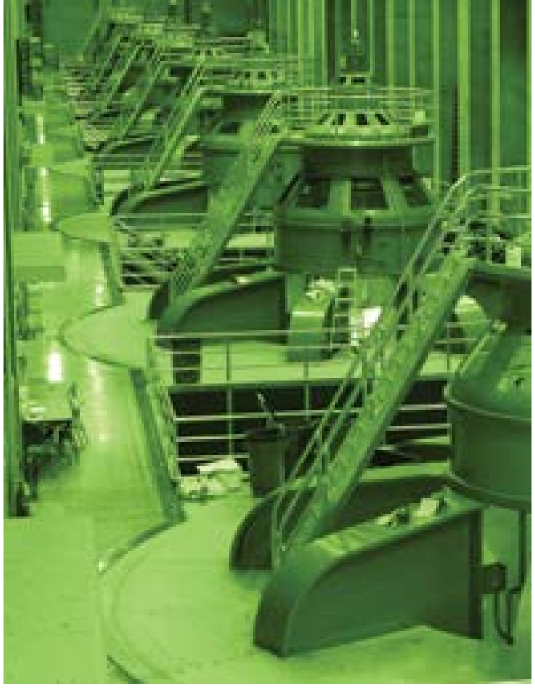
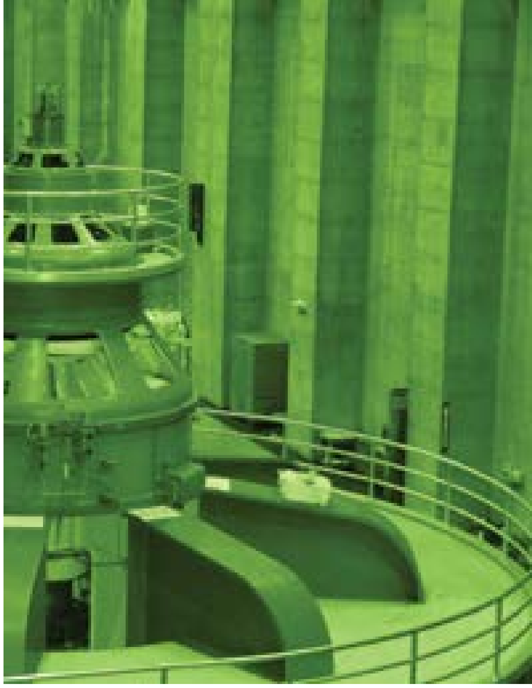



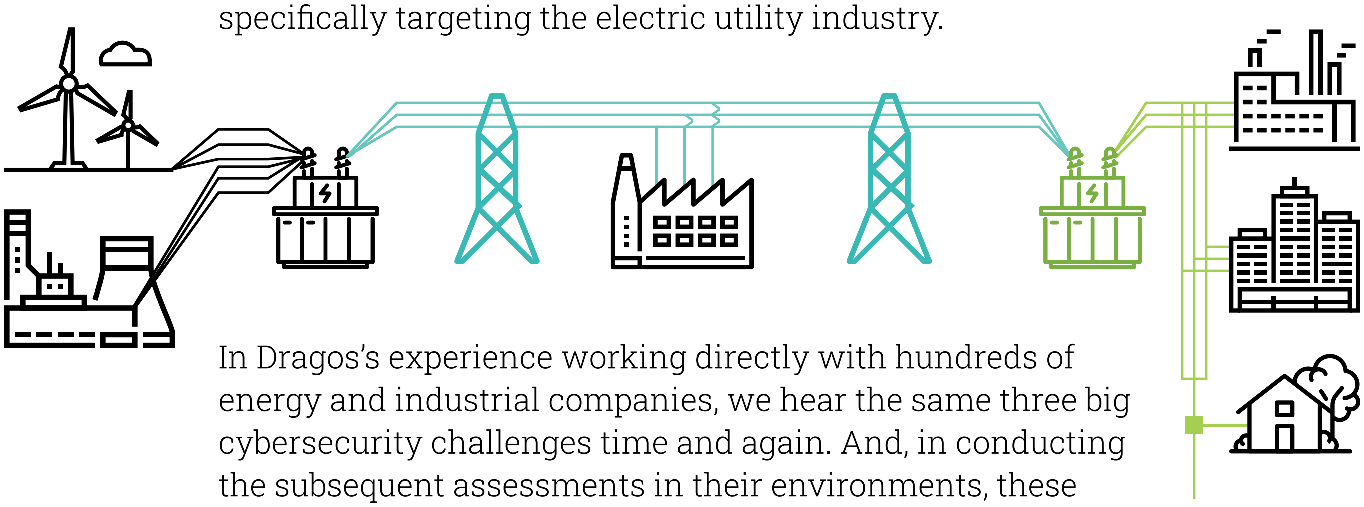
Top 3 Cybersecurity Challenges Facing Electric Utilities

HOW COMPANIES CAN BETTER SECURE SMART GRID TECHNOLOGY

DRAGOS

INTRODUCTION

The business benefits of digital transformation in electric grid operations are tremendous, but this progress also greatly expands the cyber risk to the OT environment - safety, unscheduled downtime, and negative impact on corporate brand are most often cited. When electric utilities use cloud-connected software to better automate their operations, bolster predictive maintenance, or connect industrial devices to business intelligence platforms, they are by definition more tightly coupling Operations Technology (OT) with Information Technology (IT) systems. At the same time, an accelerated shift to remote access greatly opened the “attack surface” to threat vectors that didn’t exist in the recent past. Dragos now has identified and tracks 15 different industrial threat activity groups, 14 of whom like ELECTRUM and XENOTIME are specifically targeting the electric utility industry.



In Dragos’s experience working directly with hundreds of energy and industrial companies, we hear the same three big cybersecurity challenges time and again. And, in conducting the subsequent assessments in their environments, these challenges are affirmed by what our team finds. The good news is that there are practical steps asset owners and operators can take in order to enhance the security of their Industrial Control Systems (ICS) environment and effectively mitigate cyber risk – today.

THE THREE CHALLENGES ARE:

1 Complete OT Asset Visibility

2 Understanding & Detecting OT Threats

3 IT & OT Cybersecurity Gap

CHALLENGE 1

Getting to Complete, Automated OT Asset Visibility

From turbines to temperature controllers and everything in between, asset owners know that safety, uptime, and reliability can all be impacted by cyber attacks. Even more common are operational issues that can cause outages, ranging from faulty equipment to simple misconfigurations or operator error. That's why knowing what's on the OT network, and precisely which assets are communicating with one another, is critical to keeping operations running.

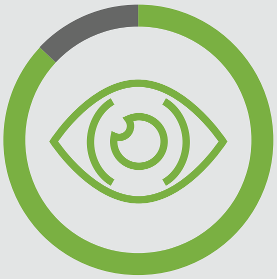
Many organizations have taken steps in the right direction by building an enhanced asset inventory and monitoring IT to OT boundary communications, but lack true visibility of the OT environment.

Without central visibility into asset vulnerabilities, and a closed loop to manage the controls which address them, whether they include patching, configuration changes, or port/protocol/ routing changes, cybersecurity teams will be spread thin if they are relying on offline spreadsheets and checklists between multiple locations.

When organizations lay the groundwork by fully identifying and inventorying their OT assets, every cybersecurity process becomes easier, whether it is leveraging threat detection, initiating incident response, actively managing assets for vulnerabilities and weaknesses, or implementing overarching strategic OT security initiatives. Continuous OT asset visibility and monitoring capabilities make it possible to discover:

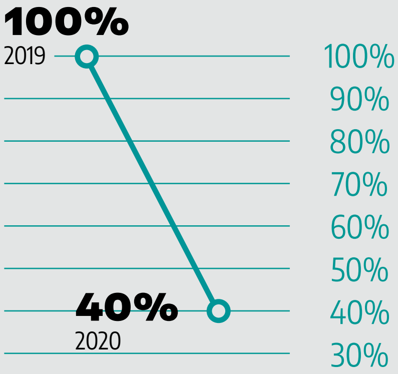
- ✓ **connectivity and communications channels operators didn't know existed,**
- ✓ **active threats operating quietly in the environment,**
- ✓ **insecure configurations,**
- ✓ **latent vulnerabilities,**
- ✓ **rogue assets and more.**

87% of electric industry customers had limited or no visibility into their ICS environments



Source: Dragos 2020 ICS Cybersecurity Year in Review

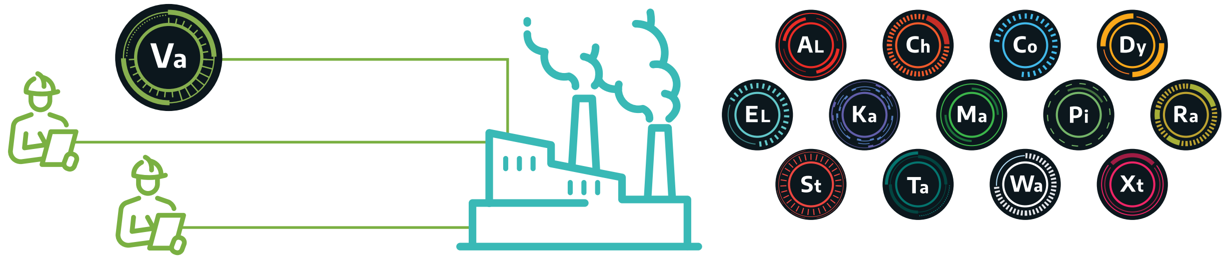
External Routable Network Connection to Electric Industry ICS Environments Believed to be Air-Gapped



Source: Dragos 2020 ICS Cybersecurity Year in Review

> **"When [the engineers are] busy, there are things, especially documentation, that goes by the wayside, and having the asset verification where we can see things coming and going as they're being added to the network has been actually very useful for them and for us."**
>
> — Mark Johnson-Barbier
> Cybersecurity Architect
> Salt River Project

ICS ACTIVITY GROUPS TARGETING ELECTRIC SECTOR



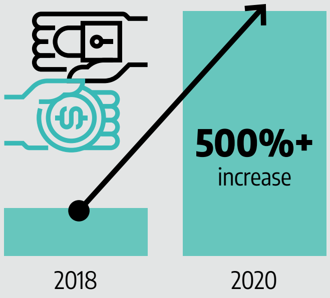
CHALLENGE 2

Understanding and Detecting Threats to OT Environments

Though OT infrastructure was once locked down by hardwired assets and segmented environments that were difficult to breach, the digitalization of operations has increased connectivity and opened up industrial environments to state-sponsored and financially-motivated threat actors. Dragos adversary hunters now track 15 distinct threat activity groups, and 14 of them specifically target the electric sector.

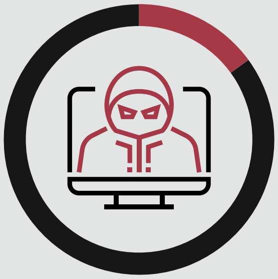
Some of these activity groups, like PARISITE and KAMACITE, serve as access operations for other groups who may deploy ransomware or malware capable of directly impacting industrial processes. They are eyeing vulnerabilities in the IT environment, and at the Demilitarized Zone (DMZ), as a viable entry point to OT infrastructure. This includes compromise of Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) assets, which are common access points for OEMs and integrators to gain access to operations environments. Although many organizations focus on prevention and segmentation, obtaining access through a compromised VPN may allow an adversary into an ICS network – which underscores the necessity of strengthening the pillars of a successful ICS cyber strategy: detection, response, and recovery.

Ransomware attacks on industrial entities increased **more than 500%** since 2018



Source: "Ransomware in ICS Environments," Dragos/IBM, December 2020

Only **25%** of Dragos penetration testing customers in the electric industry were able to detect Red Team activity in real-time



Source: Dragos 2020 ICS Cybersecurity Year in Review

#1 MITRE ATT&CK FOR ICS TTP:

Valid Accounts T0859

Source: Dragos 2020 ICS Cybersecurity Year in Review

CHALLENGE 3

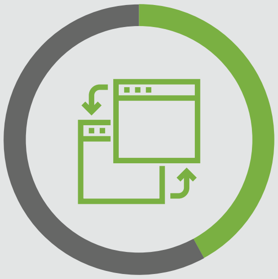
The IT/OT Cybersecurity Gap

Fundamentally, OT is very different from IT. While it is IT security's purpose to protect information in the business environment, OT has a different mission, different systems, different threats, and different impact on organizations than IT. Safety, environmental impact, and process availability are key for OT. Many of the basics of IT security simply do not apply and should not be copied and pasted into the OT environment.

For example, vulnerability and patch management are fundamental to IT security, but much less important for OT because many of the vulnerabilities in OT don't necessarily threaten the ultimate safety or mission of that OT system. A recent Dragos study found that some 77% of all industrial vulnerabilities don't actually introduce any risk, and a further 43% of vulnerability advisories (42% in electric) were inaccurate. Which means that in the industrial world a patch-at-all-costs mindset doesn't make sense so much as one that has organizations smartly patching but prioritizing mitigation strategies like segmentation and threat detection instead.

In the event of a suspected cyber incident, the IT/OT cybersecurity gap can be exacerbated. Security teams investigating an incident need access to detailed logs of network communications in the operations environment, but according to Dragos's incident response (IR) cases in ICS over the past year, this is often a manual, time-consuming process meaning many critical questions go unanswered. In at least one case, the impact led to public reporting without an understanding of root cause analysis where cyber activity was heavily suspected, but no evidence was available. Lack of effective communication across IT and OT teams during a crisis can lead to inadequate resource allocation, compound risks to assets and personnel, and create lingering effects on bottom line operations.

42% of electric industry ICS vulnerability advisories contain incorrect data



61% of those advisories had a patch, but no alternate mitigation advice.

0%

of IR cases were facilitated by automated logging into ICS network

0%

of customers in the electric industry had a communications plan linked to IRP activations

Source: Dragos 2020 ICS Cybersecurity Year in Review

OT = IT + Physics

The overarching lesson is that there are definitely lessons to learn from IT cybersecurity but as organizations seek to improve OT cyber capabilities it doesn't make sense to copy and paste your enterprise cybersecurity strategy into the ICS. Where might this communication and bridge-building begin? Many organizations benefit greatly from workshops, also known as tabletop exercises, that utilize consequence-driven scenarios to help IT and OT personnel understand what information, communications, and actions are required in the event of a cyber incident.

From there? Contact us today so that we can understand where you are in your ICS cybersecurity journey and work together to build a roadmap to safe, reliable operations.

> **"Where Dragos differentiates from many [competitors] is in the ICS-focused expertise of its team, reflected in its intelligence-centric approach, where its deep and detailed knowledge of the specifics of the ICS threat landscape are born out of experience."**
>
> — 451 Research

Dragos is your industrial cybersecurity ally

Dragos, Inc. was founded with the mission to safeguard civilization against one of today's most dangerous, far-reaching threats: cyberattacks on OT networks and control systems. Our ICS/OT practitioners have been the first responders of the world's most significant industrial cyber-attacks, including the 2015 and 2016 power grid offenses in Ukraine, as well as the 2017 Saudi petrochemical safety system attack, and know industrial adversaries better than any other organization.

Armed with this knowledge, our team of industry experts created purpose-built solutions to deliver unprecedented knowledge and capability to protect operational systems. We've worked with 9 of the 10 largest industry organizations spanning generation, transmission, and distribution operations to help them better understand and protect their OT environments.

THE DRAGOS DIFFERENCE:

TECHNOLOGY

The Dragos Platform is the most effective and efficient ICS/OT Technology on the market, going beyond asset visualization with analytics that identify threats and are correlated to the leading industry standard MITRE ATT&CK for ICS.

EXPERTISE

Dragos has the largest and most trusted team of ICS/OT experts with over 700 years of practitioner experience. Our team has helped hundreds of organizations, and nations, assess and strengthen their security posture and improve the capabilities of their IT and OT cybersecurity teams.

FRONTLINE ALLY

Your success is our success. We're committed to ensuring you're equipped and empowered to identify and respond to threats before they become breaches. With Dragos as your ally, you are a part of the mission. The mission where ecosystems are empowered, adversaries are outsmarted, and civilization is safeguarded.

To learn more about how Dragos can help you solve these challenges, email us or visit us on the web.

DRAGOS

Dragos is an industrial (OT/ICS/IIoT) cybersecurity company on a mission to safeguard civilization.

Dragos is privately held and headquartered in the Washington, D.C. area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

Dragos.com