INDUSTRIAL STRENGTH CYBERSECURITY FOR ELECTRICAL SUBSTATIONS

In recent years, there has been a continual rise in sophisticated cyber attacks on electric infrastructure globally with the intent of causing significant operational disruptions. Substations are critical components of the generation and transmission of electricity, making them a top target. Cyber attacks, if successful, can disconnect generation and transmission lines resulting in grid failures and widespread blackouts.

For years, Dragos has enabled the electric utility industry to manage cybersecurity risk with the most effective and efficient industrial control systems (ICS) / operational technology (OT) cybersecurity technology on the market. Our Threat Intelligence team closely monitors threats to industries, identifying and tracking 19 different threat groups, 16 of which specifically target the electric industry.

THE CHALLENGES

Substations are often located in remote and dispersed locations, and monitoring and controlling these sites has often been difficult. To solve this problem, utilities began installing remote terminal/telemetry units (RTUs) at substations. Early RTUs were initially custom-made units, but later versions relied on standard hardware such as programmable logic controllers (PLCs) or industrial PCs.

Intelligent electronic devices (IEDs) are a more recent technology development, and these devices are now installed at most substations to some extent. These IEDs generally communicate with the substation RTU. Supervisory Control and Data Acquisition (SCADA) systems are used for remote supervision and control.

Communicating with substations poses significant challenges from a cybersecurity perspective. Where remote access is possible through cellular or satellite communications, opportunities for attackers to access OT environments increases. Older substations using serial communications face threats from on-site personnel through the use of transient devices (e.g., laptops), unauthorized routable connections, and compromised USB peripherals.

THE SOLUTION

Visibility into substations provides the ability to identify and correlate suspicious network, host, and process events and can assist in identifying intrusions as they occur. Prioritizing the security ofsubstations based on criticality to the grid must be done, recognizing that their importance can vary from peak load to low load periods.

Addressing the OT visibility challenge requires a technology platform that provides comprehensive visibility of assets, vulnerabilities, and threats.

CASE STUDY

One of our largest electric utility customers based in Europe trains their Commissioning Engineers on how the Dragos Platform can detect and identify attacks on the substations. They launch real attacks and then show the engineers what this looks like on the devices, how it's seen and tracked in Platform, and how to react if it is a real event.

ASSET VISIBILITY
What is on my network?

The Dragos Platform passively identifies industrial assets and network communications with its comprehensive protocol, vendor, and equipment coverage. Backed by our exclusive ICS/OT vulnerability knowledgebase, you'll know precisely which vulnerabilities to remediate with a patch, and those that can safely be mitigated by other means based on our team's recommendations.

THREAT VISIBILITY
Who is on my network?

The Dragos Platform, the only offering on the market enabled with the industry standard threat framework MITRE ATT&CK® for ICS, detects threats using our industry-leading threat analytics, and provides security teams with expert guided investigation and response with our playbooks.

IT-OT GAP
How to fill the gap?

We understand the differences between IT and OT domains, and the logical and cultural boundaries between them. Our products and services focus on filling the need for the knowledge and capabilities required to provide support in the OT domain, including its mission, mean time to recovery driven metrics, and safety and resilience-oriented priorities.

OUR EXPERTISE

We offer the largest and most trusted team of ICS/OT experts with practitioner experience across electricity generation, transmission, and distribution, as well as in contributing to NERC CIP, NIST CSF, and C2M2.

YOUR FRONTLINE ALLY

Your success is our success. We're committed to ensuring you're 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.

ABOUT DRAGOS, INC.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquarted in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.