DRAGOS

Case Study:

Implementing the Dragos Platform to Solve ICS Cybersecurity Challenges in the Electric Industry

By: Dragos, Inc.

Foreword

Electric utilities are an integral component of critical infrastructure, and as such, are unique targets for adversaries who aim to disrupt their operations and the day-to-day lives of people who depend on them. The interconnectivity between IT and OT networks continues to grow– expanding attack surfaces within electric utilities' industrial control systems (ICS) environments–and introducing new threats and compromises previously not visible to organizations.

For example, the first malware framework designed and deployed to attack electric grids (CRASHOVERRIDE) occurred in Kiev, Ukraine in 2016, which targeted a transmission substation and resulted in electric grid operations impact.[1] More recently–as reported by the Dragos Intelligence team in the 2018 ICS Year in Review report–in April of 2018, numerous electric utility organizations were forced to shut down communication connections and suffered hampered data processing due to a cyber incident caused by a commonly-used business tool.[2] Additionally, the Dragos Threat Operations Center (TOC) engaged with numerous electric-focused utilities throughout 2018, with the electric industry contributing into the overall 56% of all TOC engagements throughout the year.[3]

As the number of adversaries specifically targeting the electric sector continues to grow, electric utilities must have a holistic picture of their environments, the adversarial tradecraft targeting them, and they must be armed with the tools to effectively identify and respond to threats. The Dragos Platform helps industrial organizations achieve this by providing comprehensive network asset visibility and identification, knowledge of threats through intelligence-driven threat behavior

[1] Dragos' whitepaper analyzing CRASHOVERRIDE in-depth can be found here: https://dragos.com/resource/crashoverride-analyzing-the-malware-that-attacks-power-grids/

[2] More on ICS-specific threats targeting industrial organizations can be found in Dragos' 2018 Year in Review: ICS Threat Activity Groups and the Threat Landscape: https://dragos.com/wp-content/uploads/yir-ics-activity-groups-threat-landscape-2018.pdf

[3] Read Dragos' TOC 2018 Year in Review report here: https://dragos.com/resource/lessons-learned-from-threat-hunting-responding-to-industrial-intrusions/

©2019 Dragos, Inc.

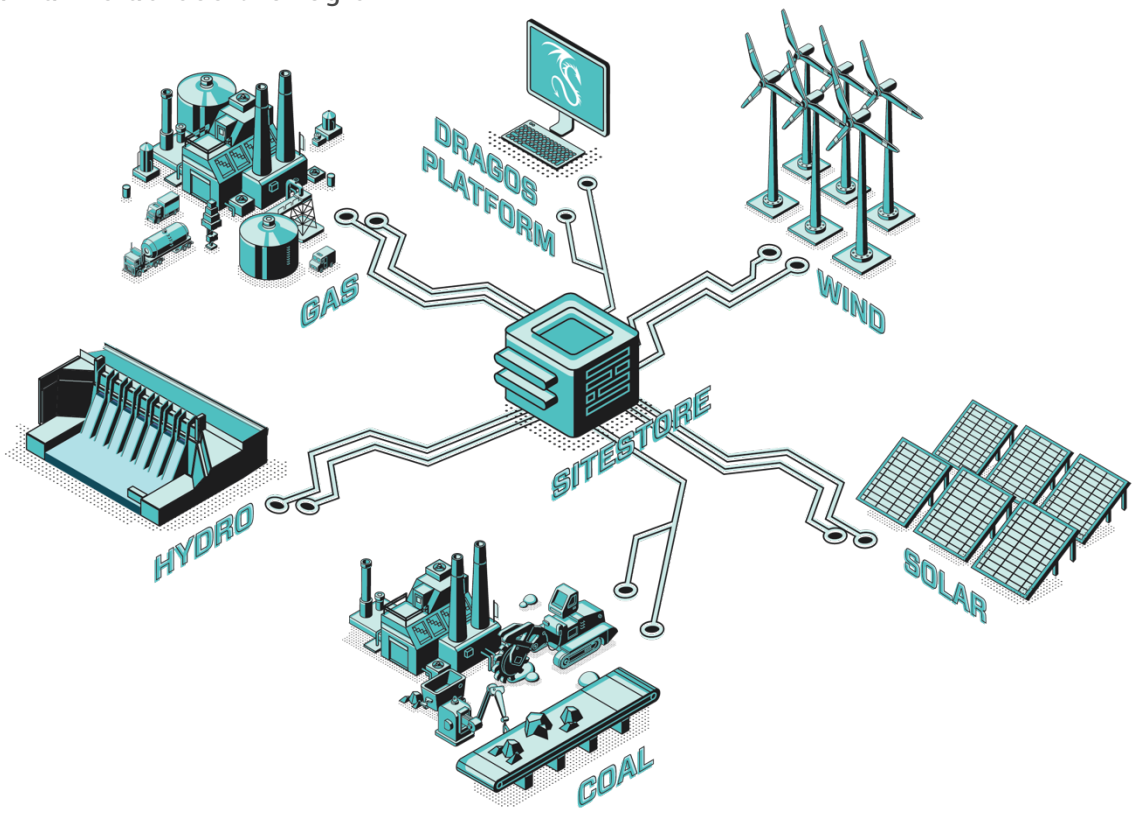
analytics, and a workbench with prescriptive, step-by-step playbooks to investigate incidents.

This case study reviews an electric utility company in the U.S.[4] that successfully implemented the Dragos Industrial Cybersecurity Platform in early 2018 and discusses the challenges faced by plant managers, IT teams, and OT teams in driving enhanced ICS/OT security and how the Dragos Platform helps combat these challenges.

Introduction

A mid-sized electric utility in the US that serves more than one million customers adopted the Dragos Industrial Cybersecurity Platform in early 2018. This utility generates electricity across low-sulfur coal, natural gas, wind farms, and solar farms.

Dragos deployed 16 sensors across the utility's two data centers to monitor communications in the Energy Management System (EMS) and Demilitarized Zone (DMZ), four gas plants, two coal fire generation plants, three wind farms, and its solar farms across the region.



[4] The utility name is withheld for the public report, but is available as a reference to prospective customers.

©2019 Dragos, Inc.

Challenges of Securing Electric Utilities

The electric grid can, at a high level, be categorized into three functions: generation of electricity at power plants, transmission from the power plants across typically long distances at high voltage, and lower-voltage distribution networks that power customers. Along these long transmission and distribution systems are substations that transform voltage levels, serve as switching stations and feeders, and fault protection. Many industries feed into the electric grid, and those differences require an in-depth understanding of the different systems and communications–which means, there is no one-size-fits-all security approach to protecting them and it requires comprehensive understanding of the highly heterogeneous nature of their environments.

The challenges expressed by the electric utility discussed in this case study include:

- Lack of visibility of ICS environment and asset management
- NERC CIP Compliance Considerations
- Lack of resources for a dedicated ICS security team
- Lack of insights into OT-specific threats and how to respond to these events

Challenge: Lack of ICS Visibility & Asset Management

The ability for electric utilities to have in-depth visibility of their ICS environments, know what assets they own, and comprehensively understand asset communications is the prerequisite to effective threat prevention, detection, and response; however, gaining an in-depth understanding for this utility was not reasonable for a 3-person ICS cybersecurity team (expanded from the IT side to the OT side) tasked with manually viewing and tracking over 30,000 assets on its network with large volumes of data and a physical separation of hundreds of miles. Without effective, automated management of these assets, this utility lacked the ability to get an accurate picture of what was occurring in their ICS environments, track down every asset manually, or keep up with a vast, dynamic network.

Solution:

The Dragos Platform's in-depth, automated passive asset discovery capabilities, coupled with unique mapping and zoning abilities, allow this utility's analysts to gain a comprehensive understanding of their assets beyond simply understanding the protocols transmitted and provides them the ability to see their assets represented in an easy-to-categorize map view. Analysts can quickly and automatically organize their different assets by custom zones, as well as view a particular device's history, the last time seen, the protocols used including deep packet inspection of ICS protocols, and create alerts for any new device seen on the network.

©2019 Dragos, Inc.

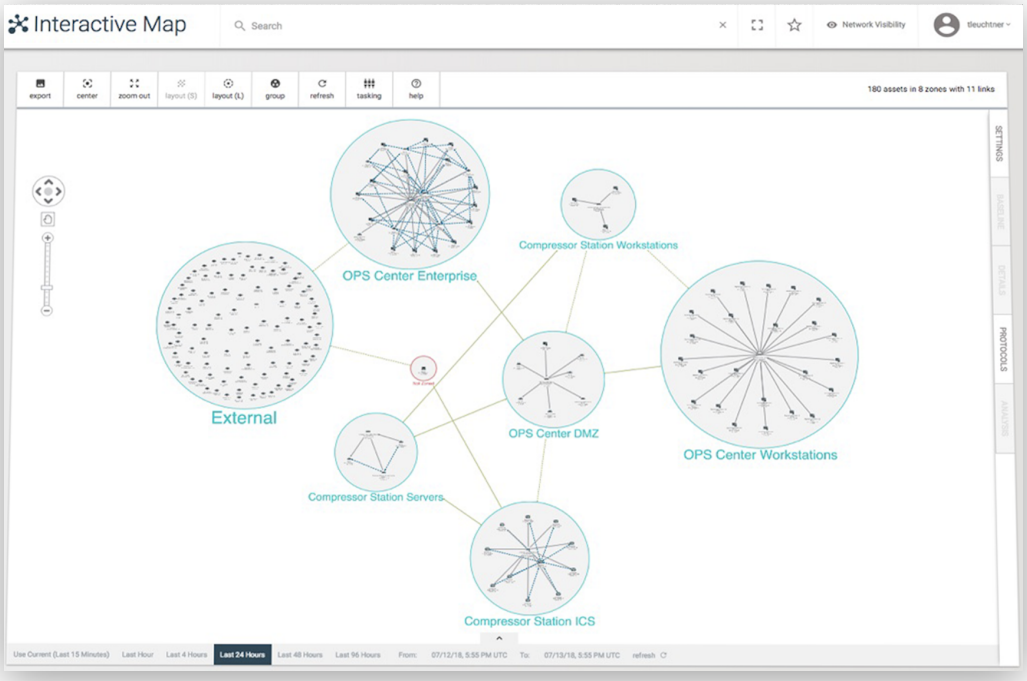


Figure 1: The Dragos Platform Interactive Map

This visual representation of the electric utility's environment provides a dynamic understanding of not only the 30,000 assets in the environment, but how all of those individual assets communicate, their relationships with other assets, and their involvement in the industrial processes in which they function. The Dragos Platform also enables this utility's analysts the ability to view these assets and network communications in a single platform for analysis. Analysts have access to data from multiple sources, including asset identification information, packet captures, logs (System, Event, PLC, RTU), historians, and network traffic, so they can correlate and compile the various data sources in one place–significantly reducing their amount of time searching for data and enabling a multi-data source view of their industrial operations.

To further this utility's asset visibility, the Dragos Platform provides analysts the ability to track asset changes over time and enable historical timelines of each assets' status–which is key for them in determining if changes in their environment are intentional (non-malicious) or unintentional (accidental or malicious). Analysts can create baselines of their environment to compare to later or create complete historical timelines that are dynamic to compare at different points of time, which is especially valuable to support their investigations and incident response.

©2019 Dragos, Inc.

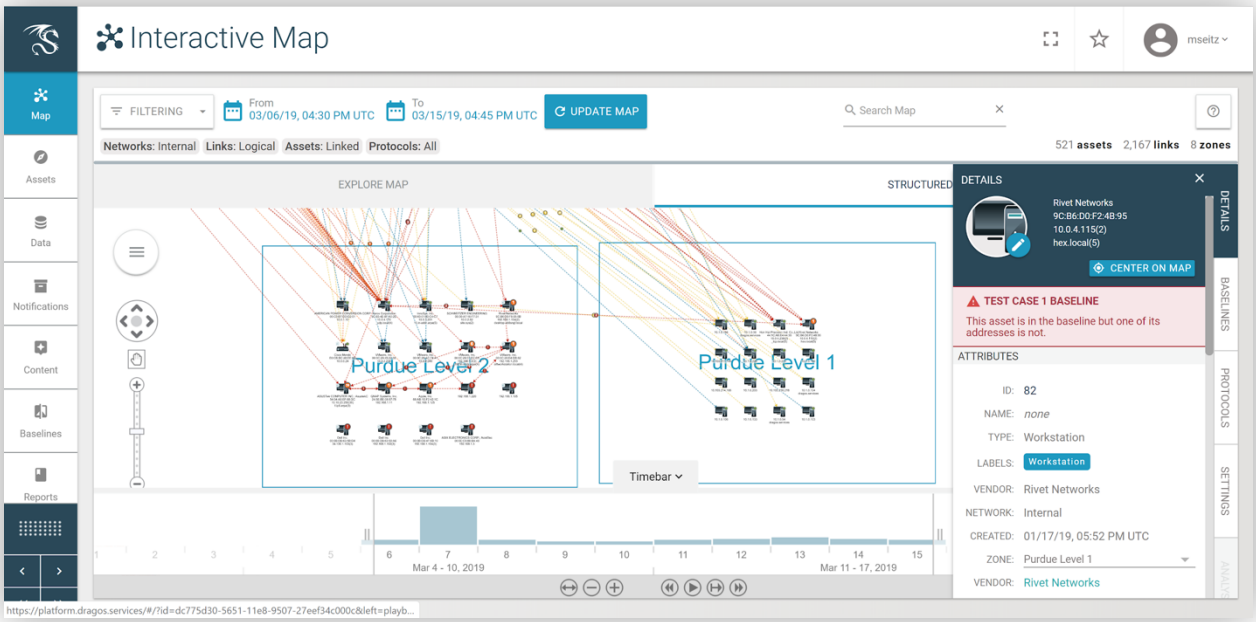


Figure 2: The Dragos Platform Interactive Map with Baseline Display

In addition to more effective threat detection, the Dragos Platform's in-depth asset identification capabilities also provides this utility with:

REDUCED FINANCIAL INCURMENT

Efficient asset identification procedures save analysts' time, thereby, saving money.

EASIER COMPLIANCE

In-depth asset identification helps analysts classify and track information necessary for compliance (such as NERC CIP standards and regulations for electric utilities), including IP addresses, vendor and model of the asset, host name, OS version, and more.

IMPROVED INCIDENT RESPONSE PROCEDURES

Accurate, efficient asset identification helps analysts plan effective incident response strategies by prioritizing assets and budgets and preparing contingency plans to mitigate damage from unexpected malfunctions.

OPTIMIZATION

Effective asset identification allows this utility to allocate resources to provide the greatest protection and resiliency to data, processes, and systems that matter most.

©2019 Dragos, Inc.

Sub-Challenges: NERC CIP & Establishing Trust

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) regulations and standards are also important to consider for electric utilities considering implementing new technology into their environments. NERC CIP requires utilities to comply with standards and requirements covering a variety of critical assets' security as part of an effort to better protect the U.S. electrical grid from both physical and cyber attacks.

This utility was able to deploy the Dragos Platform without NERC CIP compliance issues, because it was designed with security in mind and is capable of being NERC CIP compliant. This means security controls required for compliance, including: user account management, security event monitoring, documented default ports and services, and software patching are all supported natively–avoiding any difficult implementation processes or challenges that would significantly delay deployment, incur financial impacts, or disrupt operations.

It is also important to note that this utility expressed concerns about bringing in an outside team to navigate its ICS environment–which is an honest and understood concern by the Dragos team. Inadvertent denial of service and downtime are often the result of ICS technologies that intrude in environments and cause too much "noise" for local security teams. To initiate a relationship of trust between plant managers, operators, IT/OT managers, and security teams, our team took time to visit this utility onsite, understand their specific challenges, listen to their concerns, and in-depthly understand their environment. Additionally, as the Dragos Platform is passive network monitoring software, this utility achieved in-depth, passive views of their assets without fear of network disruption, downtime, or noise from our team. Ultimately, due to Dragos' relationship with a wide variety of ICS vendors such as Emerson, Schweitzer Engineering Labs, and General Electric, it was a quick process to gain approvals to deploy the system in the ICS.

Challenge: Lack of Resources for a Dedicated ICS Security Team

Many industrial organizations–including this electric utility–face resource and budget constraints, along with an undeniable shortage of experienced ICS practitioners in general. In many cases (or most cases), IT teams are tasked with bridging the gap in OT security and can find themselves spread too thin without the added resources and experience to sufficiently expand to the OT side.

Solution

To combat these challenges, the Dragos Platform empowers this utility's analysts with our team's ICS-specific knowledge, so they can independently function, learn from our practitioners who have decades of hands-on ICS security experience, and rely on our team's experience to supplement where theirs may lack.

Threat behavior analytics, characterized by the Dragos Intelligence team and based on the ICS-specific adversaries they track, are codified into the platform to provide analysts with context-rich alerts and pinpoint malicious activity accurately. Instead

©2019 Dragos, Inc.

of solely anomaly-based detection technologies, the Dragos Platform's threat behavior-based detections provide more effective threat detection and reduce the amount of false positives this utility's analysts receive by providing higher fidelity alerts, rich with context of "why" an alert is being given.

Threat behavior analytics (characterizations of adversary tactics, techniques, and procedures) are not bound to atomic elements like indicators or anomalies; they are constantly tracked and updated by our ICS threat intelligence, characterized into analytics, and fed into the Dragos Platform–so if that specific adversary behavior pattern is recognized, the Dragos Platform will provide this utility's analysts with an accurate, fast notification of the malicious activity. Not only does this help this utility's ICS security team scale with their limited resources, but it provides a high degree of confidence when identifying threats in their environment.

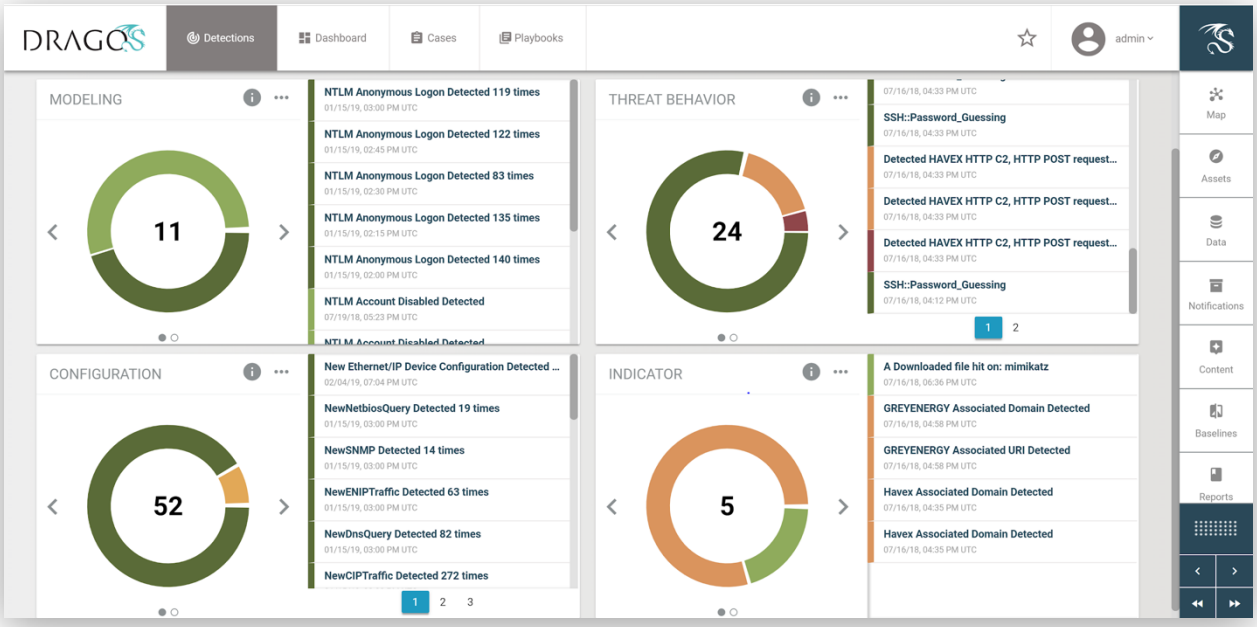


Figure 3: The Dragos Platform Detections Dashboard

To additionally supplement this utility's ICS security team, the Dragos team hosted them in our 5-day ICS training course–specifically tailored to help those making the shift to ICS security– where they learned: how to more effectively assess their industrial environment, as well as various types of industrial environments, through architecture reviews, vulnerability assessments, penetration testing, and red team exercises; how to conduct effective ICS threat hunts, including how to properly plan, create hypotheses, collect and analyze data, and automate lessons post hunt; and how to perform continuous monitoring, investigation, case management, and other SOC-related responsibilities based off real-world attack scenarios.

©2019 Dragos, Inc.

Challenge: Lack of Insights into OT-Specific Threats and How to Respond

The most common challenge this utility faced is one that our team continually observes with industrial organizations throughout the industry: a lack of visibility into the threats specifically targeting their networks and the knowledge of how to respond to them.

Solution

The first step we took to solve these challenges for this utility was providing visibility of the ICS adversaries targeting the ICS industry, specifically electric-facing. The Dragos Threat Intelligence team currently tracks eight ICS activity groups, with four publicly known to specifically target electric utilities: RASPITE, ELECTRUM, COVELLITE, and ALLANITE. Each month, our intelligence team releases private intel reports to this utility via its WorldView subscription, so they not only have visibility of any threats or vulnerabilities specifically facing the electric industry, but they are provided with recommendations to identify and respond to them.

In order to effectively respond to threats if they occur, the Dragos Platform provides this utility's analysts with unique step-by-step investigation playbook inside of a workbench and case management tool to aid their investigations, reduce dwell time, and offer insights from our team as to how to best investigate incidents. Investigation playbooks are custom-authored by our threat operations team and include step-by-step guidance to this utility's analysts to start down the correct (and efficient) path to respond to potential threats. Because our threat operations team has first-hand experience hunting and responding to ICS threats, their guidance not only supplements this utility's team, but helps reduce their time to act and increases effectiveness of their response.

©2019 Dragos, Inc.

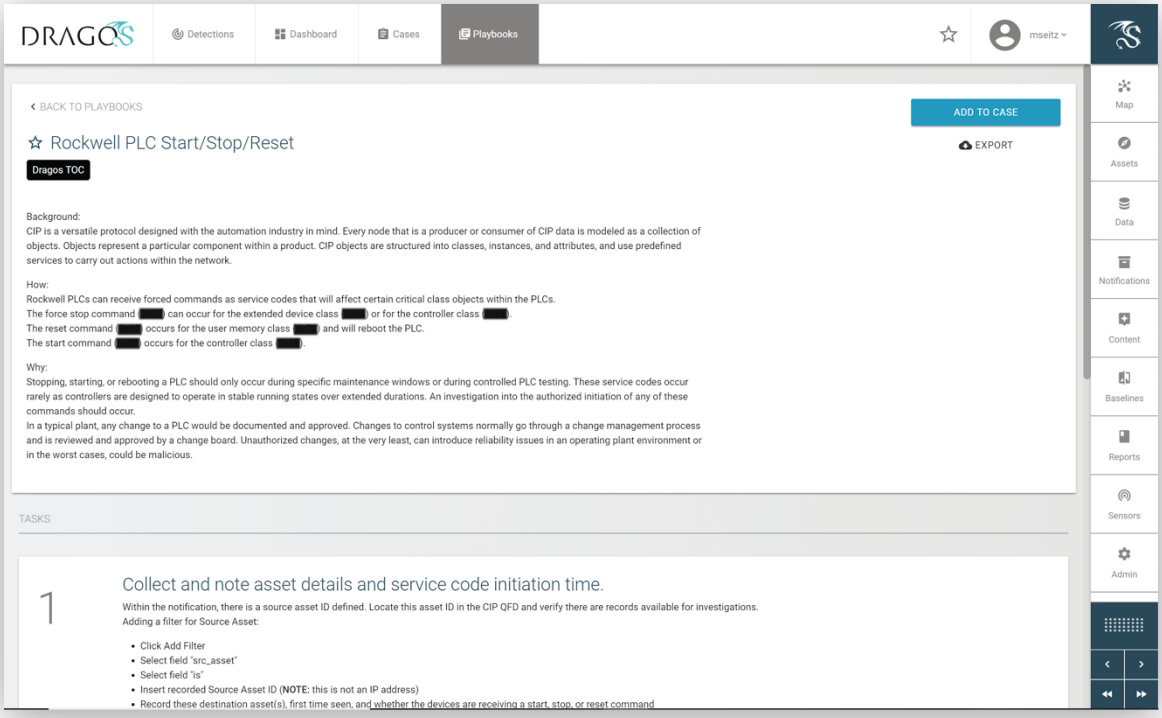


Figure 4: Dragos Platform Investigation Playbook

To streamline this utility's team's investigation processes even further, the Dragos Platform also provides query-focused datasets. Query-focused datasets (QFDs) are pared down datasets that combine disparate data to enable this utility's analysts to prove or disprove a given hypothesis quickly and reduce the overall time they spend triaging suspicious activity. QFDs pair well with threat behavior analytics and playbooks in providing context to alerts or network behavior. When a notification alerts that a given threat behavior occurred on the network, QFDs quickly offer meaning behind the observed behavior. As new playbooks and threat behavior analytics are created by our team, we provide QFDs as further sources of information to enable this utility's analysts to find relevant information quickly.

©2019 Dragos, Inc.

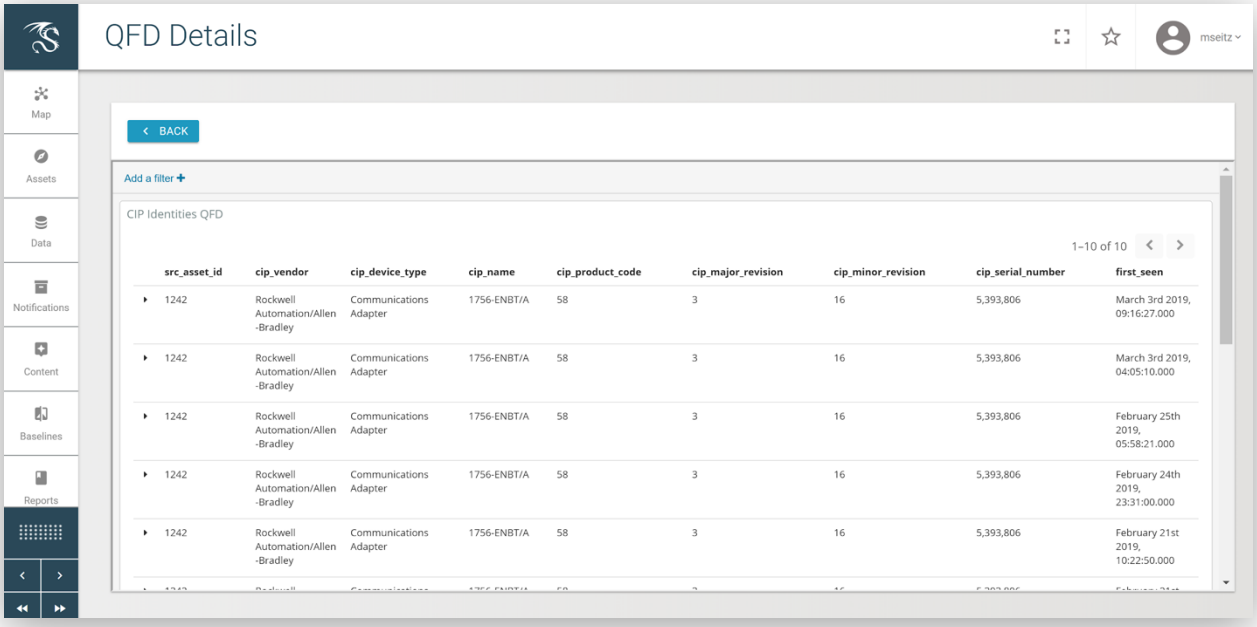


Figure 5: Dragos Platform Query Focused Dataset

Additionally, to support this utility's analysts in achieving a sound investigation and response process, our incident response team is available to deploy onsite to this utility and respond to active incidents or intrusions should its team require assistance. Once deployed, the platform allows the response team to identify, scope, and contain activity occurring in the environment. This is enabled both through network traffic and host-based analysis. During recovery operations, the Dragos Platform also generates visibility to confirm the incident is resolved and that there is not a recurrence. This is not only an opportunity to quickly support utility analysts in stabilizing their networks should they need it, but it is also an opportunity for our team to collaborate with plant managers, operators, and security teams to educate them, help them learn side-saddle, and provide recommendations to avoid future incidents.

Conclusion

This case study examines how the Dragos Industrial Cybersecurity Platform provides comprehensive industrial asset identification, threat detection, and response for an electric utility in the U.S. to successfully combat low visibility of their ICS assets and environments, scale its resources for dedicated ICS security, and gain an in-depth understanding of the threats to their environments and how to respond.

If you would like to learn more about this case study, please contact sales@dragos.com to speak with a Dragos team member.

©2019 Dragos, Inc.