NATURENER & DRAGOS, INC.

Case Study: Protecting Wind Farms Using the Dragos Platform

FOREWORD

This case study reviews NaturEner's adoption of and success with the Dragos Platform, discusses specific challenges faced by renewable energies (specifically wind), and examines how the Dragos platform provides visibility and facilitates triage, detection, and response across NaturEner's network.

Dragos focuses on arming organization with the resources required for comprehensive network security. Threat behavioral analytics and playbooks are deployed and routinely updated, along with a built-in case management system, to help organizations optimize resources and operate as though each had a senior, dedicated network security team.

NaturEner implemented the Dragos platform in July of 2017, which consisted of nodes at each wind farm and a central monitoring node at its corporate headquarters in San Francisco. The Dragos Platform now monitors all wind farm networks and Energy Management System (EMS) networks.

"We immediately saw value as the platform showed us in detail what was running on all of the networks. This was known information on the EMS network, but we had not been doing inventory scans on the wind farm ICS networks."

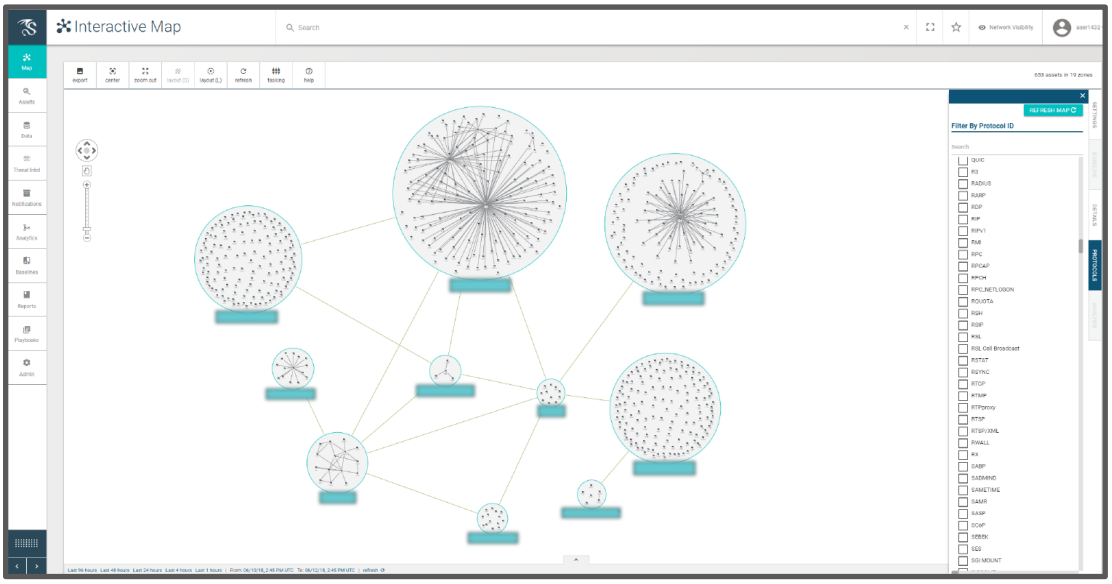

Figure 1: Wind Farm Assets Logically Grouped with Traffic Summary

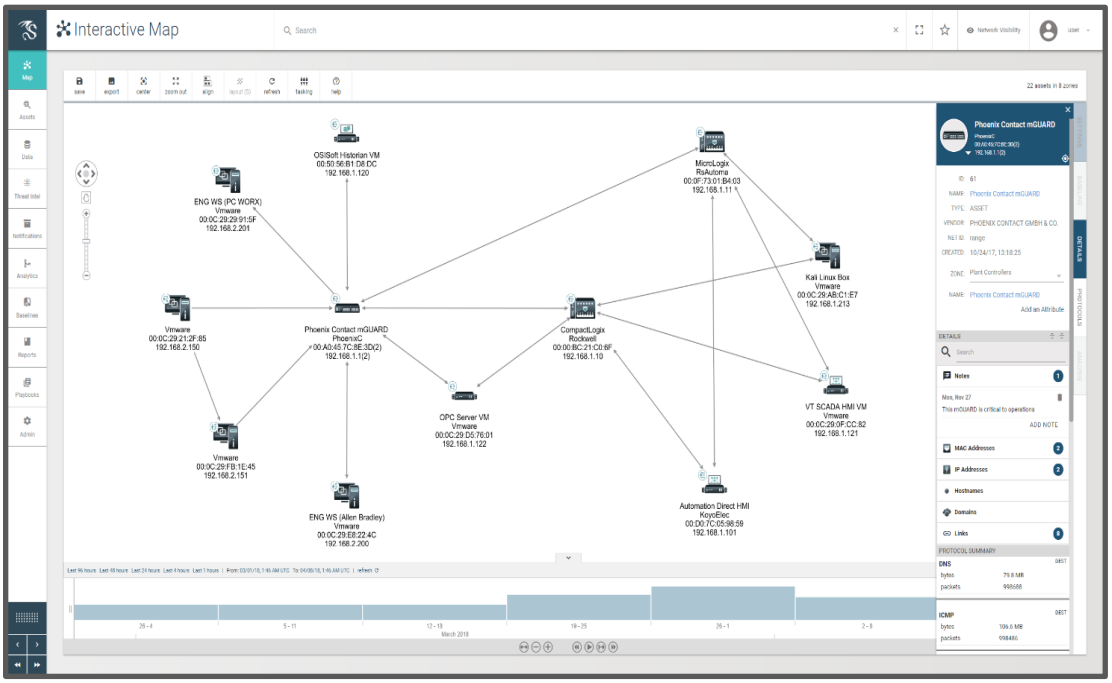

Figure 2: Specific Subnet with Asset and Traffic Details

Challenges and Solutions

Industrial Control System (ICS) networks are unique in topology, design, and workflow. Each ICS sector has specific requirements producing unique security implications. Visibility of the network and host behaviors are critical to identifying what protections are required and detecting intrusions. These challenges are not unique to NaturEner, renewable energy, or even ICS networks and deserve consideration by others looking to improve their security posture.

Shared ICS Challenges

- System and subsystem configuration (patch level, best practices, etc) are restricted by vendor and warranty
- Distributed networks impede ease in central monitoring
- Reliability and safety often take priority over cyber security

Wind-Specific Challenges

- Many individual units to keep up to date (firmware, configurations, etc.), which is challenging and time consuming
- Each unit also acts as a mini substation, introducing additional complexity
- Often no secondary or tertiary monitoring systems for safety shutoffs and monitoring
- Multiple external remote connections are common (turbine vendor, 3rd party services, etc.)

Large Geographical Footprint

NaturEner, like other ICS organizations, has subnets across multiple geographic locations, potentially hundreds of miles from one another. This physical footprint makes continuous monitoring a direct challenge, as data needs centralized aggregation for analysis.

NaturEner deployed the Dragos Platform to each US subnet, including all EMS, wind farm (SCADA), and production networks. Traffic from each subnet was aggregated to a centralized data store. This data store facilitates data correlation for analysis between sites, as well as triage and incident response, if the Dragos Platform detects a compromise. NaturEner analysts can now review traffic across the NaturEner ICS and business enterprises through a single platform.

Sparse Monitoring Timeframes

Some subnets do not have sustained connections and may only generate network traffic periodically. Triage and analysis of these networks is time-consuming, due to collection of samples over a longer period of time.

This challenge is mitigated through continuous monitoring at strategic capture points across NaturEner's domain. While comparing baselines can be an effective way to isolate changes within the environment, there is a risk of the baseline including existing adversary communications and data.

The Dragos Platform enables the analyst to combine changes to baseline with threat behavior analytics, ensuring that even "low and slow" attacks are detected.

Management of Vendor Devices

Vendor devices, specifically those used for wind assets, are used to monitor and perform actions (such as Turbine resets). These devices interact with company assets in the ICS network as a part of their warranty services. This workflow presents two significant challenges:

1. The endpoints are poorly managed for user authentication and verification (generic logins, repudiation or non-attributable actions by individuals who have access). This vulnerability results in the potential for legitimate functions to be abused by adversaries if those systems are compromised. If authentication is not a valid verification of approval, differentiation between appropriate vs. adversarial actions is convoluted and requires several additional data points to investigate.

2. These same endpoints extend to or straddle many other customer sites and assets with unknown levels of security, which significantly expands the attack surface.

NaturEner's continued network operation and warranties require these vendor devices. Improvements to the authentication of users or processes against the devices require external vendor support. The Dragos Platform passively monitors device communications across the network. This traffic can be organized into custom network zones, as defined by each organization.

"We've been able to track who is talking to whom over what ports, and most importantly, see traffic from our warranty vendor's various sites and systems."

Vendor Access

In some cases, vendors have direct access to their equipment, but the ICS organization may not monitor these communications.

This lack of monitoring is not an oversight or immaturity, but rather a requirement from the vendor and part of a contractual agreement. While these are additional ingress points to the ICS network, organizations may not be able to support them with the same security controls or manage dedicated switches and firewalls. The Dragos Platform monitors three of NaturEner's US network segments' ingress and egress points of presence, as well as core traffic. Through the platform, NaturEner was able to reveal direct, vendor-to-device communications not previously monitored. Analysts can now review details about the communications (frequency, protocols, and device pivoting) for signs of malicious activity.

Asset Inventory

Because networks grow with the business, it is not uncommon to lose awareness of asset inventory, subnet behaviors, or how data moves throughout the network. In these situations, it is very arduous to identify and catalog assets, traffic load, and the flow of information.

Asset management is handled within the Dragos Platform by parsing traffic for unique source and destination information. All devices can then be graphically represented in a mapped view and organized based on custom zones, so analysts can view a device's history, last time seen, protocols used, and create alerts for any new device seen on the network.

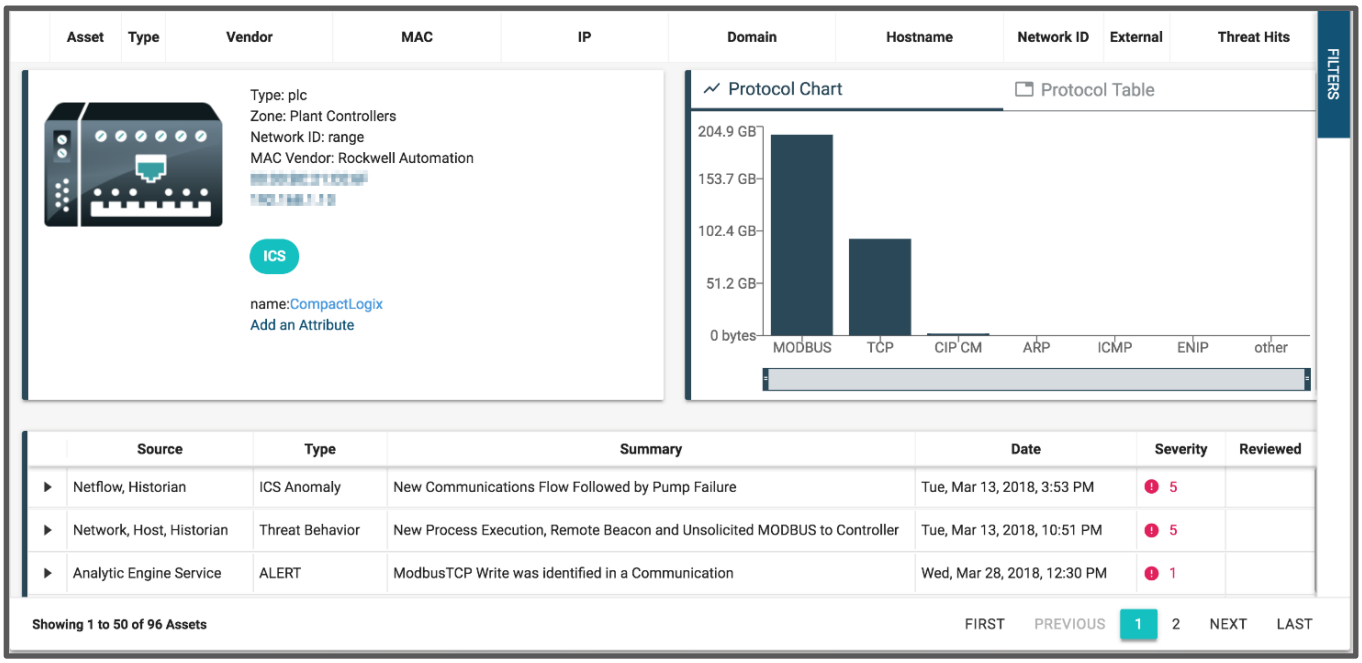

Figure 3: PLC Asset Details

Anomaly Detections Alone are Ineffective

The entire network supporting a wind farm is constantly spinning up and down based on natural elements, so everything appears as an anomaly. Security devices monitor turbine speeds and apply braking as necessary. These events can be tracked through device communications but cannot be accurately predicted or parsed for anomalies without simultaneously considering natural, environmental variables. For instance, if an avian watch tower operator identified a protected species of bird approaching a wind turbine, she may use a secure wireless device to remotely disable that turbine. This network event would appear as an anomaly in most other toolsets, but it is actually a part of managing and curtailing the plant based off of environmental considerations.

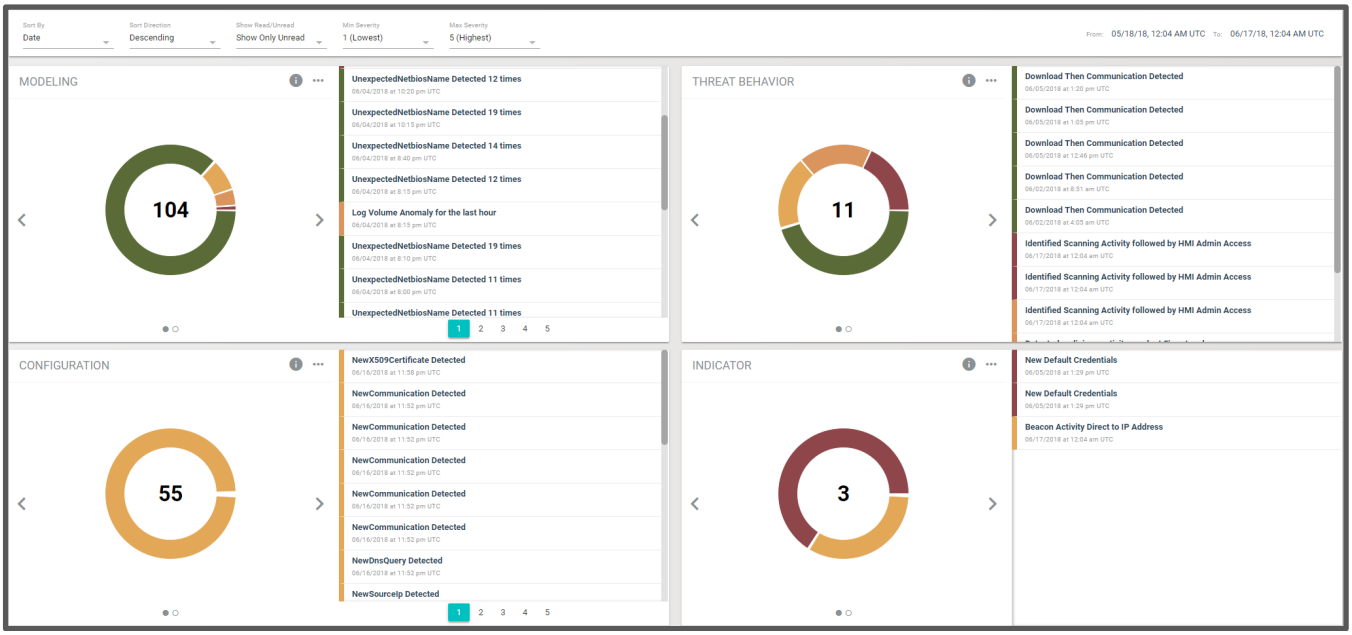

Figure 4: Detections Dashboard

While Dragos can detect on anomalies or signature matching, our primary detection is based on the tradecraft used by known threat actors. The Dragos Platform applies custom analytics that watch for a series of events, rather than a single atomic value. These are considered Threat Behavioral Analytics (TBA)[1]. As an example, an analytic may aggregate detections of a machine reaching out to the internet, downloading a binary file, or remotely shutting down a turbine within some time window. Additional verifications may also be considered, such as users logged into the box or source/content of the binary file.

Processing all available data and providing context to alerts prevents analyst fatigue and allows resources to be directed to activity of concern, given the specific environment.

Limited Resources, Vast Network

Every organization faces resource constraints. Staffing is the most critical component of protecting any network; however, the market for experienced ICS cybersecurity professionals is low. Some organizations cannot fund dedicated security staff, so the roles are split between operations. For energy providers, customer charge rates can be limited, due to regulatory law, so revenue is not completely based on the open market. The resulting mission is to do more with less.

[1] Signatures (IPs, domains, hashes) have proven ineffective for the detection of threats. It is trivial for adversaries to manipulate these values to avoid detection. It is much more difficult for adversaries to deviate from their tradecraft. This is where behavioral analytics play an important role. Dragos' intelligence and Threat Operations Center (TOC) teams are leading the industry in ICS threat research and implementing this knowledge into the platform to facilitate detection. These content packs are regularly updated and based on real-world case studies. More information can be found here.

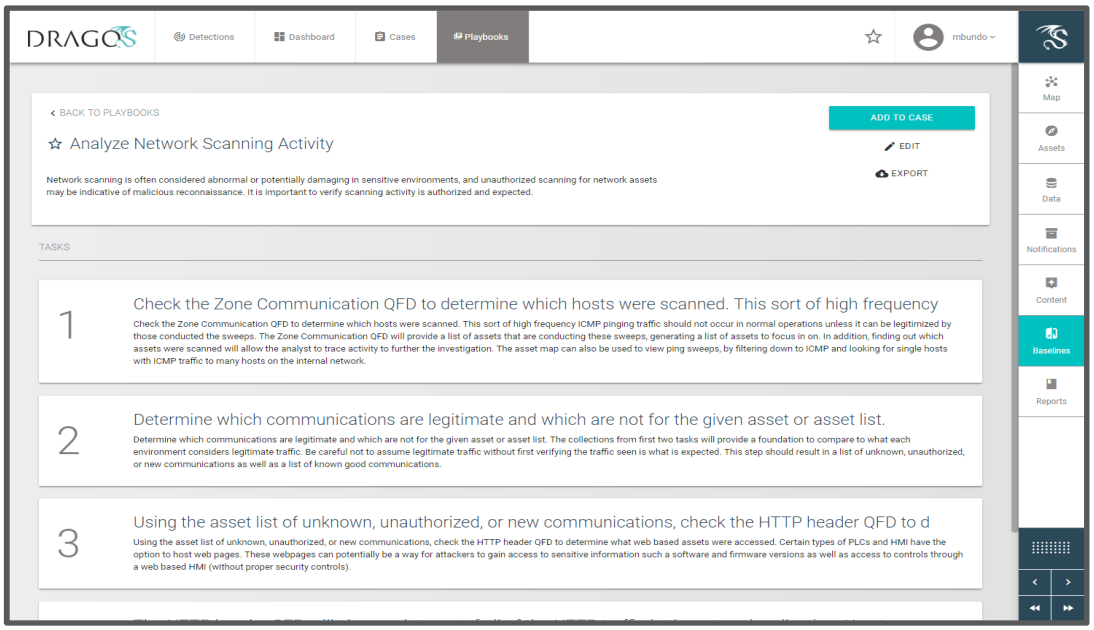

Figure 5: Sample Playbook in Case Management System

Through constant and passive monitoring, the Dragos Platform brings visibility of assets and network communications to a single platform for analysis. Additionally, the Dragos Platform offers playbooks[2] and case management, where analyst can leverage industry experience and notes can be tracked with evidentiary files. The goal is a single pane of glass for data analysis, so responders can perform their tasks without bouncing between multiple tools or gather data from multiple sources.

Conclusion

NaturEner operates 399MW of wind power for North America and is expanding into Alberta, Canada. As a leader in sustainable, compliant, renewable energy, NaturEner is also focused on protecting its assets and operations. Implementation of the Dragos Platform allows NaturEner to monitor for adversaries, optimize internal resources, and assume a proactive security program. NaturEner can continue to focus on energy generation and delivery, while being confident its infrastructure is protected.

"Over time, as we've monitored the infrastructure and learned how our devices are talking, we have a better sense of what is happening in our network. Girded with that knowledge and the Dragos platform tool suite, we hunt for issues, intrusions and improperly configured devices, thereby increasing our security footprint across the organization."

[2] Dragos is developing hunting playbooks that are specifically focused on active campaign and group TTPs. These playbooks describe specific queries and analysis techniques that help junior analysts hunt and identify traffic indicative of an adversary. Dragos' industry veterans are also codifying their knowledge into response playbooks. These do not take the place of traditional incident response (IR), but facilitate it with incident handling and response. They are essentially the "What would Dragos do?" steps to help an analyst perform triage. Case management further supports IR by capturing data points and investigative notes during an investigation as does the ability to request full packet captures. More information can be found here.