Achieving OT Network Visibility and Detective Controls in a NERC CIP World

Tim Conway

SANS

Analyst Program

Overview

Achieving OT Network Visibility and Detective Controls in a NERC CIP World

Written by **Tim Conway**

June 2021

DRAGOS

Living in a Regulated Industry

Cybersecurity standards are in a continuous state of evolution: Requirements are written and implemented, and compliance programs are maintained. Over time, events occur that provide new insights to emerging operational risks, and organizations look to new innovative technologies to help manage the risks to their businesses. This dynamic landscape creates challenges for asset owners and operators, regulators, and solutions providers, all of whom are working hard to adhere to internally developed standards while simultaneously looking ahead to a time when the standards may need to mature. This constant push and pull poses a considerable risk of stranded capital investment if the standards are always in a state of flux. Of equal risk is the technology debt and regulatory lag that prevent effective defensive approaches if the standards have no room for innovation. The urgent need to address increasing cyber threats is the driving force behind the Biden Administration's efforts to protect US critical infrastructure and specifically the Department of Energy's 100-day plan to enhance the cybersecurity of electric utility Industrial Control Systems (ICS).

Attempts to achieve balance between compliance and security can easily be seen within many registered entities facing the difficult task of building and maintaining compliance programs for the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards. As these entities consider the widespread impacts of NERC CIP to their people, processes, and technology, they have implemented various projects to meet the changing standards. As a result, they've come realize that the truly hard work is the process of maintaining an effective compliance program.

Recent Compliance Monitoring and Enforcement Program (CMEP) efforts from NERC have resulted in "Practice Guides" to help provide compliance guidance to auditors across the NERC regions. These practice guides were developed with the expectation that many entities would likely pursue additional Operational Technology (OT) detection and monitoring capabilities throughout CIP-impacted facilities as a part of the 100-day plan. Whereas the "ERO Enterprise CMEP Practice Guide on Network Monitoring Sensors, Centralized Collectors, and Information Sharing" document[1] provides guidance to auditors on device categorization and areas to consider, this paper will focus on what the entity needs to consider when evaluating a technology to incorporate within its CIP program. The CMEP Practice Guide provides reference to general implementations of technical solutions for auditors to consider as they review many vendor implementations. Because an organization has to pick one, however, this paper will walk through what that looks like if it selects Dragos, a leading solution provider in this space.

[1] "ERO Enterprise CMEP Practice Guide on Network Monitoring Sensors, Centralized Collectors, and Information Sharing," June 4, 2021, www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf

Regardless of where an organization is in this standards continuum, there are often multiple stakeholder views that leadership needs to consider when deciding which new technology solutions need to be integrated into a new or existing CIP program. Figure 1 represents the typical battle within most organizations.

These perspectives and many others are at play with every technology decision across an organization's CIP programs on a daily basis. For these reasons, consider all positions when making a decision about a technology solution that will be integrated into a CIP program.

This paper examines one of the more common technologies being pursued currently across the CIP universe of electric utilities: OT network visibility and detection solutions.

Note: NERC uses specific terminology that has defined meaning in the context of its protocols and rules. Throughout this paper we have chosen to preserve NERC's terminology and associated capitalization. For more information, see NERC's Glossary.[2]

Figure 1. Typical Perspectives About New Technology Deployments

[2] "Glossary of Terms Used in NERC Reliability Standards," www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

Figure 2. Process of Pursuing Technologies Integrated into a CIP Program Solution

Considering a New Solution: The CIP Gauntlet

Figure 2 presents some of the reasons why organizations might pursue technical solutions. Regardless of the reason, however, there is an evolutionary process that an organization goes through when evaluating a CIP solution. Here are the typical stages:

1. Admit you have a problem.
2. Determine whether the solution creates more problems than it solves.
3. Decide how the solution can help you manage the existing problems.
4. Discern whether the solution can help you address future problems.
5. Determine whether the solution provider understands that you have a problem.

As we walk through these five stages of CIP evolution, we will also look at the Dragos Platform as one of the leading products in the ICS network visibility and detection space. The platform is very likely on the short list of product offerings to review and consider for entities managing NERC CIP programs. Specifically, we will look at the Dragos Platform V1.8 and the on-premises deployment approach including the Dragos SiteStore and distributed Dragos Sensors.

Admitting There Is a Problem Is the Hardest Part

Building programs to achieve compliance is the easiest task on an entity's to-do list, but they typically require the greatest capital investment. During this project phase, the organization will determine what the requirement language means, select an approach to achieve the intent of the interpreted requirement language, develop policies and procedures on how to operationalize the program, and then implement the technical solutions and procedural controls. As CIP history has rolled forward, entities have learned that they may have achieved initial compliance, but it was with high levels of reliance on one or more of the following:

- Spreadsheets
- Procedural controls
- Physical controls
- Calendar alerts for periodic performance of actions
- Work management ticketing systems for performance reminders
- Scripts to copy logs for retention
- Events that highlighted gaps in a CIP program
- Large amounts of human heroics

Recognizing the need for an effective program that goes beyond initial compliance is the first step.

Understanding the problem space here can be a challenge and might be counterintuitive—the stronger your program and your solutions, the more violations you will discover. If you do not know what a compliance violation is and do not run an active program, then you will likely not find any violations until an audit team does. Similarly, if you are not actively monitoring your operational networks and implementing detective controls, then you will likely not find any threats until a potential system-impacting event occurs. NERC CIP eventually brings entities to the following realization: "We either need to run an effective CIP program now or do it later and face a fine. Either way, we need to get there."

As organizations recognize the problems within their CIP programs and consider pursuing technical solutions to integrate into their CIP programs, they progress to the next stage: "Will this solution make my problems worse?"

Will the Solution Help?

When considering a technical solution to enhance a NERC CIP program, assess how the solution will fit within that program. The solution must first meet the compliance program's requirements. To highlight this review process, let's look at the Dragos Platform device's SiteStore and Sensors.

Ideally, while all of the standards integrate with each other within an effective CIP program, there are some standards that pertain to devices more specifically.[3] In evaluating the Dragos Platform Sensors and SiteStore components, this paper focuses on the compliance requirements of the following standards specifically:

- CIP-007, including some elements of CIP-004
- CIP-009
- CIP-010
- CIP-011

When evaluating a particular solution to be utilized in a CIP program, individual components will pass through a series of decision gates. Some of those decision gates that apply to OT network visibility tools include:

- Why is it subject to CIP?
  - What does it do? (In the case of OT network visibility tools, they are typically used to satisfy specific CIP requirements across numerous standards.)
  - Where is it? (In the case of OT network visibility tools, they typically have sensors or collectors within CIP-identified Electronic Security Perimeter [ESP] network segments and aggregators outside of the CIP ESP network segments.)
  - What data does it contain? (In the case of OT network visibility tools, they typically have sensitive system information, logs, and event data that needs to be protected.)
- Is it a Cyber Asset?[4]
  - What are the programmable electronic devices, including the hardware, software, and data in those devices? (In the case of the Dragos Platform, Dragos Sensor and SiteStore certainly satisfy the Cyber Asset definition.)
- Is it a Bulk Electric System (BES) Cyber Asset?
  - A BES Cyber Asset is one that, if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, misoperation, or nonoperation, adversely impact one or more facilities, systems, or pieces of equipment, which, if destroyed, degraded, or otherwise rendered unavailable when needed, would affect the reliable operation of the BES. (In the case of the Dragos Platform, there are no associated real-time reliability tasks being performed by the components that would affect the BES within 15 minutes. An entity needs to evaluate its CIP-002-documented approach for misuse considerations with each Cyber Asset to ensure it has established "misuse" consideration boundaries.)

---

[3] www.nerc.net/standardsreports/standardssummary.aspx

[4] www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

- Where is it?
  - What is the Impact Rating[5] of the facility where the solution is implemented? (In the case of the Dragos Platform, the solution will likely be found in High Impact Control Centers and in Medium Impact Control Centers, Generating Stations, and Transmission substations. The solution elements may also be found in Low Impact Control Centers, Generating Stations, and Transmission substations, but the CIP requirements for these Low Impact facilities are not as significant or direct as with the high and medium facilities.)
- Is it inside an ESP?
  - If a Cyber Asset is connected using a routable protocol within or on an ESP, then that device should be treated as a Protected Cyber Asset (PCA) within the same impact rating as the ESP it is in. (In the case of the Dragos Platform, the sensors within the ESP would be treated as High or Medium PCAs, depending on the impact rating of the facility.)
- What does it do for CIP?
  - Cyber Assets that perform electronic access control or electronic access monitoring of the ESP(s) or BES Cyber Systems are treated as Electronic Access Control or Monitoring Systems (EACMS). (In the case of the Dragos Platform, the SiteStore receiving electronic access monitoring of BES Cyber Systems would be treated as an EACMS.)

With an understanding of why the various elements are subject to CIP—and specifically how they are subject to CIP based on the various Standards Requirements[6] applicability tables—an entity can now begin to identify which requirements must be satisfied by a particular solution. Let's look at the requirements that apply to the Dragos Platform and the capabilities that exist to integrate the solution into an entity's CIP program.

Does the System Purchased for Compliance Comply?

Prior to highlighting each Standard and the applicable Requirements, it is important to understand that no solution is inherently "compliant." The Dragos Platform and associated Dragos Sensors and SiteStore can be configured to satisfy compliance requirements, which is an important differentiator, because not all solutions on the market are configurable. To demonstrate ongoing compliance, your organization needs to provide performance evidence that it has implemented a program to sustain compliance with the requirements over the life of the assets. This isn't something you buy—it is something you do. This paper covers the standards with specific applicability to Dragos Platform assets.

CIP-007

CIP-007 is the Systems Security Management Standard and provides the requirements that need to be satisfied by applicable systems within a CIP program. There are 5 parent-level requirements and more than 20 subrequirements within CIP-007. Table 1 on the next page shows the applicable requirements and associated impact rating specifics.

---

[5] "CIP-002-5.1a—Cyber Security—BES Cyber System Categorization," www.nerc.com/pa/Stand/Reliability%20Standards/CIP-002-5.1a.pdf

[6] "Mandatory Standards Subject to Enforcement," www.nerc.net/standardsreports/standardssummary.aspx

Table 1. CIP-007 Applicable Requirements and Associated Impact Ratings

Requirement	Description	Dragos Sensor	Dragos SiteStore
R1.1, R1.2	Enable only required logical network-accessible ports, prevent against unauthorized access to physical ports.	Although Dragos Sensor and SiteStore contain a number of container-to-container communications networks, as well as associated ports, the system can lock down network-accessible logic ports through a local iptables fw rule set and interface configurations that limit the network-accessible ports to only those required for communications with the endpoints and SiteStore. In addition, the sensor device can be configured to disable unused physical ports through logical configurations.	The SiteStore is typically categorized as an EACMS based on the logical implementation and is not applicable to R1.2. The logical network ports would be configured in a similar manner as the Dragos Sensor.
R2.1, 2.2, 2.3, 2.4	Patch sources for CIP-010 baseline-related items must be identified and a patch management process for tracking, evaluating, and installing applicable security-related patches on a 35-day calendar cycle shall be implemented. Security patches will be evaluated for applicability and then in the next 35-day cycle, they will be applied, mitigated, or added to an existing mitigation plan.	For both the Dragos Sensor devices and the SiteStore devices, CIP entities would list Dragos as their patch source and would verify within a rolling 35-day calendar cycle if any applicable security patches have been released. Security-related patches do not include bug fixes, feature updates, or knowledge packs and would only apply to specific security-related patches. If an applicable security-related patch was available, then the entity would need to identify that fact during its first patch assessment 35-day window and move the applicable patch into the next 35-day window to apply, mitigate, or update an existing mitigation plan. Maintaining access to ongoing security-related patches requires an active Dragos support agreement. For customer-specific software applications intentionally installed on the Dragos Platform solutions, the entity would need to include the intentionally installed software in the entity CIP-010 baseline and identify a unique patch source.	The SiteStore approach is the same as the Dragos Sensor approach.
R3.1, 3.2, 3.3	Deploy methods to deter, detect, or prevent malicious code and implement a process for signature or pattern updates.	For both the Dragos Sensor devices and the SiteStore devices, Dragos has implemented controls to prevent malicious code through firmware validation and utilizes Clam AV on the devices. Entities need to follow their established signature update procedures to update the detections in Clam AV.	The SiteStore approach is the same as the Dragos Sensor approach.
R4.1, 4.1.1, 4.1.2, 4.1.3, 4.2, 4.2.1, 4.2.2, 4.3, 4.4	Perform event logging, including successful logins, failed logins, failed access attempts, and detected malicious code. Alerts must be generated for event logging failure and detected malicious code. Logged events shall be retained for 90 days and for High-Impact facilities, a summary of the logs will be reviewed every 15 days.	The Dragos Sensor and SiteStore can generate logs for successful logins, failed logins, failed access attempts, and detected malicious code, sending those to the SiteStore for log retention and alerting if malicious code is detected. The capability to alert on failure of logging can be established based on communication loss to the SiteStore. Log retention is a requirement satisfied on the SiteStore storage configuration. Log review is a procedural task within a CIP program. In addition, the Dragos Sensor and SiteStore can be configured to send logs to a variety of other third-party SIEM solutions or ingest logs from other solutions.	The unique requirement applicability of an alert that needs to be generated for a failure in event logging that would be visible in the alerting system creates an odd circular requirement for an alerting system. This requirement would typically be satisfied by the observable loss of the alerting system, which in this case is the SiteStore, where the logging and alerts of logging failure would appear.
R5.1, 5.2, 5.3, 5.4, 5.5, 5.5.1, 5.5.2, 5.6, 5.7	Enforce interactive user authentication, enforce password complexity and length, require password changes every 15 months, and limit unsuccessful authentication attempts or alert on an exceeded threshold of unsuccessful attempts. All default and shared accounts must be inventoried. Identify individuals who have authorized access to those accounts and change the known default account passwords.	For interactive user accounts, the Dragos Sensor and SiteStore can support local accounts and connectivity to directory-based systems where the R5 requirements can be easily achieved (see Figure 3 on the next page). For default user accounts, any problems are typically resolved during initial deployment with the Dragos service team. During a Dragos Sensor or SiteStore deployment, the default accounts can be inventoried and passwords can be altered through a series of scripts and commands that the deployment team can walk personnel through. The entity can then establish new passwords and determine who will have access to them.	While everything that was referenced for the Dragos Sensor applies to the SiteStore, in the CIP-004 Requirement 5.4, there is a requirement for default password changes based on a triggering event. Because individuals with access to the default account passwords leave the organization voluntarily or through termination, the entity must change the passwords within 30 days for EACMS devices associated with Control Centers. Although the SiteStore is typically categorized as an EACMS and a sensor is a PCA due to its location in the ESP, it would be wise to treat the sensor to the same change requirement due to its role in the EACMS monitoring function. The challenge for entities is maintaining the change requirements over the life of the asset and requires access to Dragos support for response within the appropriate timeframe.

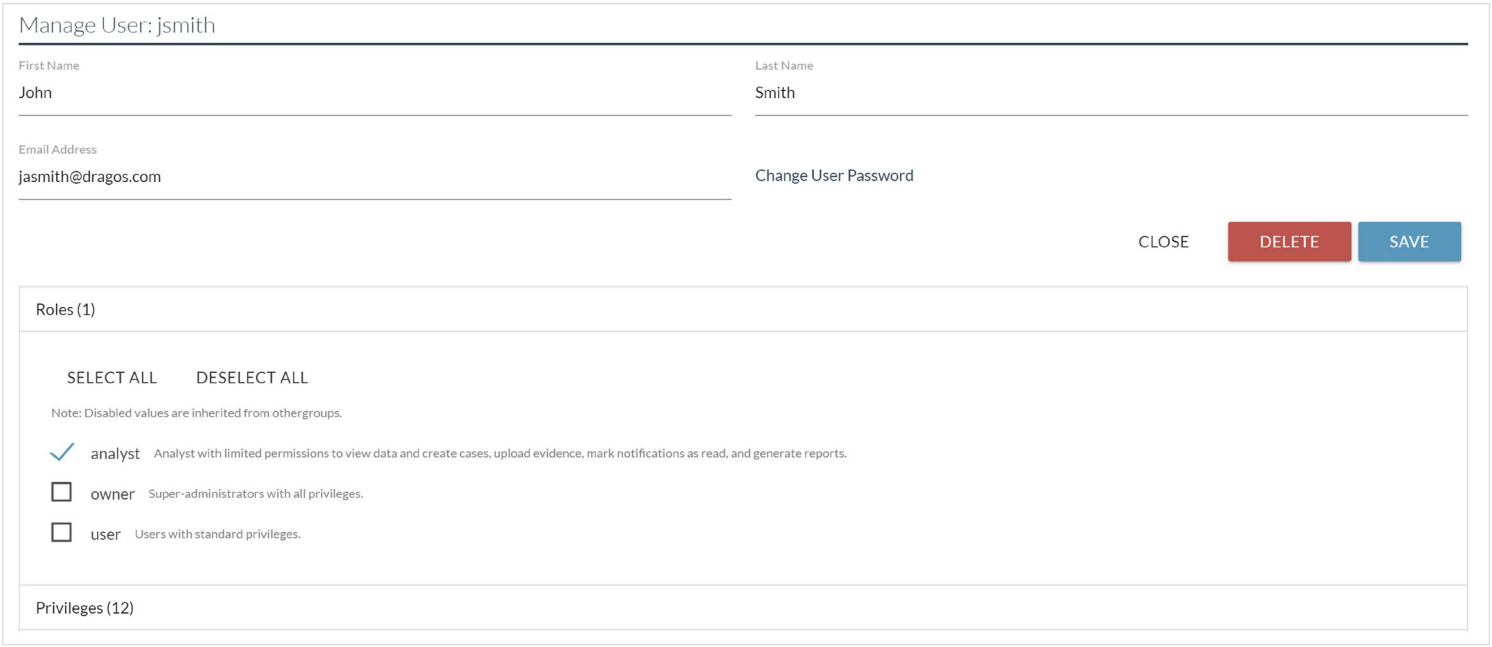

Figure 3. User Role Management on the Dragos Platform

CIP-009

CIP-009 is the standard that addresses recovery plans for BES Cyber Systems and contains a number of requirements that apply to the Dragos SiteStore as an EACMS but not to the Dragos Sensors as a PCA. As mentioned earlier, however, it would be wise to configure the Sensors to comply with the applicable EACMS applicable requirements, due to its role in the monitoring function.

Much of CIP-009 Requirement 1 is looking for recovery plans, identification of individual roles and responsibilities, processes to back up information required to recover the function, verification of the backups, and methods to preserve forensics data from the device if there has been an identified Cyber Security Incident. In the case of the Dragos Platform assets, entities will need to develop not only the processes used to back up the system configuration from the Dragos Sensor and the SiteStore, but also a process to test the recovery of the system build and configuration and methods to perform a backup of all system data for use in analysis after the fact, but before a system is recovered. Dragos provides a series of scripts to perform these backup and recovery tasks, as well as platform backup capabilities to export the configurations in use (see Figure 4).

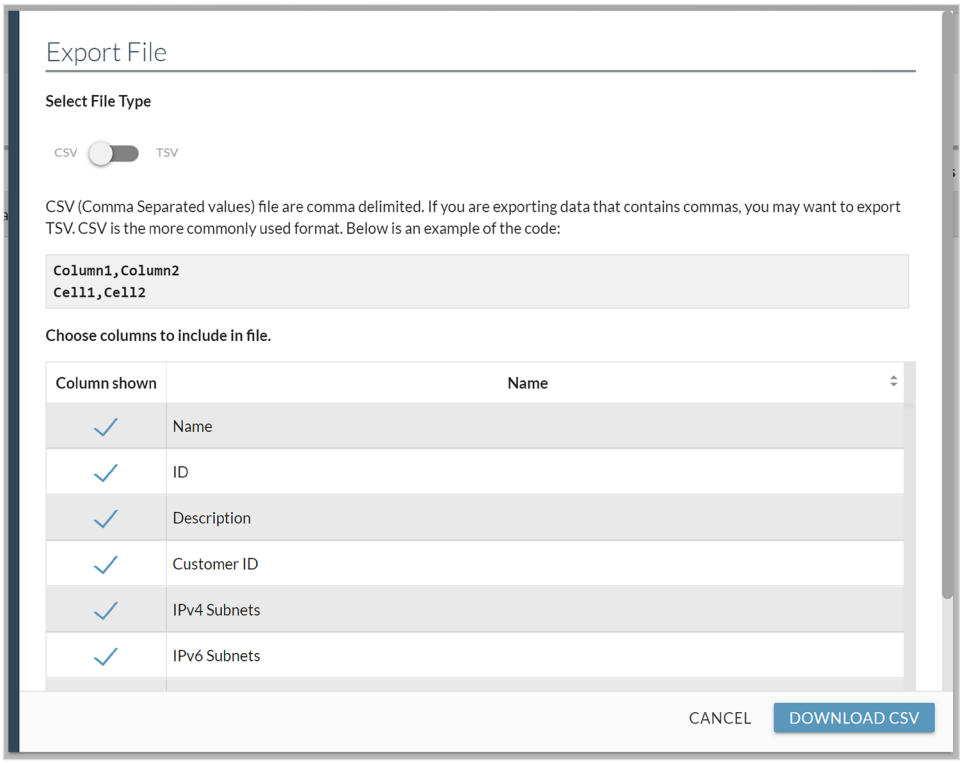

Figure 4. Back Up (Export) Configuration on the Dragos Platform

The other CIP-009 requirements are more programmatic, with associated performance periods and evidence retention demonstrating testing, validation, and plan reviews.

CIP-010

CIP-010 is the standard that addresses Configuration Change Management and Vulnerability Assessments for BES Cyber Systems and other applicable systems. The complicated standard has some unique considerations with regard to its applicability to the Dragos Platform. Table 2 presents the specifics.

Table 2. CIP-010 Applicable Requirements and Associated Impact Rating Specifics

Requirement	Description	Dragos Sensor	Dragos SiteStore
R1.1, 1.1.1, 1.1.2, 1.1.3, 1.1.4, 1.1.5	Document the baseline configuration that includes the operating system, intentionally installed software, custom software, logical network accessible ports, and security patches applied.	The Dragos Sensor and SiteStore operating system in the V1.8 reviewed platform is CentOS. However, due to the level of customization in place now and in the coming version 2.0, it is safer to consider the OS as a customized Linux implementation created by Dragos because it contains numerous packages, dockers, scripting language processors, custom applications, associated security patches, and configuration files resulting in the network-accessible logical network ports. During system deployment, the Dragos support team can run a series of scripts to generate an as-built system baseline.	The SiteStore approach is the same as the Dragos Sensor approach.
R1.2, 1.3, 1.4, 1.4.1, 1.4.2, 1.4.3	The remaining subrequirements within Requirement 1 are programmatic in nature, pertaining to authorization of changes, updating baseline, ensuring security controls have not been impacted, and documenting the verifications. R1.5 and 1.6 do not apply.	Programmatic inclusion is in process over the life of the Dragos Sensor and SiteStore.	The SiteStore approach is the same as the Dragos Sensor approach.
R2.1	The programmatic process of monitoring for changes to the baseline is covered here.	Programmatic inclusion is in process over the life of the Dragos Sensor and SiteStore.	The SiteStore approach is the same as the Dragos Sensor approach.
R3.1, 3.3, 3.4	Every 15 months, perform a paper or active vulnerability assessment prior to adding a new, applicable Cyber Asset. For Control Center associated systems, perform an active vulnerability assessment. For all assessments, document the results and remediation plans. R3.2 is not applicable.	Programmatic inclusion is in process over the life of the Dragos Sensor and SiteStore. The Dragos product team is developing remediation plans or mitigation plans.	The SiteStore approach is the same as the Dragos Sensor approach.
R4	Programmatic protection requirements cover Transient Cyber Assets (TCA) and Removable Media (RM).	Programmatic inclusion is in process for the use of TCAs or RM with the Sensor or SiteStore assets over the life of the Dragos Platform.	The SiteStore approach is the same as the Dragos Sensor approach.

CIP-011

CIP-011 is the standard that addresses information protection and is the last standard for which this paper defines the unique applicability considerations to the Dragos Platform. The first requirement in CIP-011 addresses the programmatic need for a method to identify BES Cyber System Information (BES CSI) that includes information about the BES Cyber System that could be used to gain unauthorized access or pose a security threat to the BES Cyber System. Almost more important is determining what is not BES CSI, meaning the information does not include individual pieces of information that could be used to gain unauthorized access to BES Cyber Systems, such as, but not limited to, device names, individual IP addresses without context, ESP names, or policy statements.

Considering these definitions and additional information about BES CSI, it is safe to assume that the contextual logs, alerts, indicators, and security event-related information from BES Cyber Systems that is stored and processed in the sensors and SiteStore would be treated as BES CSI. Therefore, additional access control requirements of CIP-004 apply to users of the Dragos Platform in relation to granting access, reviewing access records, and removing access in line with the overall CIP-004 program.

In addition, the Dragos Sensor and SiteStore are subject to CIP-011 Requirement 2 for data destruction or sanitization prior to disposal or reuse.

The standards review element of product selection is one of the more important steps in evaluating a solution for appropriate fit within a CIP-regulated environment. The Dragos Platform, consisting of associated sensors and SiteStore devices, is absolutely capable of meeting the compliance requirements during initial build and implementation with routine deployment support from Dragos customer support. Maintaining a CIP-compliant solution is achievable with the Dragos Platform. Compliance will rely heavily on entity programs, processes, and for some requirements, ongoing support from Dragos.

Does the Solution Do What It Was Purchased to Do?

When looking for solutions and tools to aid in an entity's performance of CIP obligations, be sure to put them through the CIP approval gauntlet covered in this paper. If a solution does not meet the compliance requirements, regardless of how awesome the security team thinks it is, it will create self-reported violations, or worse, lead to the discovery of a possible violation during an audit. Do you really want a situation requiring programmatic changes, mitigation plans, reconfiguration of the associated solution, or a replacement of the solution? After a solution has passed the gauntlet, the entity can start implementing it to solve the problems it was selected to address. In the case of the Dragos Platform, any of the following standards may have been the driving force behind the product selection:

- CIP-002: BES Cyber Asset identification and inventory
- CIP-005: Malicious communications detection
- CIP-007: Security event monitoring and alerting
- CIP-010: Change management of BES Cyber Assets, especially non-traditional OT devices

This section covers solution feature sets that specifically align with performance of these requirements.

CIP-002

CIP-002 is the standard that sets the scope of an entity's CIP universe. All assets the organization owns and operates are evaluated against the CIP impact rating criteria to determine whether those assets should be considered High, Medium, or Low Impact. Then the difficult efforts begin to identify the Cyber Assets and BES Cyber Assets used by, located at, or associated with the facilities.

In some of these facilities, obtaining an accurate inventory can be a significant challenge requiring months of effort. Leveraging a system like the Dragos Platform, which can be implemented with OT environment visibility and passively see device communications, over time will almost certainly assist an entity in its efforts to identify and inventory device types present in their facilities.

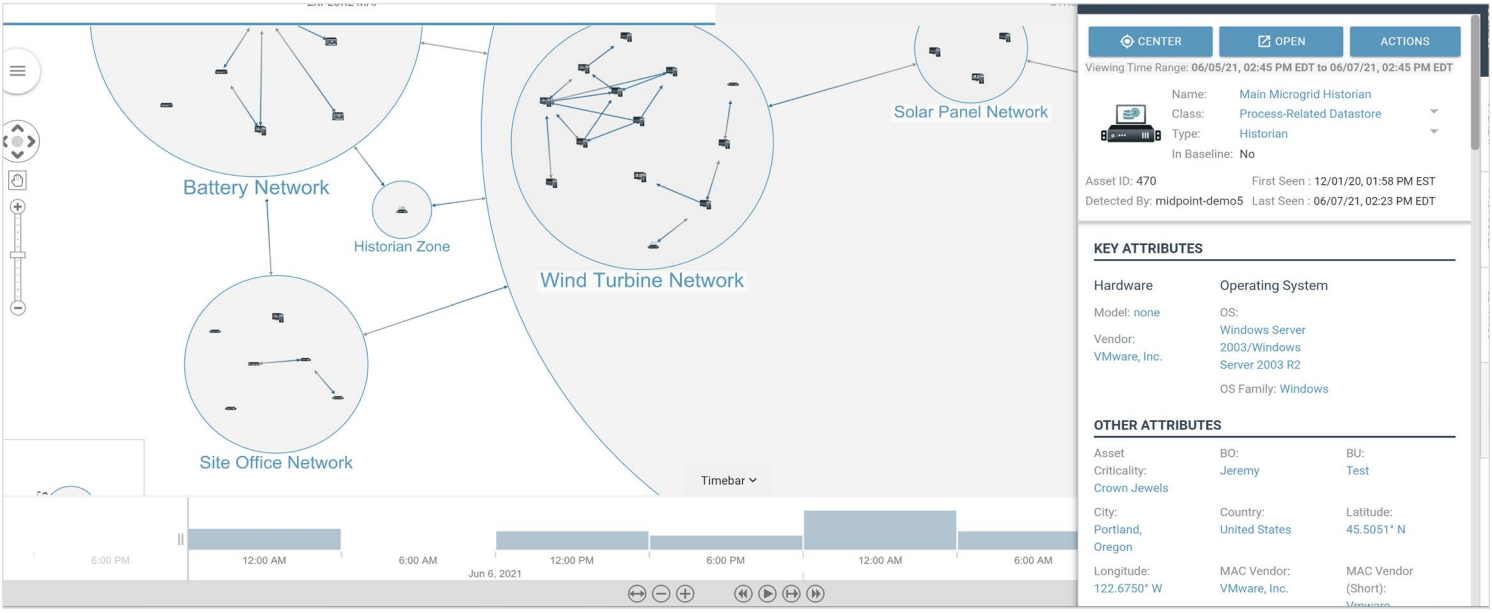

Figure 5. Asset Maps Showing Zones on the Dragos Platform

The asset maps (shown in Figure 5) provided in the platform offer many options, including:

- Displaying conversations
- Baselining environments and monitoring changes to baselines of communications
- Rolling back views with a time slider, enabling determination of what the environment looked like at a previous point in time (helpful in demonstrating that the architecture and assets were consistent throughout an audit period and identifying when a change or security-related event of interest may have occurred)

These types of capabilities can be expanded by creative compliance teams to track when a Transient Cyber Asset was added to an environment and demonstrate that it only lived in that space for less than 30 consecutive days (as defined in the NERC Glossary of Terms).[7] They can also be helpful in demonstrating negative conditions such as the absence of "shared BES Cyber Systems" communicating with each other across segmented generation units to achieve impact rating reductions under CIP-002 Attachment 1, Criteria 2.1.

Leveraging the asset inventory and the device details (see Figure 6) can be of great benefit to compliance teams as they track all the assets subject to CIP and the various applicability designations. Having a view-only capability to the Dragos

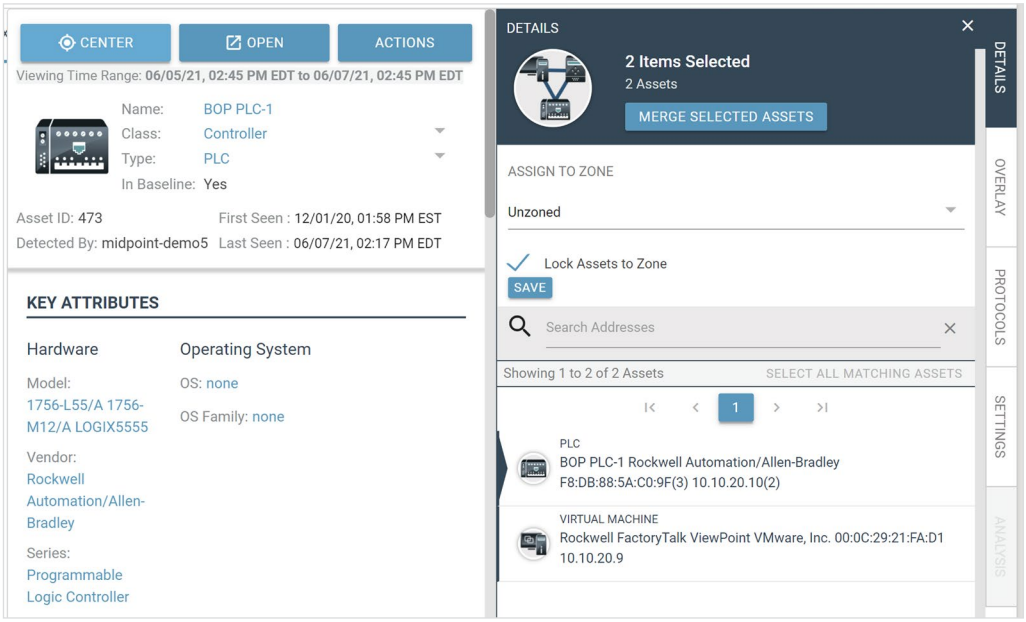

Figure 6. Asset Attributes and Details on the Dragos Platform

[7] "Glossary of Terms Used in NERC Reliability Standards," www.nerc.com/pa/Stand/Glossary%20of%20Terms/Glossary_of_Terms.pdf

Platform can allow a compliance analyst to review static inventory lists against those that are actively discovered within an environment and information about the communications observed, including the devices involved. This review could be important in incident identification, ESP rule establishment, classifying asset communications that perform External Routable Connectivity, and appropriate remote access approaches.

While CIP-002 consists primarily of requirements that direct entities to perform applicability reviews and categorization efforts, it also has within it the inherent need to identify the Cyber Assets and the unique applicability of those devices. This identification may have previously been performed with spreadsheets, manual wire-tracing tasks, system build documentation reviews, and other tools at each site, but this task is required to be reviewed every 15 months. Due to the burden of effort, it is easy to miss a new asset addition or removal.

As tools like the Dragos Platform are utilized by entities for compliance with requirements in other standards, security and compliance teams should consider it for additional areas of inclusion across an entity's broader program.

CIP-005

CIP-005 is a standard with specific focus on Electronic Security Perimeters (ESPs) that, through a series of preventive and detective controls requirements, are designed to be the first line of defense for an entity. CIP-005 is also one of the CIP Standards where a solution like the Dragos Platform directly addresses a number of the requirements.

Within CIP-005, the most common requirement that would send entities out to evaluate solutions like the Dragos Platform is CIP-005 R1.5. This requirement applies at High- and Medium-Impact rated Control Centers and directs entities to implement detective controls for known or suspected malicious communications for inbound and outbound communications. Historically, entities have pointed at their firewalls and asserted that the rulesets would appropriately block malicious communications. Over time, however, questions such as, "Does that mean every communication that is blocked is malicious?" and "Does that mean everything that is allowed is non-malicious?" have become frequent. Adversary attacks have shown that attackers commonly utilize the existing tools and technologies within a target environment to perform adversary actions. In this way, an adversary may use approved communications methods to pass through a perimeter device and then perform many actions within a perimeter that will go undetected. In an effort to detect the adversary attack approaches, entities moved toward deployments of Intrusion Detection Systems within and outside of ESP environments because they needed to satisfy the requirement language to detect ingress and egress malicious communications. Although these approaches provide great detections for traditional IT attack activity, they do not typically render useful insights into malicious communications within OT environments.

As companies such as Dragos developed the OT visibility market, organizations have adopted these solutions within OT environments because they provide ICS-aware detections. Demonstrating sensor placement with visibility to ingress and egress communications is necessary to demonstrate compliance with CIP-005 R1.5. As shown in Figure 7, the Dragos Platform architecture places sensors within the ESP and outside the ESP to demonstrate appropriate compliance of the R1.5 language.

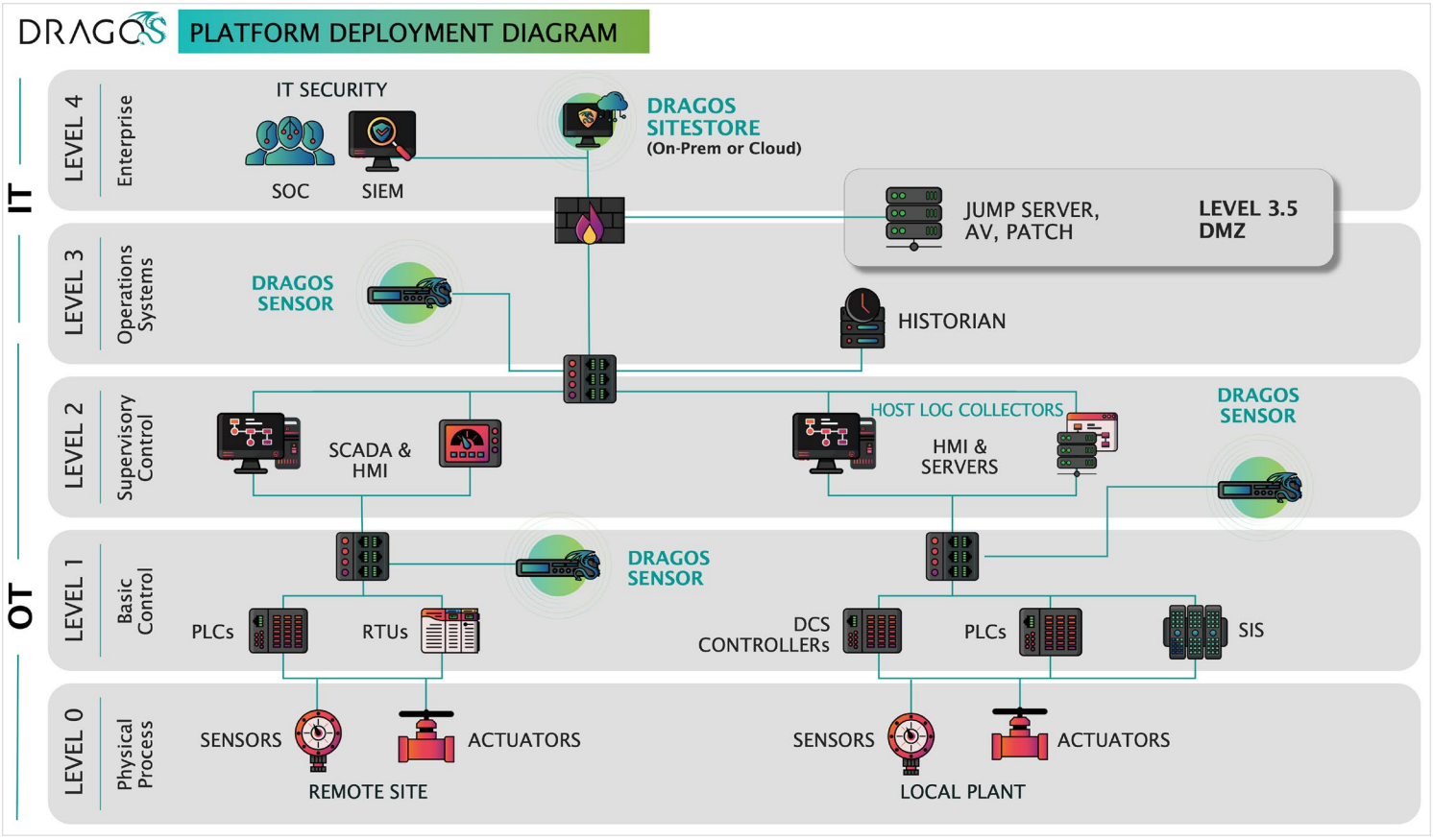

Figure 7. Dragos Platform Deployment Diagram

There are a few other CIP-005 requirements worth mentioning where the Dragos Platform may have some worthy capabilities in a CIP compliance program:

- **CIP-005 R1.2: All External Routable Connectivity must be through an identified Electronic Access Point (EAP).** The Dragos Platform can help entities identify any communications that could be occurring externally (and not going through an identified EAP) through the use of the Asset map and the communications analysis capabilities.
- **CIP-005 R2.4: Determine active vendor remote access sessions (interactive or system to system).** The Dragos Platform will certainly capture the communications that occur and can be used to identify which connections exist. Entities can also implement additional displays and dashboards to indicate when an interactive session or potentially baseline routine system-to-system remote access is established to highlight when an event of interest occurs. (See Figure 8 on the next page.)

While CIP-005 provides the initial electronic perimeter defense requirements, additional CIP Standards exist to ensure additional security protections are in place in the event that the perimeter is compromised.

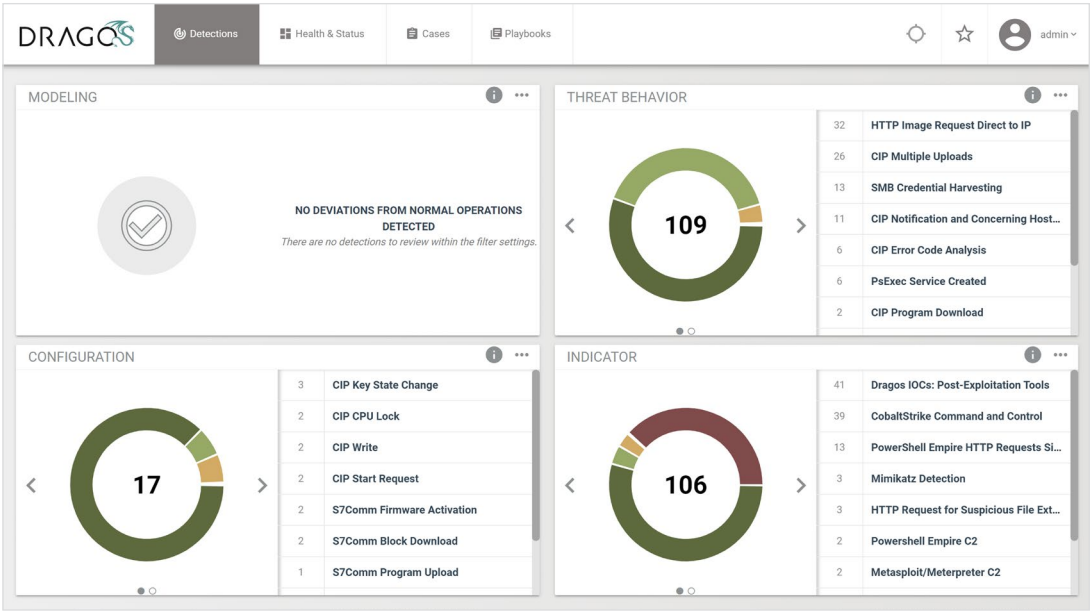

Figure 8. Dragos Platform Threat Detection Dashboard

CIP-007

CIP-007 is the Systems Security Management Standard that focuses on the hardening of assets through a series of procedural and technical controls. CIP-007 addresses broad topics, such as restricting accessible ports and services on an applicable Cyber Asset, patching, malicious code detection, and account management. The requirements directly applicable to solutions like the Dragos Platform are found in CIP-007 R4: Security Event Monitoring.

CIP-007 R4.1 provides specific guidance about what types of events must be logged on an applicable Cyber Asset:

- R4.1.1 addresses detected successful login attempts (see Figure 9 on the next page).
- R4.1.2 deals with detected failed access attempts and failed login attempts (see Figure 10 on the next page).
- R4.1.3 addresses detected malicious code.

Because the capability to perform logging varies and may be limited on some devices within OT environments, there are certainly some limitations on devices to perform each of these actions. These limitations are recognized in the requirement language when it states that these items need to be logged per System and per Asset capability. So, where capable, these events need to be logged and the logs retained for 90 days. In addition, for Control Center environments, a summary or sample set of the logs must be reviewed every 15 days to identify potential Cyber Security Incidents.

To satisfy these logging requirements, entities have pursued solutions capable of collecting and storing these various asset logs. For Windows system logs and **`syslog`**-capable systems, this is an area where the Dragos solution helps. The sensors can be configured to directly collect various system log file formats including **`syslog`**, **`wmi`**, and **`SNMP`** data. It can indirectly collect log data from existing SIEM solutions and forward all of that information to the SiteStore for retention and routine review, as required within CIP-007 R4.

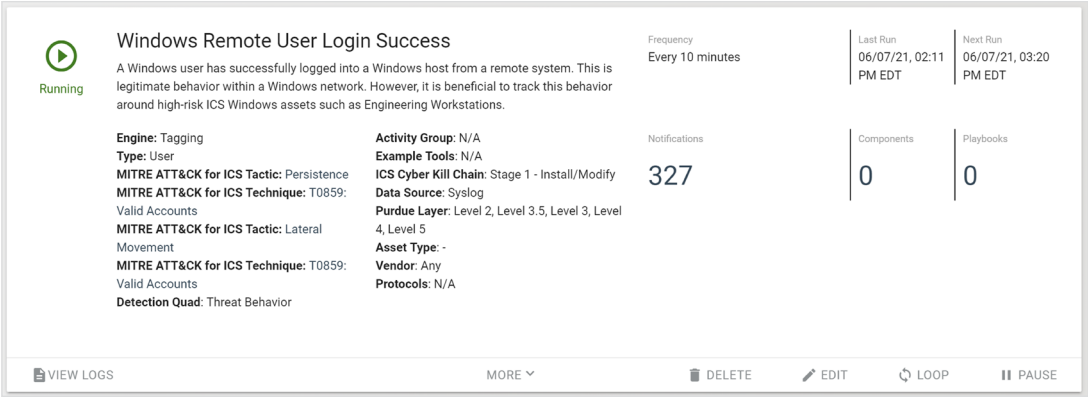

Figure 9. Remote User Login Detection Summary

Figure 10. Failed Login Attempt Detection Logging

In addition to the CIP-007 R4 logging requirements, there are also requirements to generate alerts for security events within CIP-007 R4.2:

- R4.2.1 addresses how to generate alerts for detected malicious code.
- R4.2.2 focuses on generating alerts for detected failure of event logging.

An additional alerting requirement appears under CIP-007 R5.7 for generation of alerts after a threshold of unsuccessful authentication attempts.

The manner in which these system alerts can be achieved varies by asset type. For example, a network infrastructure switch or a substation digital protection relay cannot typically detect malicious code and, thus, would not be capable of generating an alert for detected malicious code. Therefore, a solution that can ingest direct alerts as well as offer the customization capabilities to identify alert conditions within log files is ideal.

In the case of detected malicious code, some AV solutions generate an event in a system security log if a detection is triggered, while others only generate a detection notification within the application. In these cases, the data can be pulled and pushed to solutions like Dragos through the use of scripts and other approaches. Once the data has been pushed to the SiteStore, custom dashboards (shown in Figure 11 on the next page) and alerts can be created.

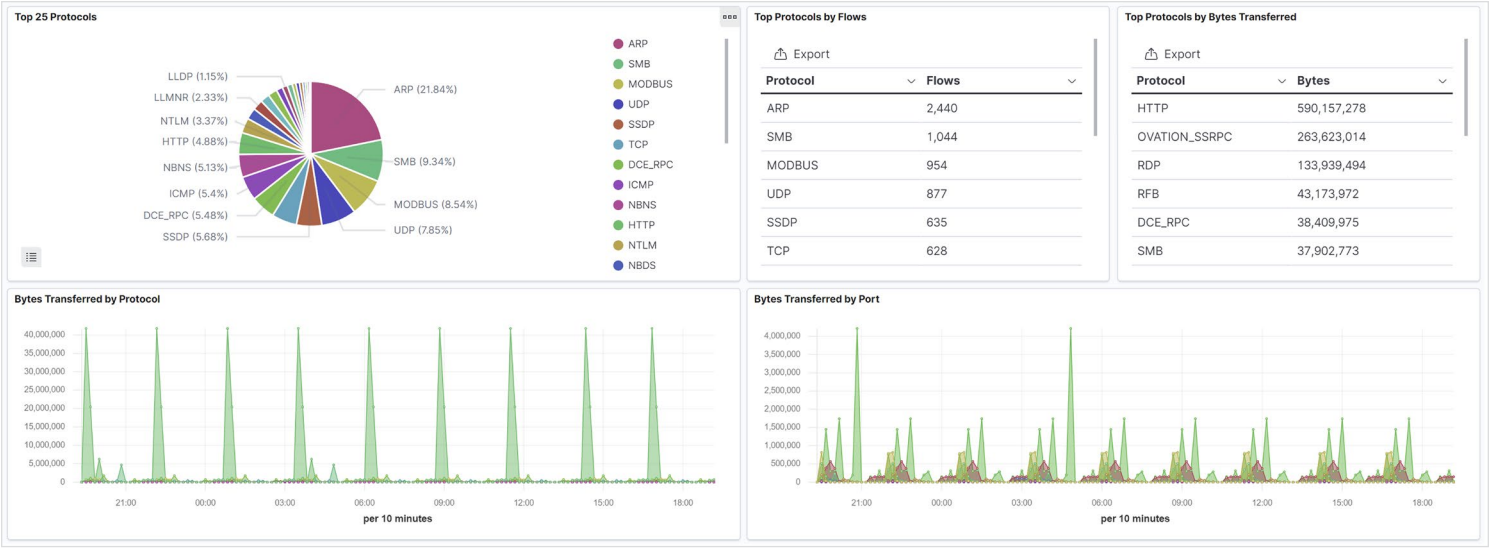

Figure 11. Dragos Platform Summary Dashboard of Ingested Data

The requirement to generate alerts for failure of logging can be tricky because although events may be generated to indicate logging failure, in many systems there is no such alarming of log failure.

Too often, entities configure dashboard screens that highlight some of the wonderful features of a tool: top talkers, top protocols, bandwidth consumption, link status, peak traffic times, and the like. Unfortunately, none of this information helps demonstrate compliance with CIP-007 R4. CIP-specific dashboards and reports that demonstrate the performance of the required logging and alerting is specifically helpful in demonstrating and ensuring compliance.

In addition to the R4 requirements, CIP-007 R1 also requires entities to configure applicable Cyber Assets in a manner that ensures only the necessary ports and services are enabled. As these network-accessible logical ports are identified and configured, the communications captured and displayed within the Asset Explorer can be used as a secondary control to show that the applicable Cyber Assets are operating as intended over time.

CIP-010

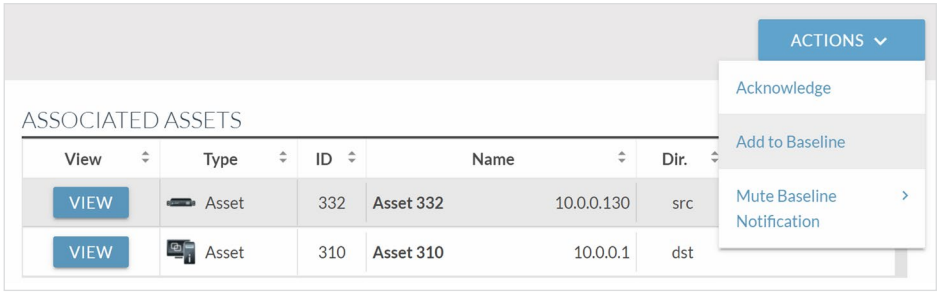

Figure 12. Related Assets for Baseline Monitoring on the Dragos Platform

CIP-010 is the Configuration Change Management and Vulnerability Assessments Standard. If you consider CIP-007 as the system hardening standard, then CIP-010 exists to ensure the system remains in that hardened configuration, ensure that changes do not affect security controls, and provide additional requirements to identify any vulnerabilities that may exist. It also ensures TCAs and RMs are used in a secure manner. CIP-010 R1 and R2 consist of programmatic and procedural elements that are required to ensure that system baselines exist and that changes to a system are verified, tested, authorized, and updated within an appropriate period of time. The performance of these tasks can be exceptionally manual, especially with ICS devices. Utilizing elements of the Dragos Platform to develop baselines of specific ICS devices (see Figure 12) and integrating these detective controls into the larger CIP configuration change management program can help demonstrate compliance for these tasks on non-traditional devices.

In addition, CIP-010 requires verification that approved changes did not alter existing security controls. Entities could leverage the Dragos Platform as an additional detective control, for example, to determine whether an approved change to a system (say a security-related OS patch) has unintentionally modified existing security controls (such as resetting local host firewall rules). Asset-specific detail dashboards can provide information that may help identify unintended changes to a baseline. See Figure 13.

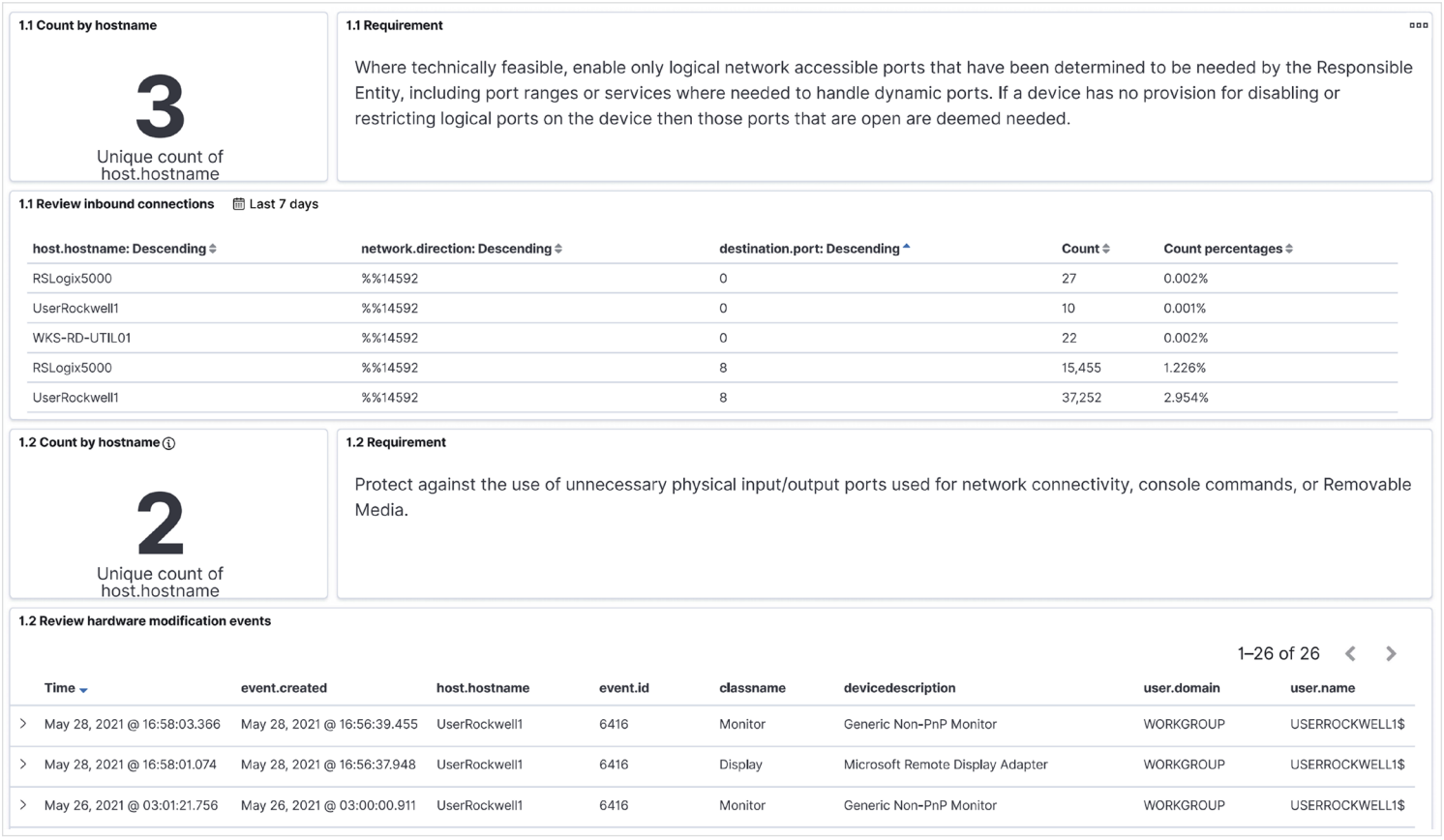

Figure 13. CIP-007-Related Event Detections Used in CIP-010

Achieving a constant level of CIP compliance across all facilities, applicable Cyber Assets, and requirements with zero deficiencies throughout an audit period is difficult. Attempting to run a CIP program effectively without the integration of security and compliance solutions is impossible. Because each solution that is added to a CIP program brings with it compliance burdens and risk, it is important to pursue a balance between security and compliance. When a solution like the Dragos Platform can be leveraged across numerous standards and requirements, then it should be given special consideration due to the broad benefits provided.

Going Beyond Compliance

While it may not feel like it to most entities that are subject to the NERC CIP Standards, the standards were developed as a minimum set of security requirements designed to ensure the reliability of the BES. Many entities frequently implement security controls in one area or another that exceed the specifics of a requirement—and they gain the security benefits of the additional capabilities. Many of these controls are preventative or detective, but there are also some extremely important security capabilities of the Dragos Platform specific to incident response and information sharing that entities should pursue.

The CIP-008 Incident Reporting and Response Planning Standard provides specific requirements in relation to processes and plans necessary for incident identification, required elements of a response plan, incident handling procedures, plan testing, notification requirements, and programmatic reviews.

These are all important and necessary elements of an effective incident response capability for an entity. Remember, though, that entities can fall prey to a false sense of security when they aim for compliance with only the minimum requirements. Having plans and procedures for "an attack" may not adequately capture the wide variety of attack scenarios that could occur. Having specific response approaches developed for various scenarios may be far more effective.

As shown in Figure 14, the Dragos Platform provides for specific playbook-driven responses based on identified detections. While this is not required for compliance, it provides a more predictable, calm, and guided approach to response activities when there may be high levels of chaos during a real-world incident.

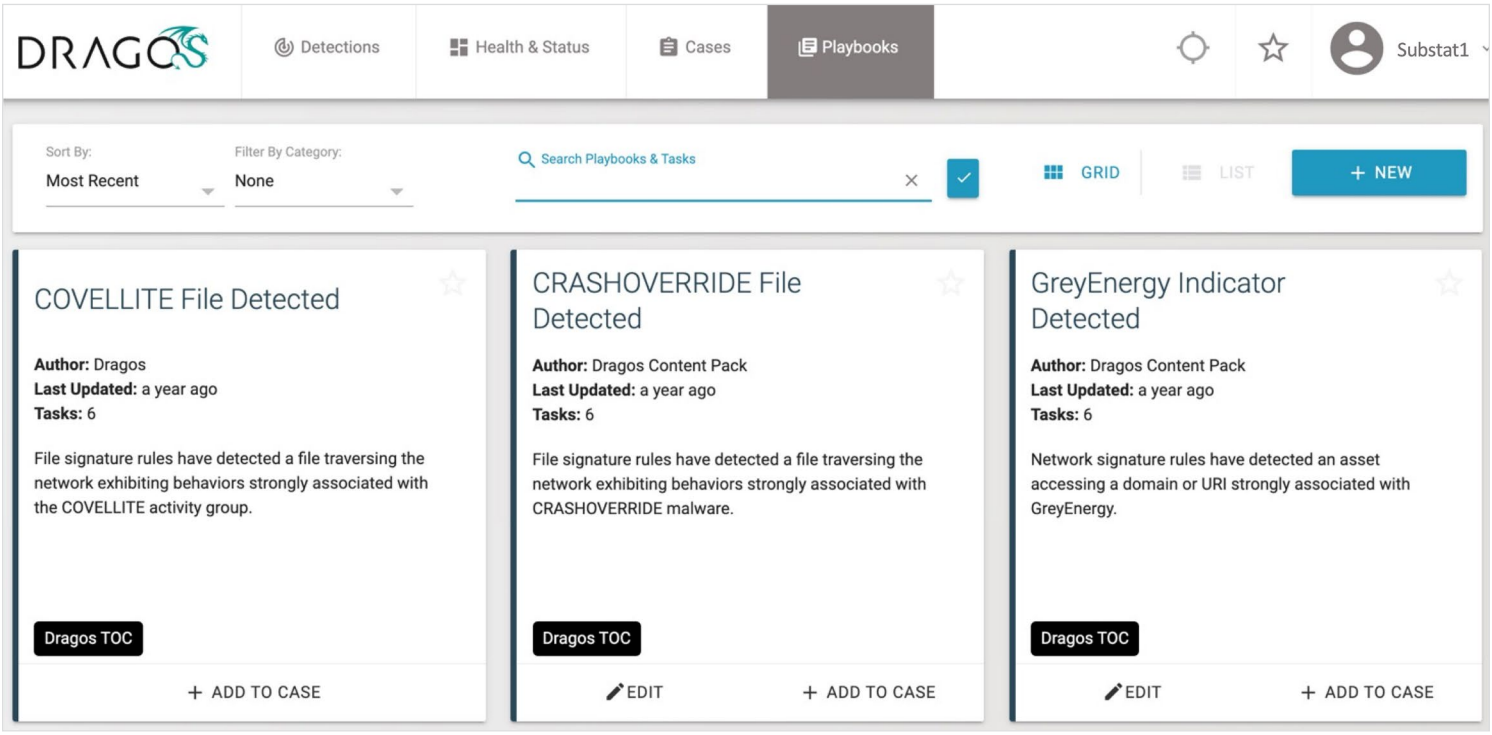

Figure 14. Incident Response Playbook Capabilities of the Dragos Platform

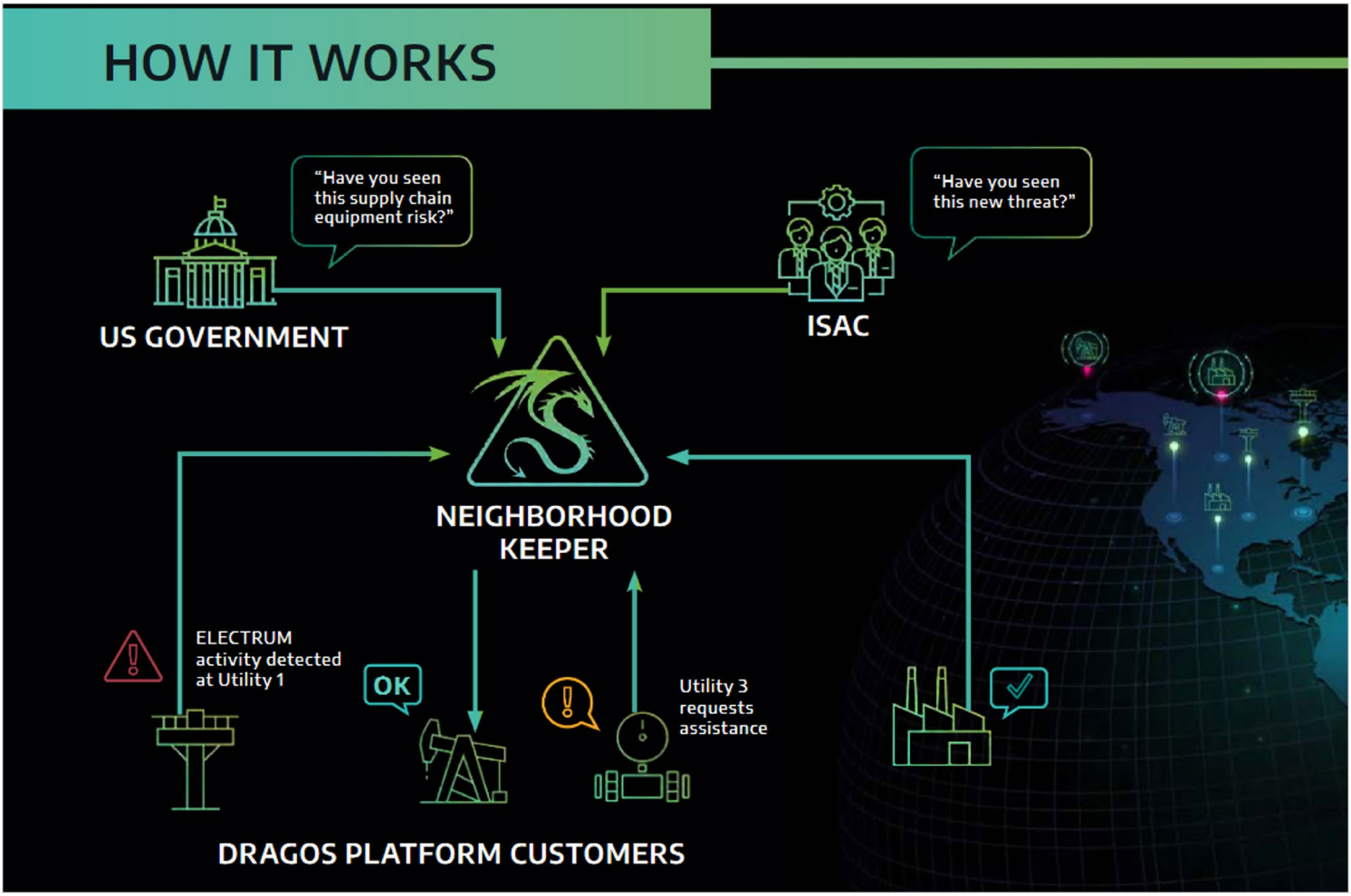

Figure 15. Neighborhood Keeper Overview

One of the more interesting capabilities of the Dragos Platform is the Neighborhood Keeper[8] program (see Figure 15). We mention it now because, although there are information sharing and notification requirements within CIP-008, the capabilities of Neighborhood Keeper go far beyond the compliance requirements. Neighborhood Keeper is a voluntary program that Dragos Platform customers can choose to participate in. An existing platform customer can deploy Dragos Sensors and SiteStore in their ICS/OT environments. Then if they choose to opt in, they can enroll in the Neighborhood Keeper program.

If an entity voluntarily enrolls, there are no additional CIP requirements to participate. For example, if the Dragos Sensors and SiteStore are associated with CIP facilities, they would need to comply with CIP as applicable assets as referenced earlier in this paper. If the Dragos Platform is being used to satisfy CIP compliance requirements, then it would already be configured and operated as mentioned in this paper based on the requirements for which it is being used. If an entity chooses to take the detection indicators and share that information with peers and the electric sector throughout North America, the only unique CIP concern that emerges is the question of whether the information being shared is BES CSI. The information protection approach taken

[8] "Neighborhood Keeper: Collective Defense for Industrial Cybersecurity," www.dragos.com/wp-content/uploads/relocated/n/Neighborhood_Keeper_Datasheet.pdf

within the Neighborhood Keeper program is one of the more powerful elements of this unique information sharing capability in that the customer-related data and potential BES CSI remains at the entity site. The only data shared is anonymized metadata that provides only details on the threat detection. No entity-specific data with any CIP-related context is shared.

This threat detection-driven anonymous alert is received by the Neighborhood Keeper participants, who can see information from across the community about what is happening based on a sector. They see what vulnerabilities or adversary methods are being detected and then use that information to inform their internal efforts. Other program participants, such as government organizations and Information Sharing and Analysis Centers (ISACs), can gather insights from the detections to determine whether there is a coordinated attack across multiple participants or sectors. They can utilize the information to inform their actions across critical infrastructure organizations.

The last item to highlight with Neighborhood Keeper is the capability to operationalize Cyber Mutual Assistance requests for help by an anonymous participant. Other participants can respond and can then further connect (if appropriate) for additional assistance. Although none of this is required for compliance, all of the features of the Neighborhood Keeper program are what the ICS community of asset owners and operators need.

Getting Married

As entities look for potential solutions to help them in their CIP programs, they are not looking for frequent or dramatic changes within their CIP environments. Entities do not want to try a solution, identify issues, and then try something different; nor do they want to select an emerging innovative company technology and then see that organization get acquired or drop a product line. Entities are looking for solutions that are sustainable and will have an extended predictable product lifecycle that can sustain multiyear deployment programs across geographies. Entities are not looking to "date" CIP solution providers, they are looking to "settle down and marry" CIP solution providers. This paper outlined many of the criteria entities should explore as they make the decision about what solution provider to marry.

Conclusion

As electric sector entities evaluate the Dragos Platform, they should consider four criteria in relation to selecting a monitoring and detection solution provider across their CIP facilities.

- **Is the solution provider company a good fit for doing business with CIP-affected entities?** Whereas a number of solution providers struggle to understand CIP and how it affects their products, Dragos truly has a focus area strength and subject matter expertise in electric sector operations, ICS environments, and NERC CIP.
- **Can the solution be configured and maintained in a compliant manner?** As discussed throughout this paper, no solution is automatically compliant—it must be capable of being configured in a compliant manner and then integrated into an entity's CIP program. The Dragos Platform V1.8 solution reviewed in this paper provides the necessary configuration capabilities for entities to pursue during deployment with Dragos support and throughout the lifecycle of the solution.
- **Does the selected solution perform the advertised functions to help with a given compliance requirement?** This paper provided examples and references to numerous NERC CIP Requirements where the Dragos Platform could be utilized by an entity to satisfy strict compliance with a requirement or as an additional security control within a CIP program.
- **Does the selected solution offer any additional capabilities beyond compliance that could help our business?** The Dragos Platform truly does bring additional detection, incident response, and information-sharing capabilities to an organization that go far beyond the compliance requirements. Its features help an entity with the dynamic challenges of providing a safe, reliable, and secure operational environment.

Adversary attacks will continue to evolve and so, too, will regulation-based Cyber Security requirements such as the NERC CIP standards. Electric entities facing these challenges cannot face them alone. Instead, they need to pursue partners and solutions that fit with their operational needs and business objectives.

About the Author

Author **Tim Conway** serves as the technical director for ICS and SCADA programs at SANS and is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. Recognizing the need for ICS-focused cybersecurity training throughout critical infrastructure environments and an increased need for NERC CIP hands-on training, Tim co-authored and instructs ICS456: Essentials for NERC Critical Infrastructure Protection. During his career, Tim has served as the chair of the RFC CIPC, the NERC CIP Interpretation Drafting Team, the NERC CIPC GridEx Working Group, and the NBISE Smart Grid Cyber Security panel.

Sponsor

SANS would like to thank this paper's sponsor: