Driving NERC CIP Compliance

A solutions-based approach to cybersecurity for power utilities in North America.

Contents

Overview

The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards are a set of requirements designed to secure the Bulk Electric System (BES) in North America. The CIP Cyber Security Standards use the “BES Cyber System” to apply requirements to groups of devices rather than individual Cyber Assets, as malware protection applies to the system as a whole and may not be necessary for every individual device to comply.

The scope of the CIP Cyber Security Standards is restricted to BES Cyber Systems that would impact the reliability of the BES, otherwise known as the impact rating. Each BES Cyber System can be categorized as High, Medium, Low or non-BES. The impact rating criteria can be found in CIP-002-5.1a, attachment 1.

Understanding the impact rating of your BES Cyber System is an important first step for compliance, as the outcome of this step will determine the pertinency of the proceeding standards. CIP-003-9 mandates responsible entities to specify consistent and sustainable security management controls to protect BES Cyber Systems against compromise that could lead to mis-operation or instability in the BES.

For high and medium impact BES Cyber Systems, responsible entities must address the following topics:

- Personnel and training (CIP-004)
- Electronic Security Perimeters (CIP-005) including interactive Remote Access
- Physical security of BES Cyber Systems (CIP-006)
- System security management (CIP-007)
- Incident reporting and response planning (CIP-008)
- Recovery plans for BES Cyber Systems (CIP-009)
- Configuration change management and vulnerability assessments (CIP-010)
- Information protection (CIP-011)
- Communications between Control Centers (CIP-012)
- Supply Chain Risk Management (CIP-013)
- Physical Security (CIP-014)
- Internal Network Security Monitoring (CIP-015)
- Declaring and responding to CIP Exceptional Circumstances

For low impact BES Cyber Systems, responsible entities must address the following topics:

- Cyber security awareness
- Physical security controls
- Electronic access controls
- Cyber Security Incident response
- Transient Cyber Assets and Removeable Media malicious code risk mitigation
- Vendor electronic remote access security controls
- Declaring and responding to CIP Exceptional Circumstances

Addressing grid security challenges with Cisco Industrial Threat Defense

The utility grid is undergoing substantial change and modernization, resulting in more devices being connected than ever before. While this additional connectivity brings tremendous benefits to the utility business, it also opens more risks with regards to cybersecurity that unfortunately cannot be addressed overnight. To help ensure success, Cisco promotes a phased approach in which each phase builds the foundation for the next, so that you can enhance your security posture at your own pace and demonstrate value to all stakeholders when embarking on this journey.

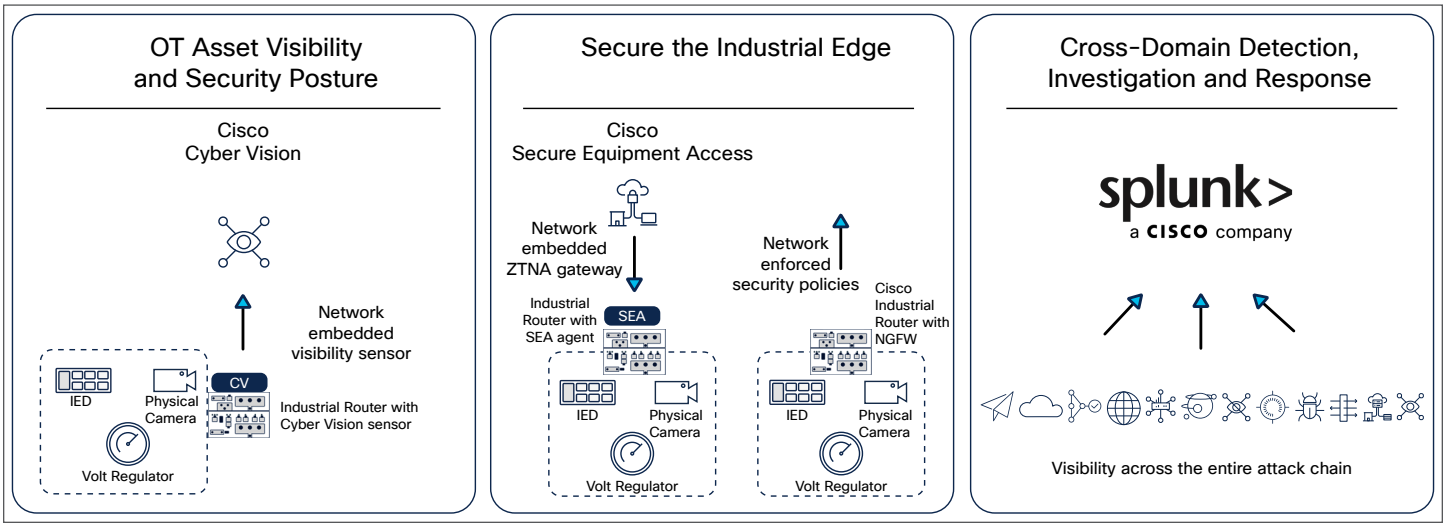

Figure 1. Cisco Industrial Threat Defense

The first step is to gain asset visibility and security posture with Cisco Cyber Vision. Cisco Cyber Vision provides asset owners full visibility into their industrial networks and their OT security posture, so they have the information they need to reduce the attack surface, segment the industrial network, and enforce cybersecurity policies. Cyber Vision helps answer questions such as: what vendors exist on the network? Are there devices that I do not recognize? What vulnerabilities can be exploited in the environment? What devices are communicating with external networks? Do these devices with heightened exposure also have a path to the critical services in the network? Combining a unique edge architecture that embeds Deep Packet Inspection (DPI) into your industrial network, and integration with the Cisco leading security portfolio, Cyber Vision can be easily deployed at scale to enable IT and OT teams to work together in building innovative industrial operations while securing the global enterprise.

While visibility is important, taking preventative measures to secure your operations is required. Cisco recommends taking a zero-trust approach to securing the grid network.

Protecting grid assets starts with controlling remote access activities from vendors, contractors, or remote experts. Cisco Secure Equipment Access (SEA) combines all the benefits of a Zero-Trust Network Access (ZTNA) solution with a network architecture that makes it simple to deploy at scale in operational environments. There is no dedicated hardware to install and manage. No complex firewall rules to configure and maintain. The Cisco industrial switches or routers that connect your grid assets now also enable remote access to them. And it features comprehensive security capabilities, with advanced cybersecurity controls and easy-to-build least-privilege policies based on identities and contexts.

When implementing a zero-trust model within an OT network, Cisco recommends building zones of trust, aligning to the IEC 62443 framework for zones and conduits. Across utility networks, organizations need advanced, agile, and secure Wide Area Network (WAN) infrastructures to connect distributed OT assets to control centers and unlock the potential of digitization. Not only do Cisco Industrial Routers offer unconditional connectivity for all your remote assets but come with a comprehensive Next Generation Firewall (NGFW) features and many more cybersecurity capabilities to block modern threats.

Finally, to solve the challenge of scattered event logs across the ecosystem, Splunk provides cross domain detection, investigation, and response. Splunk is a leading Security Information and Event Management (SIEM) solution that provides the detection, analytics, case management, incident response, and orchestration platforms all in one interface. Splunk ingests data from Cyber Vision to provide visibility into OT, and correlates that with other data sources like network access control, NGFW, among others, to provide a holistic view of the entire grid network from endpoints in the LAN, to egress/ingress points and all the way to the data center by across a multi-vendor environment.

Using Cisco Industrial Threat Defense to fulfill NERC CIP compliance

CIP-002 – BES Cyber System Categorization

NERC CIP requires BES Cyber Systems to be classified and broken down by specific classifications and security zones. The classifications require an asset to be assigned a CIP criticality as well as CIP asset type. CIP explicitly defines criticality as Low, Medium, or High and has numerous asset types (BCA, PCA, EAP are all examples). CIP-002 is in place to determine the level of risk associated with the utility under audit and is predominantly a procedure and documentation effort. However, it is necessary to understand the level of exposure and the key components in the grid. The Splunk OT Security Add-On provides a Critical Cyber Asset Scorecard to help customers understand how assets are classified in their environment.

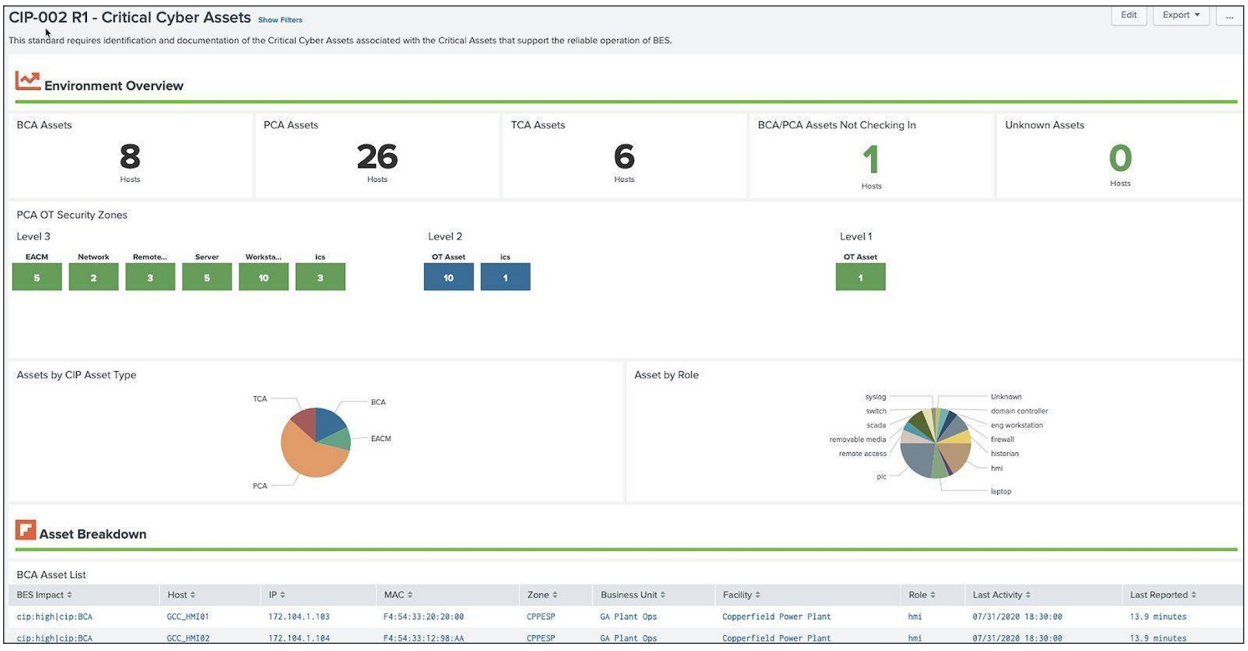

Figure 2. Splunk critical cyber asset scorecard example

CIP-004 – Personnel & Training

Security Awareness Training

NERC CIP requires that users and operators in regulated environments complete specific training as part of the certification process. For users who require certification, they must be classified into groups which determine which training is required. In addition, updates to course materials should be communicated to individuals who have previously taken this training (normally via email). Splunk leverages an email data model to identify whether notifications have been received by users and operators.

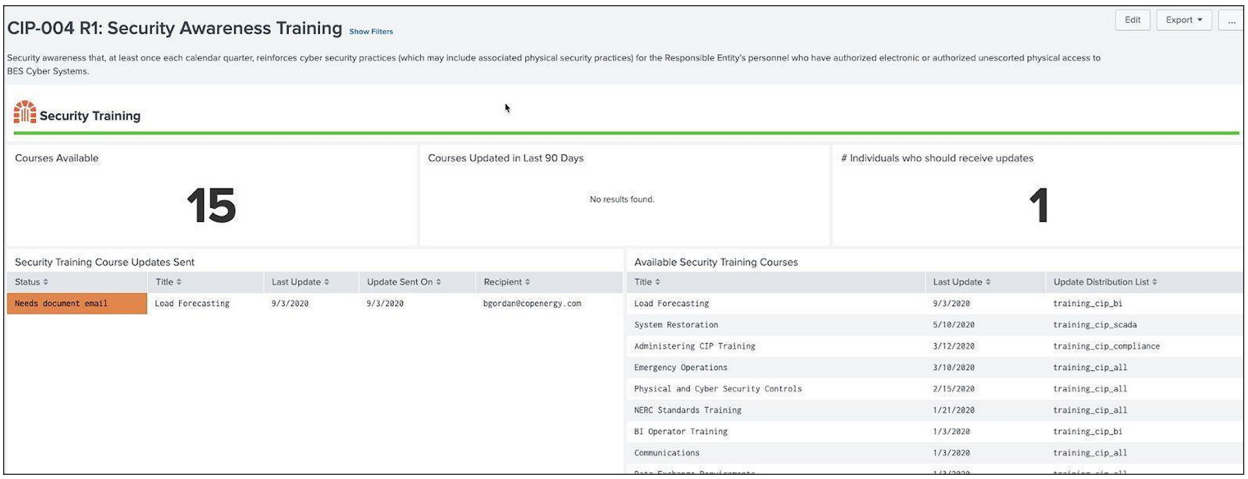

Figure 3. Security awareness training example in Splunk

Cyber Security Training

Individuals who access NERC CIP environments must be trained and certified before accessing assets remotely, onsite, or physically in that environment. NERC CIP requires that training requirements be tracked and monitored for expired certifications and then correlated with access records. The Splunk OT Security Add-On makes use of the authentication data model to determine remote or local access to systems by individuals required to be NERC CIP certified, and correlates that with their certification status.

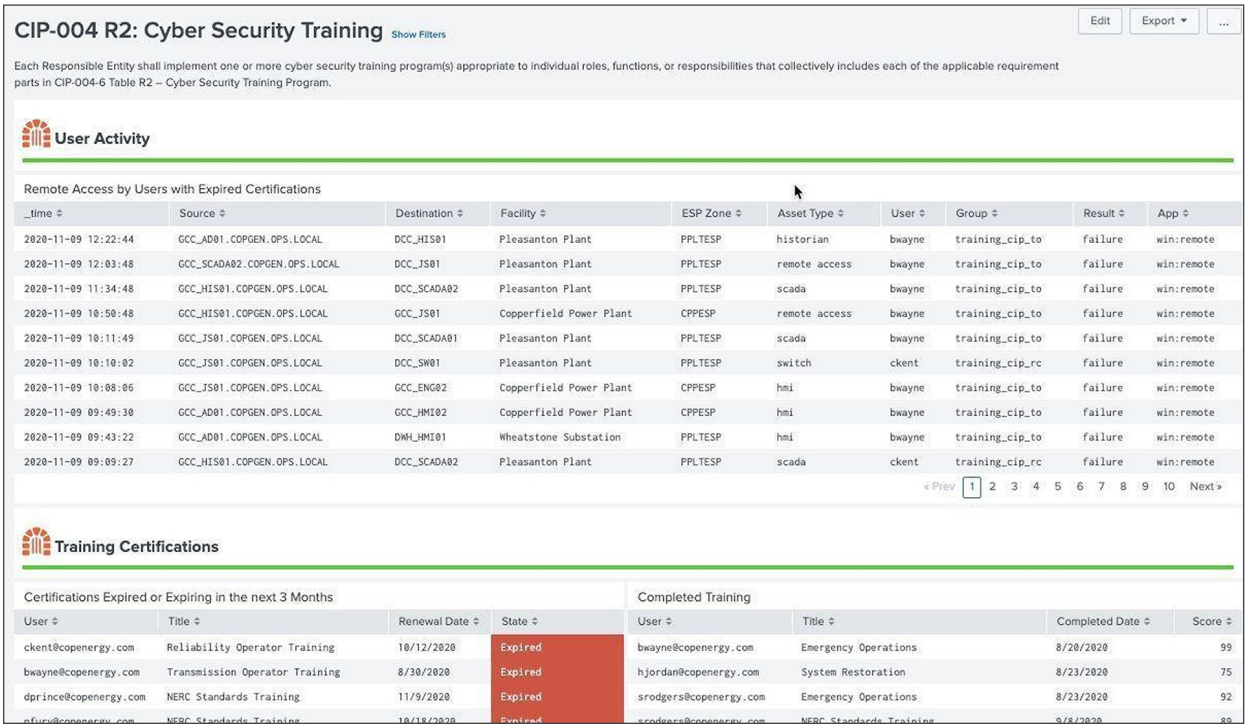

Figure 4. Cyber security training example in Splunk

Personnel Risk Assessment (PRA) program

Individuals accessing NERC CIP environments must periodically have Personnel Risk Assessments (PRA) performed not to exceed every 7 years. This certification may be performed by outside entities, but should be tracked and recorded by operators of NERC CIP assets. In addition, access to NERC CIP environments should be monitored for individuals out of compliance.

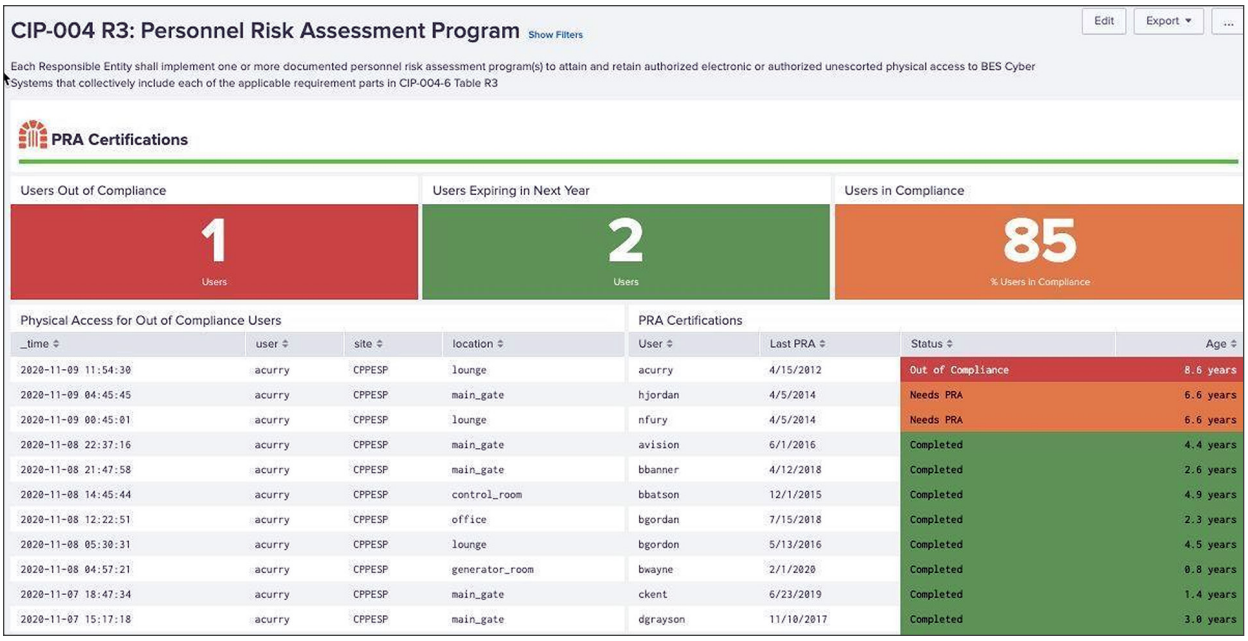

Figure 5. Personnel risk assessment example in Splunk

CIP-005 – Electronic Security Perimeter(s)

The purpose of this requirement is to manage electronic access to BES Cyber Systems by specifying a controlled Electronic Security Perimeter (ESP) in support of protecting BES Cyber Systems against compromise. All applicable Cyber Assets connected to a network via a routable protocol must reside within a defined ESP.

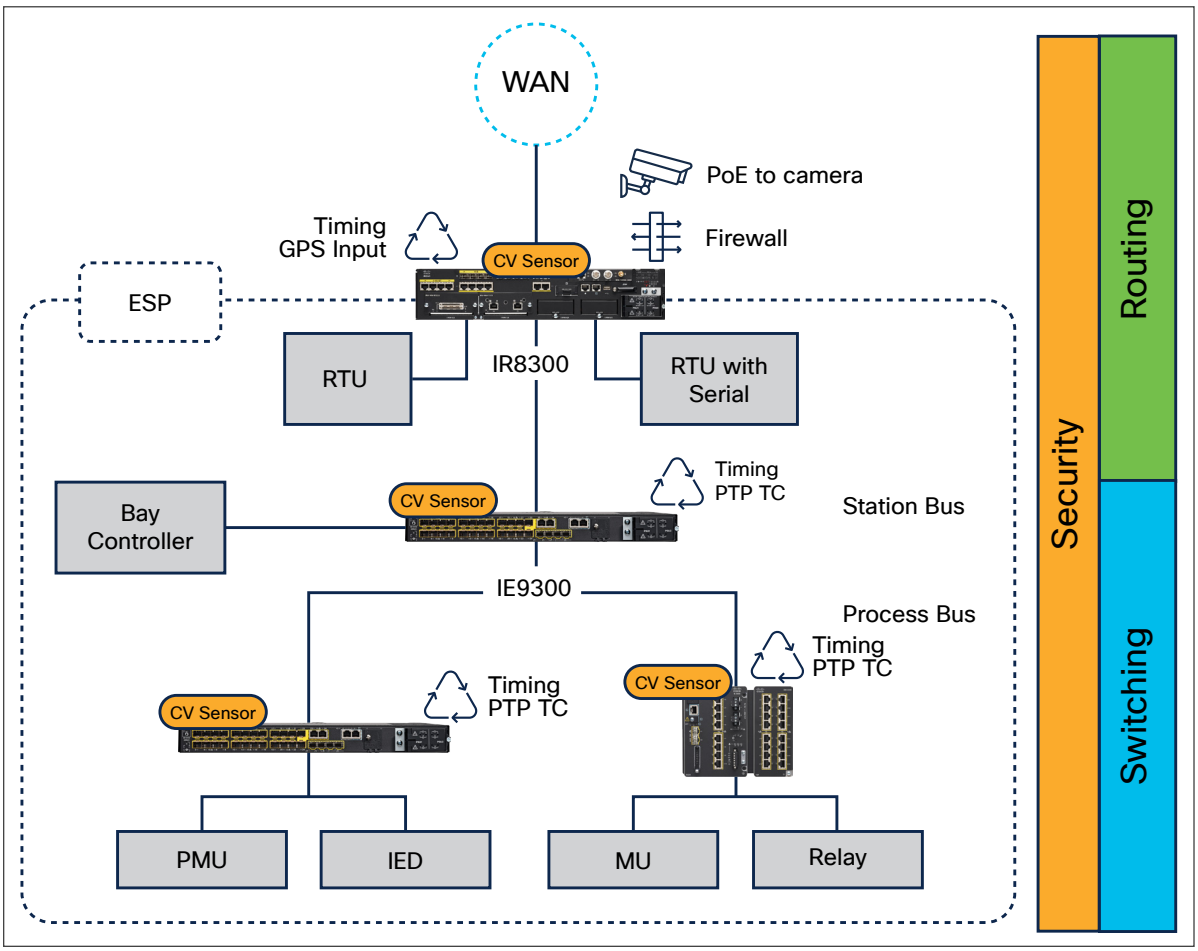

Figure 6. Electronic security perimeter in a substation with Cisco IR8340

Cisco Industrial Routers offer unconditional connectivity for all your remote assets. They can withstand extreme temperatures, humidity, and dust. They offer a variety of WAN connectivity options, including 5G/LTE cellular, MPLS, Ethernet, and fiber, through pluggable interface modules that can be easily replaced when needs or technologies evolve. In addition, Cisco Catalyst SD-WAN simplifies deploying and managing a large and complex WAN infrastructure from a central location.

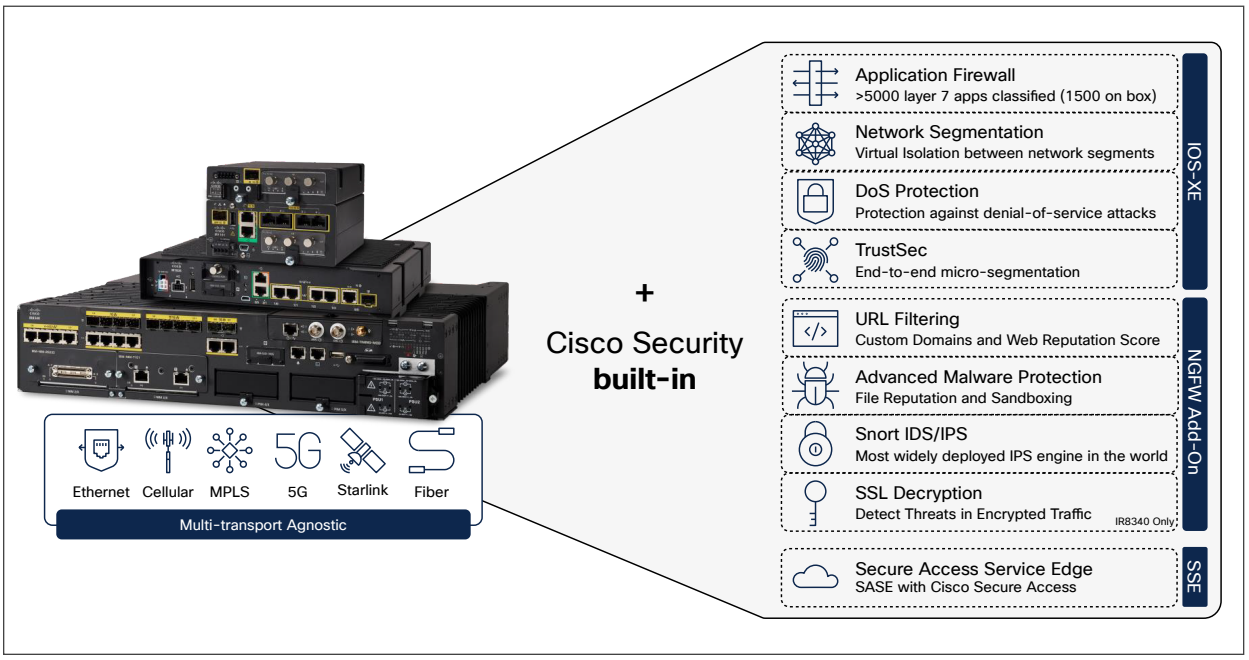

Figure 7. Security capabilities of the Cisco Catalyst IR8340

To meet the security needs at the ESP, Catalyst industrial routers come with comprehensive Next-Generation Firewall (NGFW) features and many more cybersecurity capabilities to block modern threats, including:

- Standard firewall capabilities like stateful inspection,
- Application awareness and control to block application-layer attacks,
- Integrated intrusion prevention (IDS/IPS),
- Continuously up-to-date threat intelligence,
- Asset visibility and security posture with Cisco Cyber Vision.

Converging industrial networking and cybersecurity helps ensure unified security policies are enforced across sites, eliminating gaps in defenses due to cost and complexity of integrating many point products together.

NERC CIP for renewable energy

Substation networks are not the only industry that is suspect to NERC CIP regulations. As countries invest in renewable energy generation to accelerate the move toward carbon neutrality, wind farms, solar farms, and battery storage will be mandated to comply. It is up to the Responsible Entity (any organization that operates elements of the BES) to determine the level of granularity at which to identify a BES Cyber System. For example, the Responsible Entity might choose to view an entire turbine operator control system as a single BES Cyber System, or it might choose to view certain components of the turbine operator control system as distinct BES Cyber Systems.

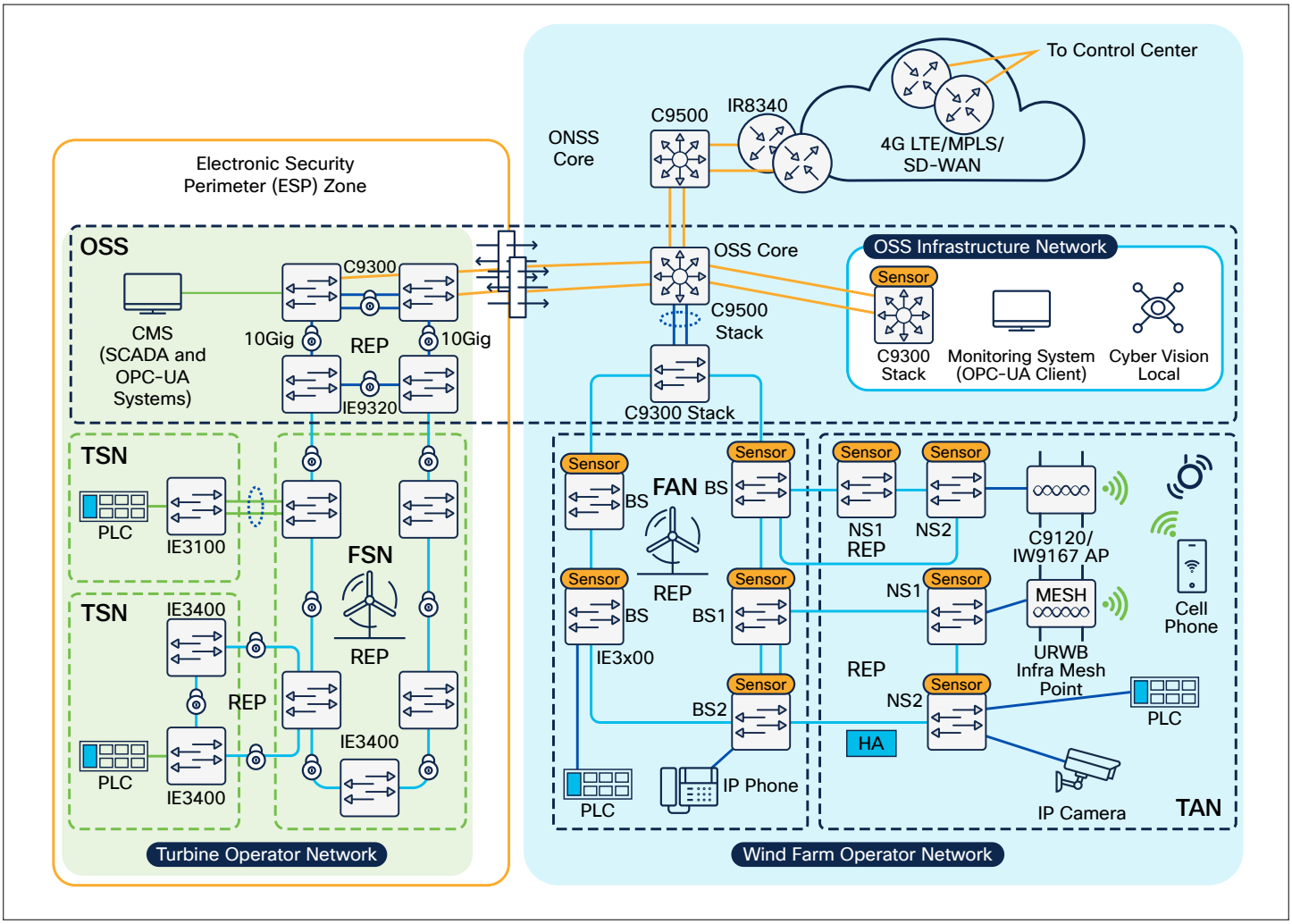

Figure 8. Electronic Security Perimeter in a Wind Farm with Cisco Secure Firewall

In the case of a wind farm, the ESP boundary may reside outside of the turbine network, located in the core network infrastructure. In this case, the Cisco Secure Firewall can be used as the identified Electronic Access Point (EAP) for NERC CIP compliance. Using the application rules hosted on the firewall, operators can deny access by default and grant specific application access to only the devices that require it, including limiting operations to read only capabilities, if using protocols such as DNP3 to gather information from the control systems.

Remote access for NERC CIP

Additionally, CIP-005-7 calls for cybersecurity measures on remote access management. Cisco Secure Equipment Access (SEA) is a hybrid solution with the Zero Trust Network Access (ZTNA) broker being a cloud service and the ZTNA gateway running in Cisco industrial switches and routers. Cloud is often a no-go for NERC CIP protected substations, however, operators can deploy SEA gateways outside of the ESP which act as the intermediary system for remote access attempts. As per requirements, administrators of the platform can force all users to undergo Multi-Factor Authentication (MFA), and to monitor, record and terminate (if needed) all active sessions.

CIP-005 Reporting with Splunk OT security add-on

For assets which are part of the ESP (normally firewalls and data diodes), they can be explicitly tagged in Splunk with the classification in the asset framework to populate the dashboards built for monitoring activity across the ESP boundary. All data that crosses the boundary must be explicitly permitted. Additional data sources from equipment such as networking infrastructure and multi-factor authentication systems help to determine if remote communications are properly secured.

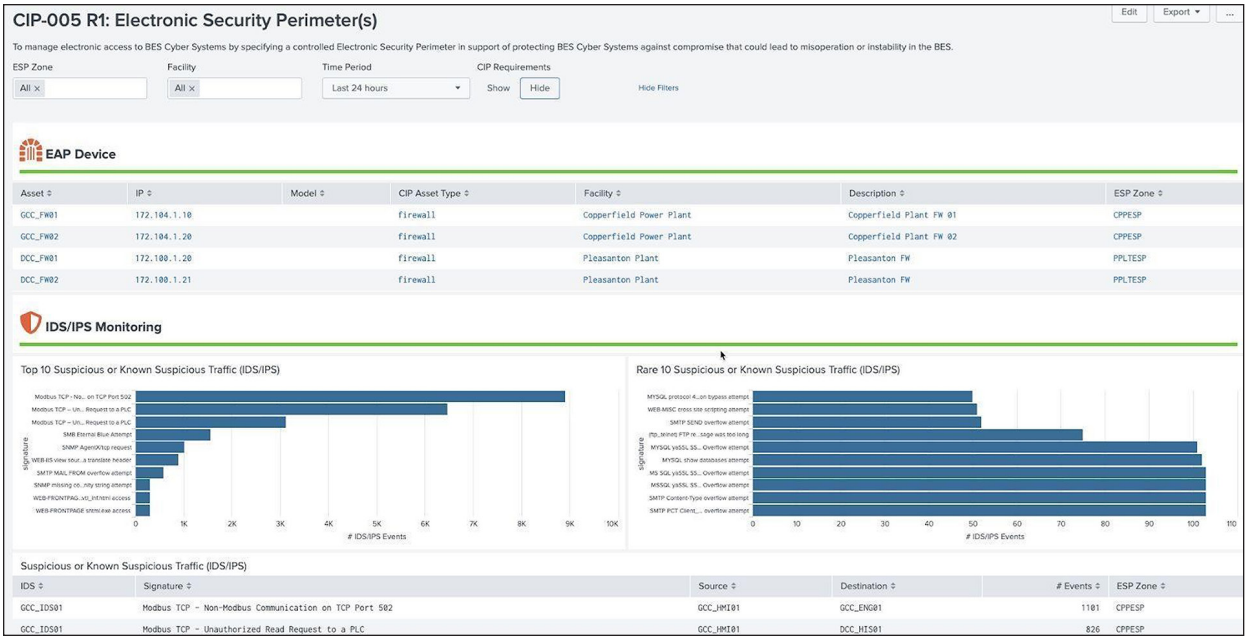

Figure 9. Electronic Security perimeter dashboard example

CIP-007 – System Security Management

The purpose of this requirement is to define methods, processes, and procedures for securing assets within the ESP. Cisco routers, gateways, switches, and firewalls can be used to minimize the attack surface of a utility. Cisco integrated access controls are robust and exceed the mandates for NERC CIP-007.

Whether utilizing the access control features in a Cisco Industrial Router, managed by Catalyst SD-WAN Manager, or the Cisco Secure Firewall, which can be managed centrally by Cisco Secure Firewall Management Center, security administrators are equipped with the means to permit only the communication channels that have deemed to be necessary for operations. To mitigate the threat of malware, the gateways can be deployed with a set of IPS signatures that recognise these signatures and patterns, with new signatures being pushed by their respective management when new packages are made available.

If events do trigger, such as cyber assets attempting to use blocked ports, or malware signatures being matched, all logs will be collected centrally. This allows administrators to deploy their firewalls to multiple parts of the network but maintain a single dashboard for viewing the health of the network.

NERC CIP also calls for security to be extended beyond the firewall, and when using Cisco switching infrastructure, protection against the use of unnecessary physical ports can be put in place. When deploying a large switching infrastructure, it is recommended to use Cisco Catalyst Center so policies can be managed centrally. Catalyst Center also becomes the home for security event monitoring on the switches and can push software patches to the network infrastructure quickly if a vulnerability in the software was to be found. If desired, network port ranges could also be locked down via IP Access Control Lists (ACLs) or Security Group ACLs with Cisco Identity Services Engine.

CIP-007 Reporting with Splunk OT security add-on

CIP-007 requires operators to keep track of the ports and services being used by machines which involves a wide plethora of data sources relevant to these requirements. Not only do the firewalls, routers, switches provide information on ports being used, logs can originate from the machines themselves or events from endpoint protection logs that monitor USB usage. Windows events (current OS) as well as Windows registry (older OS's) also play a role in determining when remote media is being used. The Splunk OT Security Add-On aggregates these logs in a single dashboard.

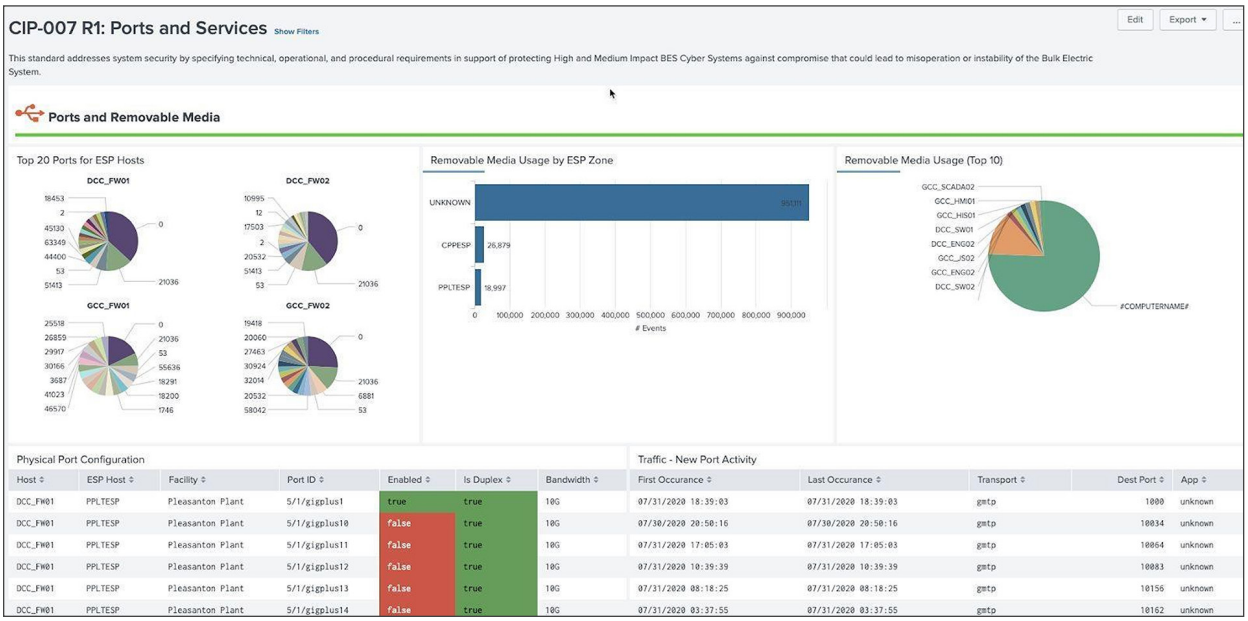

Figure 10. Ports and services dashboard example

In addition to open ports and services, Splunk collects security events and malware alerts to understand threats to the environment. NERC regulations require that logs be kept for at least 90 days and be periodically reviewed, and Splunk retains information for the following dashboards:

- Security patch management (CIP 007 R2)
- Malicious code prevention (CIP 007 R3)
- Security events investigations (CIP 007 R4.1)
- Security event monitoring (CIP 007 R4.2)
- Security log retention (CIP 007 R4.3)
- Summary of events for review (CIP 007 R4.4)
- System access control (CIP 007 R5)

CIP-008 – Incident Reporting and Response Planning

The purpose of this requirement is to mitigate the risk to the reliable operation of the BES as the result of a Cyber Security incident. The detection of an incident can occur in many part of the architecture, such as security events across the firewall, rogue devices connecting to a switch, or Cisco Cyber Vision seeing new communication in a baseline. Incident investigation typically starts with one event, but it is only when multiple sources of information have been correlated together do we get the complete picture.

NERC CIP operators are required to have defined cyber security Incident Response Plans (IRP) that identify how to respond to cyber incidents or violations of NERC CIP regulations. Part of this regulation requires a method to show notable or cyber incidents. This dashboard provides an overview of all the notable alerts that have been generated for NERC CIP regulated assets and is dependent on existing correlation rules built into Splunk Enterprise Security. The status and incident owner of each notable is reported to ensure incidents have been assigned and/or resolved. IRP plans should be reviewed at least yearly and updated and this dashboard provides a method to report on changes to IRP plans.

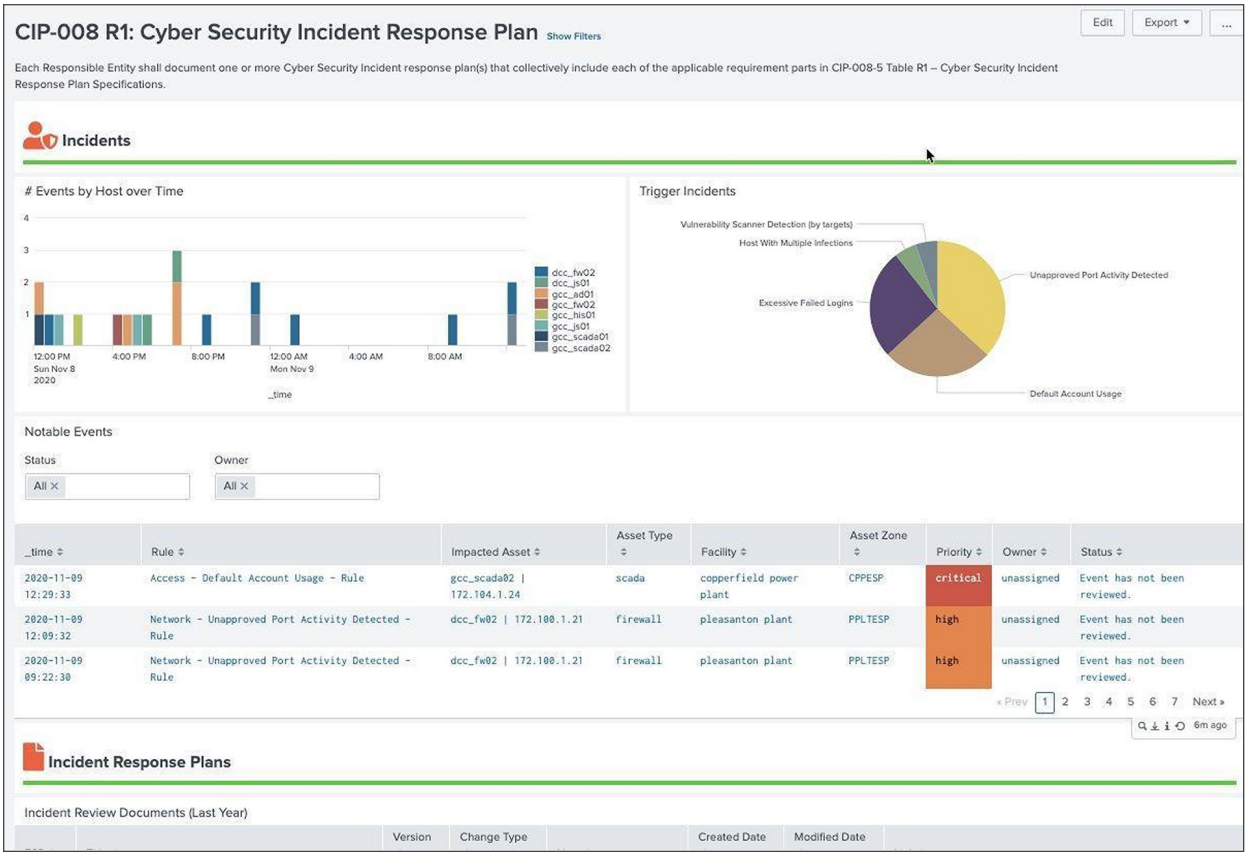

Figure 11. Cyber Security Incident Response Plan dashboard example

CIP-009 – Recovery Plans for BES Cyber Systems

NERC CIP operators are required to ensure their BES Cyber Systems can be restored quickly in case of failure or cyber-attack. This includes monitoring not only the BES Cyber System but also any CIP assets which require backup. Cisco Catalyst Center and Catalyst SD-WAN Manager provide the monitoring and recovery from failure of network equipment.

The management tools are equipped with the necessary resources to detect network outages, or overloaded traffic paths. With the use of device templates, any network failures that do result in a replacement means that these new devices can plug and play back into the infrastructure, inheriting the same configuration that was left behind by the malfunctioning device. Configuration changes should only come from well-known entities within the bounds of the utility, from the control center.

The Splunk OT Security Add-On goes beyond the network equipment and provides information about the Splunk environment, including index retention, clustering, and Splunk features tied to High Availability and Disaster Recovery. This dashboard also brings in data from backup logs to ensure CIP assets are being backed up.

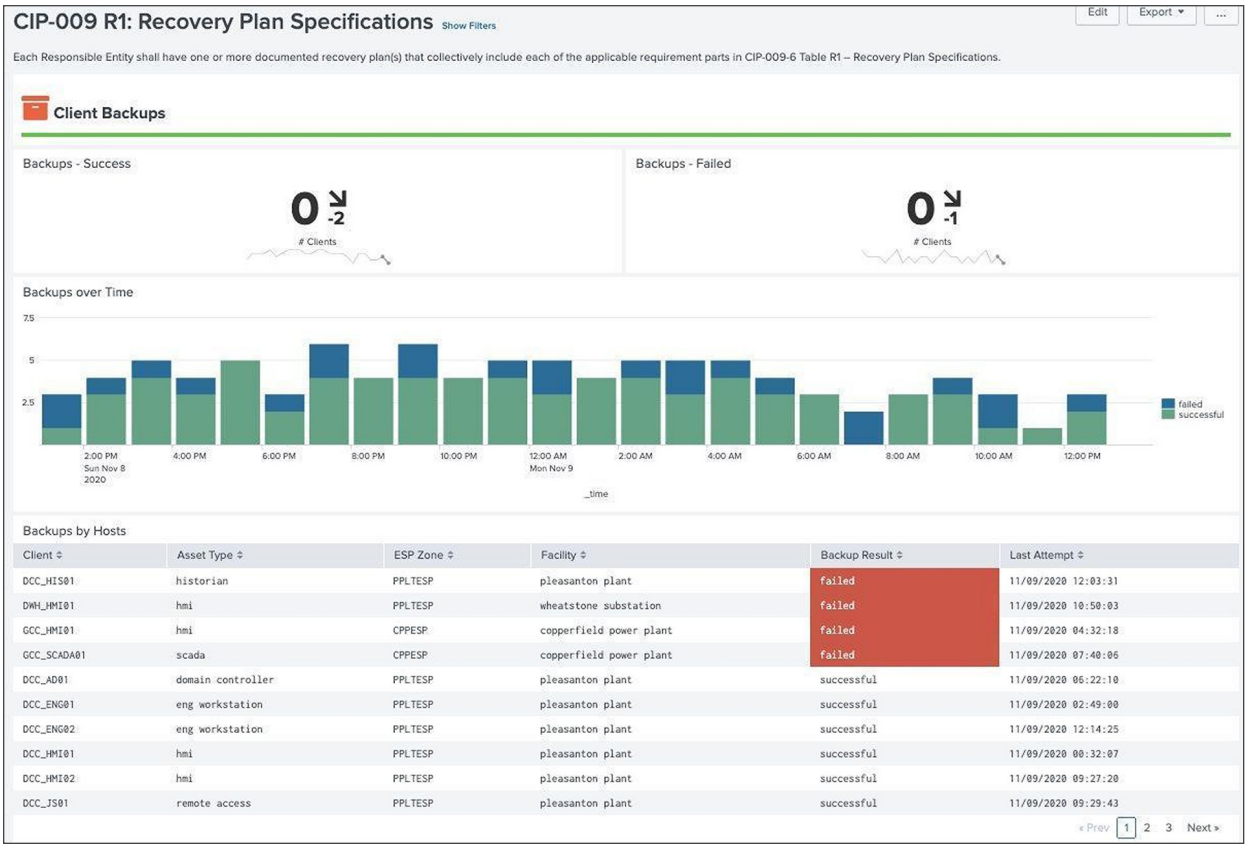

Figure 12. Recovery plan specifications dashboard example

CIP-010 – Configuration Change Management and Vulnerability Assessments

The purpose of this requirement is to prevent and detect unauthorized changed to BES Cyber Systems by specifying change management and vulnerability assessment requirements. Whether it's changing the template configurations in Cisco Catalyst SD-WAN for the Cisco Industrial Routers, or using Cisco Catalyst Center to deploy Cisco Industrial Ethernet Switches, compliance features in both platforms ensure the configurations are either 'locked' or any changes are flagged and offer the ability to push 'golden' configurations back to the devices. Read only access can be provided to users who may need to visualise these changes in the network, with write privileges kept to only those who are qualified to make them.

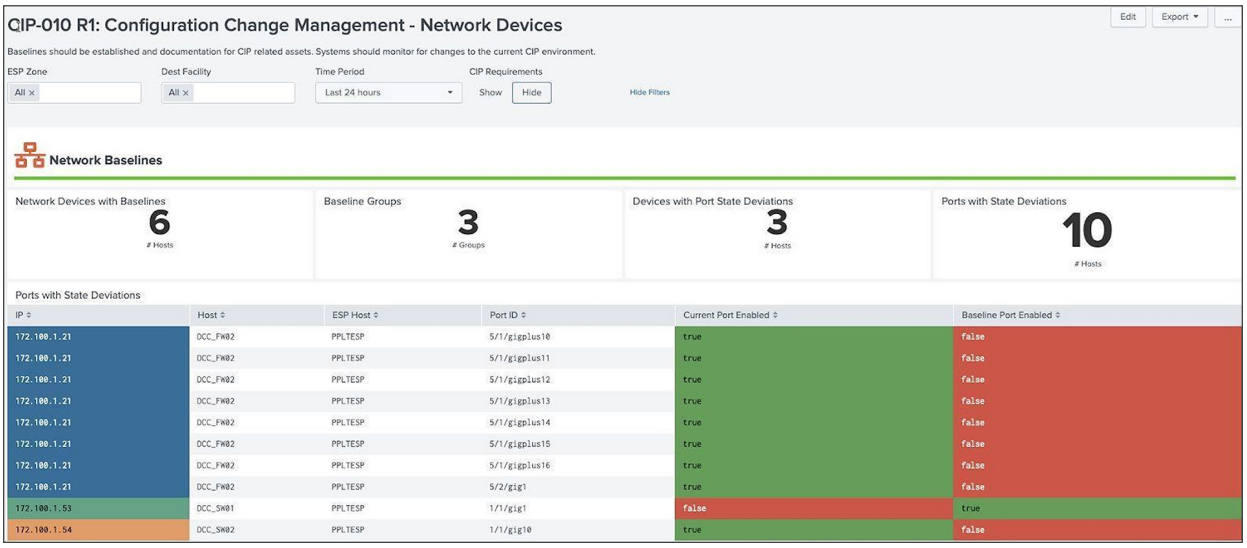

Figure 13. Network baseline dashboard example

Baselining however also applies to the Cyber Assets, not just the network infrastructure. Cyber Vision, which will be used to document the vulnerabilities of the assets, can also be used to monitor a baseline for the network. Any new asset introduced to the network, or any deviations from known communication pattern will be captured, and this new information can either be added to the baseline as an accepted deviation or flagged for investigation.

Baselines can be the result of static configurations (e.g. a list of approved patches) but ideally are generated from data sources. Some good examples of data sources to consider when generating baselines are patching approval systems (such as WSUS), asset information (endpoint protection, Splunk forwarders, etc), installed software inventories, as well networking management systems. The baseline features implemented in Splunk are designed to keep track of baselines so that assets can be reviewed against specific baselines. Keeping these baselines is also required by regulation.

Assets can be grouped together so that assets within a group should match a particular configuration. Currently, computer and network baselines are the only requirement kinds of baselines and each has specific elements which must be baselined. In the case of each Scorecards are designed to identify deviations from the baseline and provide information of how the item deviates from the baseline (for example, software that is installed but not approved) including hosts.

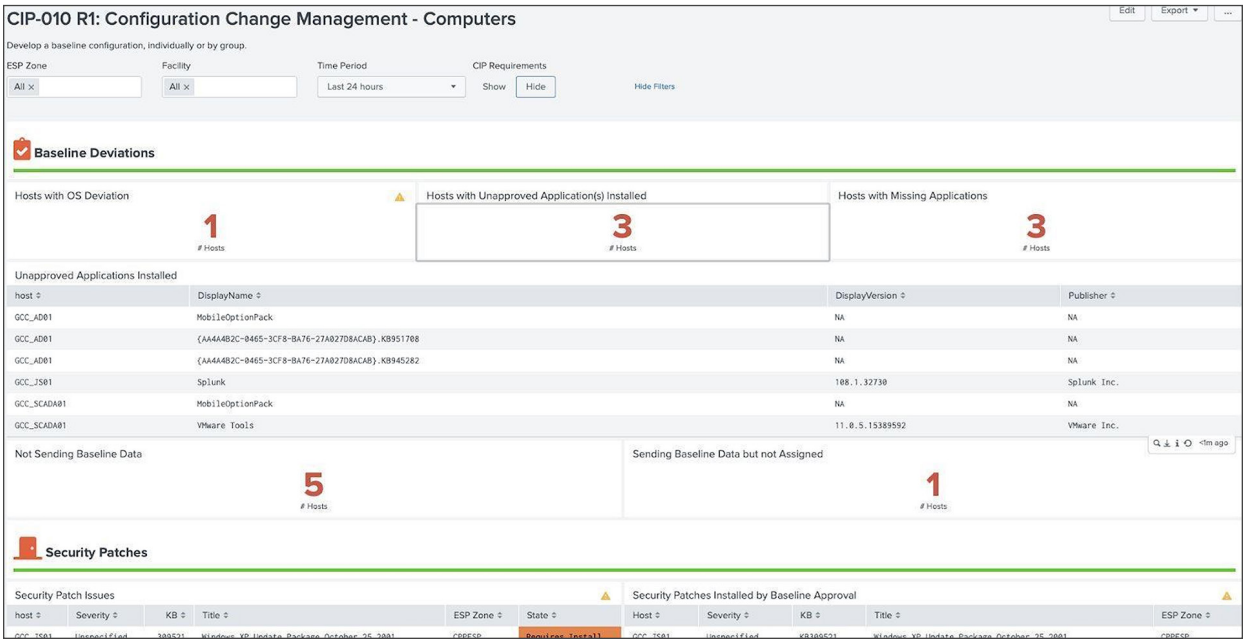

Figure 14. Computer baselines dashboard example

CIP-011 – Information Protection

The purpose of this requirement is to prevent unauthorized access to BES Cyber System information (BCSI). Not only is all access to Cisco technology protected by user access control, but network security policies also deployed through the Cisco network infrastructure will ensure that unauthorized users cannot gain access to the systems. Cisco's recommended architecture defines separate layers of security along the commination's path including micro-segmentation at both the operations center and field networks or substation ESPs. Segmentation for the ESP leveraging MPLS and IPSEC VPNs with firewall rules and Security Group Tags controlling access to and from the network or networks being traversed.

CIP-013 – Supply Chain Risk Management

The purpose of this requirement is to implement security controls for supply chain risk management of BES Cyber Systems. Cisco's Security and Trust Organization defines our secure development lifecycle (Cisco SDL), creates and maintains common security libraries, and manages our PSIRT process and privacy activities across all Cisco product lines.

Engineering teams must comply with the Cisco Software Development Lifecycle (SDL) which is certified for compliance with IEC 62443-4-1. This certification underscores that we maintain a security culture and that our products can be trusted. Some Cisco products also have IEC 62443-4-2 certifications.

The Cisco SDL process ensures security and trustworthiness are designed, built, and delivered from the ground up. Trustworthy technologies such as image signing, secure boot, Cisco Trust Anchor module, and runtime defenses help ensure that the code is authentic, unmodified, and operating as intended. A hardware-level root of trust, unique device identity, and validation of all levels of software during startup establish a chain of trust in the system.

Requirements such as the **notification by the vendor of vendor-identified incidents related to the products or services provided to the Responsible Entity that pose cyber security risk** is handled by the Cisco Product Security Incident Response Team (PSIRT). Cisco PSIRT receives, investigates and publicly reports security vulnerability information related to Cisco products. All product PSIRTs result in the delivery of both patches AND protection and mitigation advice for the period before patches can be applied.

Cisco is also an active contributor to industrial IoT relevant standard work, defining Manufacturer Usage Description (RFC 8520), participating in security standards work for ODVA (CIP/EIP), IEC 62443, IEC 61850, NIST SBOM definitions, et al.

CIP-015 – Internal Network Security Monitoring

A defense-in-depth strategy is one that protects organizations from attacks that bypass the first layer of security controls. It is a well understood concept, and one that has been adopted by most organizations over the years. The latest addition to the CIP standards is CIP-015-1, Internal Network Security Monitoring (INSM), which fixes a regulatory gap where there were no mandatory security controls beyond the network perimeter. If utilities followed NERC CIP, and then went no further, they would be exposed to attacks that bypassed that first layer of defense.

INSM is designed to address those situations where the network perimeter has been breached, increasing the probability of detecting a compromise. By providing visibility within the critical network, entities can be warned that an attack is in process and action can be taken before the attack can propagate.

Identification of assets and their communication patterns

Cisco Cyber Vision, a deep packet inspection engine within Cisco networking equipment, uncovers the smallest details of your infrastructure. It automatically builds a comprehensive inventory of all grid assets, including their communication patterns, vulnerabilities, rack slot configurations, vendor references, serial numbers, and more. By embedding the Cyber Vision sensor within the network infrastructure, Cisco offers comprehensive visibility, capturing data without the need for deploying and managing dedicated security appliances or expensive SPAN cabling.

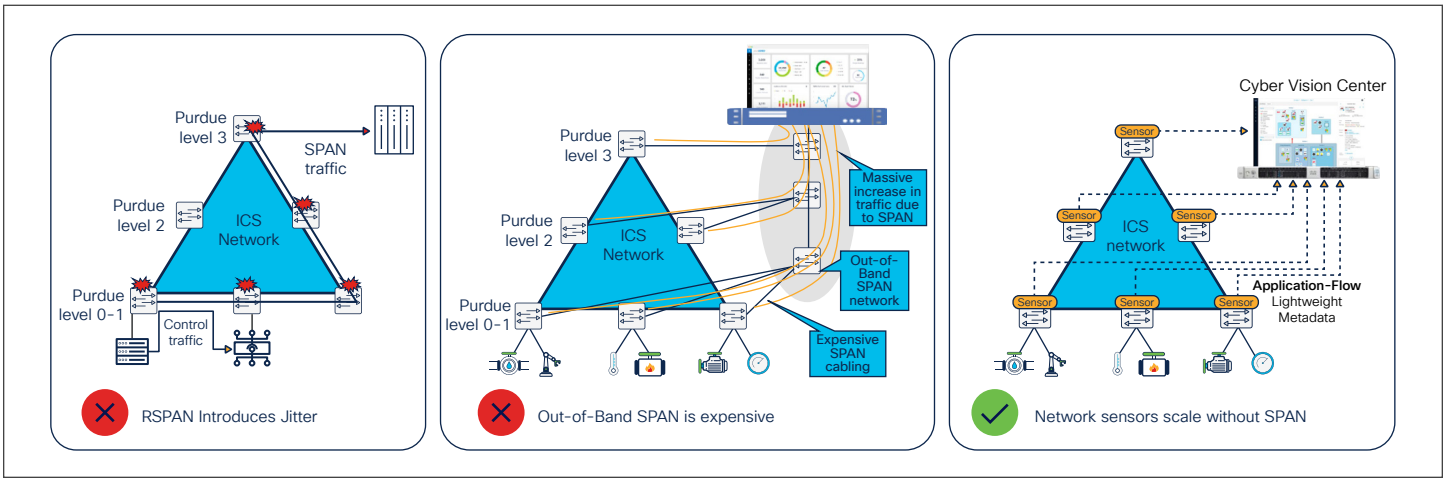

Figure 15. Architectural considerations for OT visibility

INSM calls for collection methods to gain visibility on connected assets and address the perceived risks the infrastructure faces. Cyber Vision applies a risk score to all devices and device groups discovered in the network. Using a combination of vulnerabilities, activities, and impact, risk scores provide users with the **risk-based rationale** requested by CIP-015.

Evaluating the network against an expected network communication baseline

Utility networks, especially the communication with an ESP, are usually quite static. By understanding what is normal for your network, you can more easily spot when something unusual happens. For example, if a device suddenly starts communicating using a different protocol, or has started to communicate with new devices, it might mean a bad actor has compromised the device.

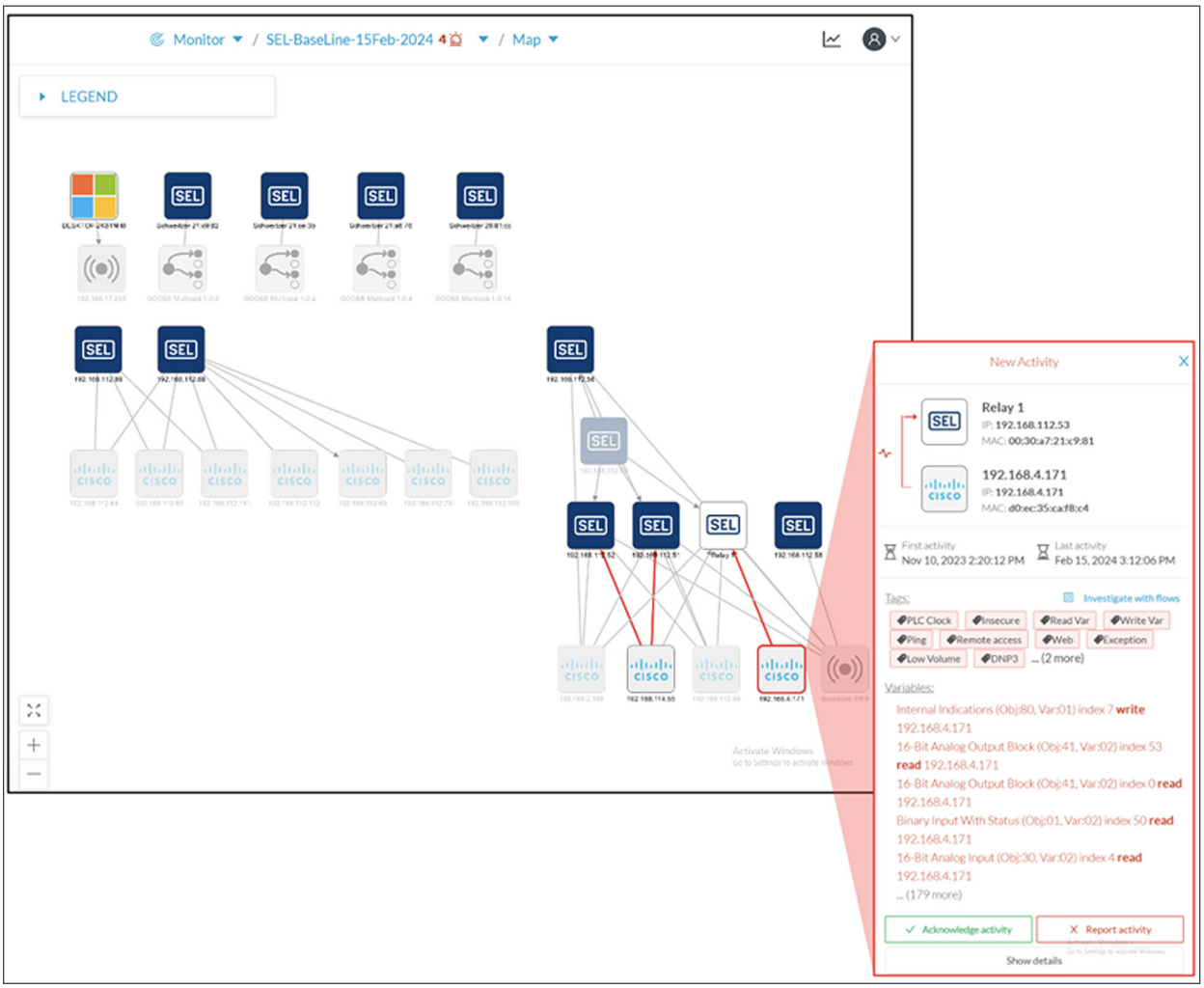

Figure 16. Cisco Cyber Vision in a utility network example

To meet the requirements proposed by NERC, Cyber Vision data can be filtered and saved as a baseline reflecting normal process behaviors. Any deviations will generate an alert. If the deviation was expected, an administrative user can acknowledge and make the new norm part of the baseline. However, if the change was unexpected, it can be reported and sent for further investigation.

Detecting anomalous activities within the ESP

NERC CIP-005-7, the requirements document for cybersecurity across the ESP, requires a mechanism for detecting known or suspected malicious activities for both inbound and outbound communications. Traditionally, this is accomplished by using an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) embedded in a boundary firewall.

With the introduction of INSM, this requirement has been extended for detecting anomalous activity within the ESP. Firewalls as a technology are listed, but will only capture data that crosses the device, leading to difficult architecture choices on where to deploy these boxes.

In addition to its capabilities to detect deviations from a baseline, Cyber Vision leverages Snort to detect malicious traffic within the operational network. Snort is the IDS engine used across the Cisco portfolio and supported by Talos, one of the world's largest private threat intelligence organization and official developer of Snort signature files.

Talos, Cisco's threat intelligence team, continuously monitors the global threat landscape, identifies, and analyses new vulnerabilities, and provides real-time threat intelligence feeds that are tailored to OT systems. Not only does the Talos expertise provide threat intelligence for Cyber Vision, but they also have a team of people dedicated to help secure critical infrastructure. For example, check out this blog by Joe Marshall – Helping to keep the lights on in Ukraine in the face of electronic warfare.

Cisco's industrial security solution

Cisco's industrial security solution provides industrial organizations with a phased approach to securing their operational networks. This approach involved building the foundation with good network design and secure components, using the network to gain visibility across the critical infrastructure, and then finally implementing policy back into the same network infrastructure for preventative and reactionary measures. INSM is one small piece of a larger security strategy, and Cisco provides the building blocks for securing the infrastructure across LAN, WAN and Cloud.

Talk to a Cisco sales representative or channel partner about how Cisco can help you secure your grid network. Visit cisco.com/go/iotsecurity or cisco.com/go/iotutilities to learn more.

C22-5239544-00 09/25