INTERNAL NETWORK SECURITY MONITORING

Leveraging SEL Ecosystem for NERC CIP-015 Compliance

Will Edwards
Schweitzer Engineering Laboratories, Inc.

Introduction

This paper explores methods to design a robust solution for internal network security monitoring, with a secondary objective of mapping these ideas to NERC CIP-015 compliance support. NERC CIP-015 focuses on establishing a process to detect and respond to anomalous or unauthorized activity on the networks protected by the responsible entity's electronic security perimeters (ESP) of high- and medium-impact bulk electric system cyber systems with external routable connectivity. The three requirements of CIP-015 are as follows.

R1

Responsible entities must implement one or more documented processes for internal network security monitoring. These processes should include:

- A risk-based approach to defining network data feeds, which are used to monitor network activity, including connections, devices, and communications.
- Methods for detecting anomalous network activity using the defined network data feeds.
- Methods for evaluating detected anomalous activity to determine further actions, such as documentation of response actions or escalation processes.

R2

Responsible entities, except during CIP exceptional circumstances, must implement one or more documented processes for retaining internal network security monitoring data associated with anomalous network activity. These data should be retained at least until actions related to the anomaly, as defined in R1, are complete.

R3

Responsible entities, except during CIP exceptional circumstances, must implement one or more documented processes for protecting the internal network security monitoring data collected and retained under requirements R1 and R2. These processes should mitigate the risks of unauthorized deletion or modification of these data.

Objective Overview

CIP-015 requires a plan with methods for defining traffic to monitor and methods for detecting and evaluating anomalies. These requirements leave a lot of flexibility for entities to decide how they want to comply. While the common opinion is that an intrusion detection system (IDS) will satisfy the requirements, we suggest that you develop your strategy based upon the root of the standards objective to reduce the risk of operational impact from adversaries. With this perspective, it makes sense to prioritize understanding your operational technology (OT) baselines and protecting against unauthorized devices and traffic. This approach provides the best foundation for detecting anomalous activity.

Improved internal network security monitoring requires a combination of technology and processes to achieve maximum defense benefits. It should be noted, unlike the National Institute of Standards and Technology (NIST) Cybersecurity Framework (identify, protect, detect, respond, and recover), CIP-015 primarily focuses on the detection and response components of risk mitigation. This paper will discuss protection aspects of solution consideration.

R1 explicitly addresses the need for enhanced security inside of the ESP; therefore, the capabilities of WAN and edge security are not relevant. The internal network for industrial control systems (ICSs) is traditionally composed of IEDs, network switches, remote terminal units (RTUs), and automation software. The network traffic associated with these technologies is what needs to be monitored for anomalous activity. From a solution perspective, it is important to consider how the addition of an IDS can be complemented by understanding the native capabilities of existing components.

For an SEL ecosystem, the Real-Time Automation Controller (RTAC), software-defined networking (SDN), and SEL Blueframe® Data Management and Automation (DMA) application suite can contribute to meeting CIP-015 internal network security monitoring requirements. Strategies and considerations for each component will be discussed in more detail.

Network Overview

Figure 1 shows a simplified diagram for the internal network. This architecture, along with proper device configuration, eliminates much of the potential attack surface associated with integrating remote signals into an ICS network. Network data feeds subject to CIP-015 consideration include traffic, such as data collection for SCADA, protection signals between IEDs, asset management monitoring, and local engineering access. The following sections provide a detailed explanation of the specific cybersecurity controls that manage risk.

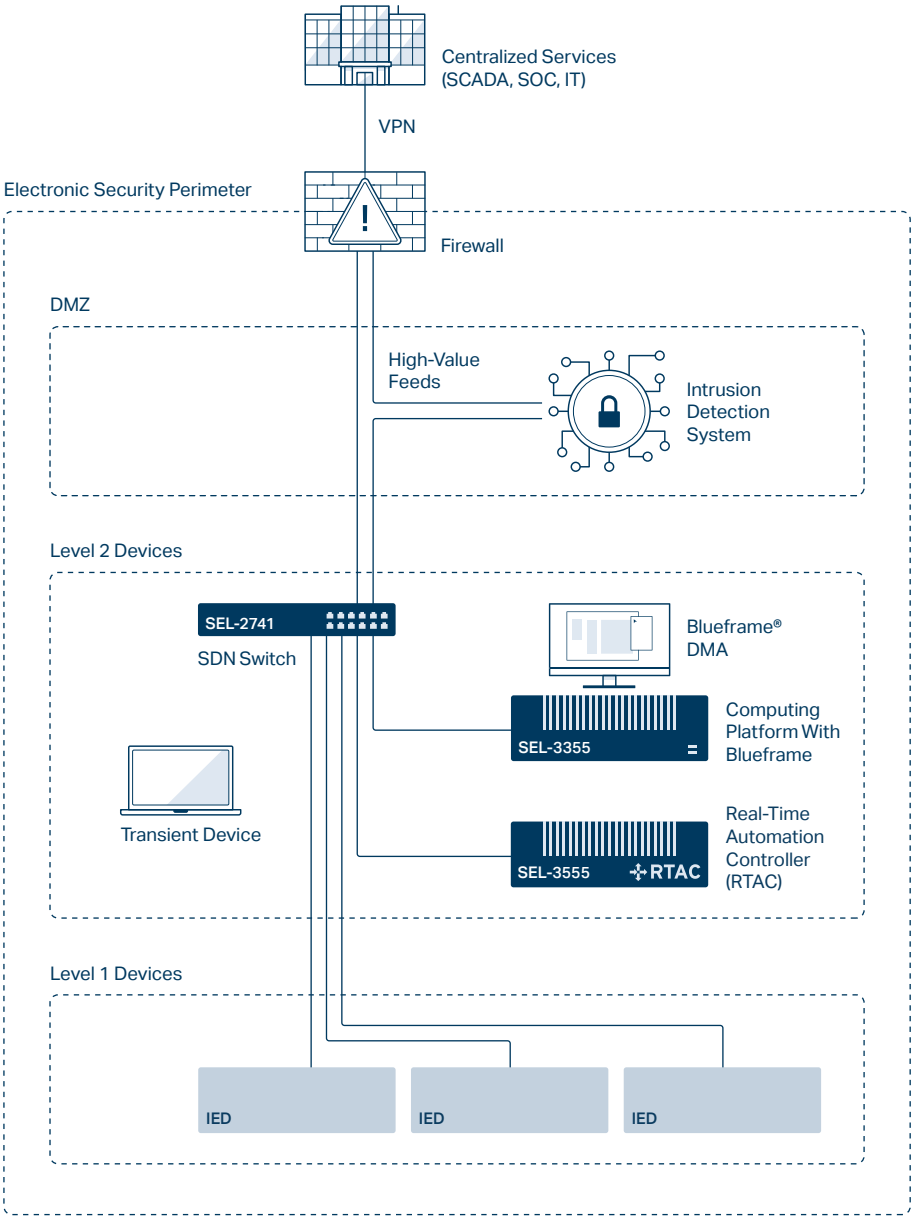

Figure 1—Simplified Network Architecture

1. Risk-Based Approach to Defining Network Data Feeds

SDN

OT SDN, by design, enforces dataflow baselines for internal networks. All unauthorized traffic is blocked by default. Network data feeds for monitoring can be granularly defined. The logical nature of software-defined networks allows for optimization of IDS sensor deployments due to the elimination of data feed ingests needing to have physical connections to each switch. SDN deny-by-default access control directly addresses R1.1 (network data feeds) by enforcing data flow baselines and blocking unauthorized traffic.

2. Anomalous Activity Detection

IDS

Beyond indicators of compromise, most vendor technologies for intrusion detection include capabilities for time-series correlation of activity that can be used for detection of threat activity.

- Comprehensive visibility through a diverse set of network, endpoint, and wireless sensors, ensuring complete monitoring across industrial environments.
- Advanced threat detection leveraging AI-driven analytics to identify vulnerabilities, anomalies, and active cyber threats at scale.
- Intelligent security insights with clear, customizable, and actionable insights into the security posture of individual assets, zones, sites, and sensors and the ability to benchmark security performance and track improvements over time.
- Advanced threat intelligence to understand and investigate threat actor activity within a network, enabling rapid investigation and response to threats.

RTAC

The RTAC can be configured to monitor various communication protocols, enabling it to detect anomalies in data traffic patterns from connected devices like IEDs and other RTUs.

- Example: The Comm Monitor tool in the RTAC allows for capturing and analyzing data from DNP3, Modbus, and SEL protocols. This helps identify unusual communication patterns indicative of potential attacks or misconfigurations.
- Network Event Capture: Further, the RTAC Network Event Capture feature allows for recording network traffic based on predefined triggers, providing valuable forensic data for investigating security events. Monitoring Syslog and SNMP messages (e.g., the switch port went down) can be used to trigger network event captures via the logic engine.
- Network Audit: The RTAC Network Audit feature provides several methods for auditing the network, including:
  - Targeting—Allows targeting of a single host, multiple hosts, or an entire network.
  - Host Discovery—Identifies devices on the network for verification against system baselines.
  - Port Scanning—Reports each open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) port for each host listed or discovered.
  - Results Storage—Audit results are stored in the AUDITS directory on the RTAC file manager.
  - Application Programming Interface (API) Access—The Network API can be used to trigger a network audit and retrieve the results.
  - Web Interface—Network audits can be initiated and collected on the RTAC web interface.
  - Logic Engine—Network audits can be initiated and collected via the RTAC logic engine.

SDN

OT SDN, with its deny-by-default, zero-trust approach, allows for granular control over network traffic. By defining strict flow rules based on device roles and expected communication patterns, SDN can effectively detect and block any deviations, including potential malicious activities. OT SDN also allows you to send unauthorized traffic to a place it can be securely retained for analysis and archiving purposes, as R2 and R3 require. This can be network attached storage, a collection computer, or desired sensor solutions.

- Traffic Metering: In SDN, traffic meters are virtual devices implemented in the SDN controller. They are used to measure and control the rate of network traffic flowing through specific network paths or for specific applications.
- Metering Rules: The SDN controller configures traffic meters with a set of rules that define:
  - Traffic to Measure—The specific traffic flows that need to be measured, typically based on source and destination IP addresses, ports, or protocols.
  - Rate Limits—The maximum allowed rate of traffic for the defined flows. This can be expressed in bits per second (bps), packets per second (pps), or other units.
  - Actions—The actions to be taken when the traffic rate exceeds the defined limits. This can include dropping packets, marking packets for lower priority, or generating alerts.
- Monitoring and Enforcement: The SDN switches, managed by the controller, monitor traffic flows and apply the configured meter rules. If a traffic flow exceeds its defined rate limit, the switch takes the specified action.
- Applications: Traffic meters are used for various purposes in SDN, including:
  - Quality of Service (QoS)—Ensuring high-priority traffic gets adequate bandwidth.
  - Rate Limiting—Preventing network congestion or denial-of-service (DoS) attacks.
  - Traffic Shaping—Smoothing out bursts of traffic for better network performance.
- Deep Packet Inspection: The multilayer packet inspection capability (Layers 1–4) of OT SDN enables detailed analysis of network traffic, enhancing the detection of suspicious or unauthorized communications.

BLUEFRAME DMA

The Blueframe platform provides access to security logs and events. Security alerts, such as Syslog, can be aggregated and forwarded to other security appliances. DMA aids in R2 (data retention) with its data-archiving capabilities. This includes the ability to collect network event captures and other reports from RTACs. All local engineering access can be proxied through Blueframe to further reduce the attack surface.

3. Unauthorized Activity Detection

RTAC SECURE AUTHENTICATION

Features such as security logging and DoS attack monitoring can alert users about unauthorized activity, such as failed connection attempts, settings changes, and user account edits. If the RTAC or Blueframe node acts as the electronic access point, this simplifies monitoring of unauthorized activity.

ALERTING

The RTAC and Blueframe support Syslog integration with security information and event management (SIEM) systems.

USER MANAGEMENT

The RTAC and Blueframe support user accounts with configurable roles and permissions, limiting access to specific functionalities based on user privileges.

SDN ZERO-TRUST MODEL

The OT SDN zero-trust model enforces strict access control. Devices are only allowed to communicate with authorized endpoints, effectively preventing unauthorized access attempts.

CENTRALIZED CONTROL

A secure control plane in OT SDN enables centralized management and monitoring of network access policies, ensuring consistent enforcement of security rules across the network.

BLUEFRAME CENTRAL AUTHENTICATION

The Blueframe platform supports central authentication using the Lightweight Directory Access Protocol (LDAP) or Remote Authentication Dial-In User Service (RADIUS), providing a centralized mechanism for managing user access and permissions across the Blueframe ecosystem, including DMA. The RTAC or Blueframe contribute to R3 (data protection) through secure communication protocols and access controls.

CREDENTIAL MANAGEMENT

The Credential Management features in Blueframe DMA offer controlled password management for various resources, reducing the risk of unauthorized access due to weak or compromised credentials.

4. Facilitating Response and Recovery

RTAC EVENT LOGGING

The RTAC's comprehensive event logging capabilities, including Sequence of Events recording and Syslog, provide crucial information for analyzing security incidents, understanding the attack vectors, and initiating appropriate responses.

DIAGNOSTIC TOOLS

The RTAC offers various diagnostic tools, such as the online packet dissector and network utilities, that aid in troubleshooting communication issues and identifying the root cause of security events.

SDN FAST NETWORK HEALING

The rapid network-healing capability (submillisecond) of OT SDN minimizes the impact of network disruptions, ensuring the availability of critical systems during and after a security incident.

CENTRALIZED CONTROL

SDN centralized control allows for swift adjustments to network configurations and security policies, facilitating rapid response and recovery efforts.

BLUEFRAME DMA DATA ARCHIVING AND RETRIEVAL

DMA's data-archiving and retrieval mechanisms, accessible via an integrated archive tool or RESTful interface, can be utilized to recover critical data and system configurations in case of a security breach. This API can also aid in the "enrichment" of enterprise tools, such as IDS, asset management and workflow ticketing systems.

Conclusion

Compliance with CIP-015 can be accomplished in many ways and will best serve a critical-infrastructure entity if they take the time to plan for success. Consider scenarios like:

- Detecting a malware infection on an IED through unusual network traffic patterns.
- Identifying unauthorized access attempts using SDN access control logs.
- Responding to a DoS attack by isolating the affected network segment with SDN.
- Utilizing DMA to analyze historical data and identify compromised devices.
- Detecting an unauthorized settings change on an IED.

All of these scenarios can be accomplished with an ecosystem that includes SDN, the RTAC, and Blueframe applications. A purpose-built OT IDS would further complement detection capabilities for customers that incorporate a staffing and training component to their strategy.

Training and staffing are not usually the first components of compliance strategy; however, they become obvious needs as system changes are implemented. Many customers recognize that their organization has limited experience with OT threat analysis and utilize SEL Cyber Services to help align their strategy with industry best practices and to augment their staff for enhanced monitoring and response to maximize return on investment. SEL Cyber Services provides:

- Unrivaled expertise in regulatory frameworks, such as NERC CIP, IEC 62443, NIST Risk Management Framework, and the SOCI Act, ensuring compliance and risk reduction.
- Comprehensive cybersecurity services, including network design, incident response, and lifecycle security management for industrial and utility environments.
- Turnkey deployment and integration services, seamlessly incorporating IDS solutions with existing security architectures to exceed regulatory requirements.

NIST Cybersecurity Framework

SEL serves many industries, including datacenters, oil and gas, mining, nuclear, water and wastewater, and power generation, transmission, and distribution. We work closely with our customers and cross-functional teams to best understand our customer's security requirements and develop a project-specific security plan.

Our standard approach is to use the NIST Cybersecurity Framework, which focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes.

The six Cybersecurity Framework core functions are shown in Figure 2. These functions are not intended to form a serial path or lead to a static desired end state. Rather, the functions should be performed concurrently and continuously to form an operational culture that addresses the dynamic cybersecurity risk. One of the keys to successfully thwarting attacks is the speed to detect, isolate, and mitigate.

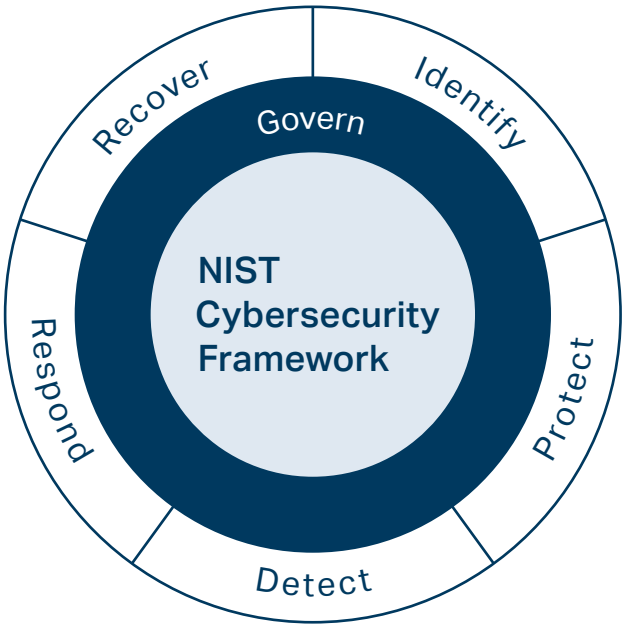

Figure 2: NIST Cybersecurity Framework

The SEL Cyber Services team is diverse in its understanding of the importance of operational, technical, natural, physical, environmental, and human cyber risks to all aspects of an energy control system.

The SEL Cyber Services team holds many accreditations in security, project management, and quality, including the following specific disciplines.

INFORMATION SECURITY

Certified Information System Security Professional (CISSP), Global Information Assurance Certification (GIAC) Response and Industrial Defense (GRID), GIAC Security Essentials Certification (GSEC), GIAC Certified Incident Handler (GCIH), Global Industrial Cybersecurity Professional (GICSP), GIAC Critical Infrastructure Protection (GCIP), GIAC Certified Intrusion Analyst (GCIA), GIAC Defensible Security Architecture (GDSA), GIAC Critical Control Certification (GCCC), SANS Security Awareness Professional (SSAP), Cisco Certified Network Associate (CCNA) Routing and Switching, Computing Technology Industry Association (CompTIA) A+, CompTIA Network+, CompTIA Security+, CompTIA IT Operations Specialist, CompTIA Secure Infrastructure Specialist, and CompTIA Cybersecurity Analyst (CySA+).

PROJECT MANAGEMENT

Accreditation under Project Management Institute Project Management Professional (PMI PMP), GIAC Certified Project Manager (GCPM), and Information Systems Audit and Control Association (ISACA) Certified in Risk and Information Systems Control (CRISC).

ASSURANCE AND AUDITING

Accreditation under ISACA Certified Information Systems Auditor (CISA) and present accreditation under GIAC Systems and Network Auditor (GSNA). SEL ES holds other International Organization for Standardization (ISO) certifications regarding quality and auditing.

SCHWEITZER ENGINEERING LABORATORIES

info@selinc.com	selinc.com	+1.509.332.1890	20250220