NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-015-1

CIP-015-1 – Cyber Security – Internal Network Security Monitoring

Introduction

This document explains the technical rationale and justification for the proposed Reliability Standard CIP-015-1. It also clarifies for Responsible Entities what Internal Network Security Monitoring (INSM) systems are and the original intent of the Drafting Team (DT). This technical rationale document for CIP-015-1 is not a reliability standard and should not be considered mandatory and enforceable.

Background

On January 19, 2023, the Federal Energy Regulatory Commission (FERC) issued Order No. 887[1] directing NERC to develop requirements within the Critical Infrastructure Protection (CIP) Reliability Standards for INSM of all high-impact Bulk Electric System (BES) Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity (ERC). INSM permits Responsible Entities to monitor traffic within a trusted zone, such as the Electronic Security Perimeter (ESP), to detect intrusions or malicious activity. Specifically, Order No. 887 directs NERC to develop Reliability Standards requirements for any new or modified CIP Reliability Standards that address three security objectives.[2] In Order No. 887, FERC directed NERC to submit these revisions for approval within 15 months of the final rule's effective date, i.e., July 9, 2024.

Summary

Network Security Monitoring (NSM) is a set of practices and processes implemented by organizations to monitor and protect their internal networks and systems from potential security threats. It involves persistent collection and analysis of network communications, application logs, operating system logs, device logs, and other security logs from an organization's internal network infrastructure and devices.

INSM is a subset of NSM and refers specifically to collection and analysis of network communications within a "trust zone," such as an ESP. INSM includes monitoring of networks that are internal to the

[1] *Internal Network Security Monitoring for High and Medium Impact Bulk Electric System Cyber Systems*, Order No. 887, 182 FERC ¶ 61,021 (2023).

[2] Any new or modified CIP Reliability Standards should address the following three security objectives: (1) the need for responsible entities to develop baselines of their network traffic inside their CIP-networked environment; (2) the need for responsible entities to monitor for and detect unauthorized activity, connections, devices, and software inside the CIP-networked environment; and (3) require responsible entities to identify anomalous activity to a high level of confidence by logging network traffic, maintaining logs and other data collected regarding network traffic, and implementing measures to minimize the likelihood of an attacker removing evidence of their tactics, techniques, and procedures from compromised devices. *Id.* P 5.

operational zones of the Responsible Entity. While the Responsible Entities may choose to use NSM systems to monitor other networks, such as corporate internet perimeters, corporate networks, or associated Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) networks, these requirements apply only to network communications between devices that are protected by the ESP of applicable BES Cyber Systems.

Reliability Standard CIP-015-1 requires Responsible Entities to implement INSM systems and processes. Responsible Entities must evaluate their networks within ESPs and identify the network data feed(s) that would be most effective for detecting anomalous activity in their particular network configurations. Responsible Entities will be required to collect, analyze, and respond appropriately to anomalous network communications within applicable networks. Responsible Entities must evaluate and escalate these anomalous activity occurrences, if appropriate, for further investigation. Subsequent investigation could include escalation to a Responsible Entity's CIP-008 Cyber Security Incident Reporting and Response Planning process(es) if the anomalous activity being investigated may be related to an actual Cyber Security Incident that meets the definition in the NERC Glossary of Terms[3].

Responsible Entities must also appropriately protect the collected INSM related network communications data to prevent unauthorized data manipulation and preserve the data as needed to facilitate additional investigation. INSM will be an on-going, or possibly an iterative, process enabling Responsible Entities to actively identify, mitigate, and escalate potentially threatening actions before they are allowed to impact the reliable operation of the BES.

General Considerations

Summary

The DT considered several options regarding the addition of INSM requirements to the CIP standards' framework. The options included addition of INSM to an existing standard, or addition of an entirely new standard. To inform this decision, the team primarily considered Order No. 887, schedule expectations, and fundamental principles of NSM as detailed in books such as: Richard Bejtlich's book, *The Practice of Network Security Monitoring*[4] and *Applied Network Security Monitoring* by Chris Sanders and Jason Smith, and E.J. Koh[5].

Creation of new Standard CIP-015

At the start of Project 2023-03 – INSM, the DT held discussions on the possibility of creating a new reliability standard or revising existing reliability standards; specifically focusing on Reliability Standard CIP-005 - Electronic Security Perimeter and Reliability Standard CIP-007 – System Security Management. After careful consideration, the DT concluded that Reliability Standard CIP-005 may not be suitable, as its primary focus is the establishment of the ESP and the network communications into and out of the ESP. In

[3] NERC Glossary of Terms
[4] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.
[5] Sanders, C., Smith, J., and Koh, E.J.; Applied Network Security Monitoring: Collection, Detection, and Analysis; Syngress Publishing; December 2013.

addition, Project 2016-06 was making modifications to Reliability Standard CIP-005 to align with zero trust approaches.

Regarding Reliability Standard CIP-007, the DT observed some similarities in logging and alerting, as outlined in Requirement R4 of CIP-007. However, after the initial posting and the subsequent stakeholder feedback received, it became apparent that Reliability Standard CIP-007 may not align with the DT's objectives. Reliability Standard CIP-007 primarily addresses security controls-specific BES Cyber Systems and associated EACMS, PACS, and Protected Cyber Assets (PCA), which does not align perfectly with the scope of INSM, as the focus of the DT lies on the data communicated within the networks containing BES Cyber Systems.

Based on the feedback received during the initial posting, and to ensure maximum flexibility for future modifications if needed, the DT decided to create a new reliability standard, designated as Reliability Standard CIP-015-1. This revised approach is clearer to the objective of detecting and evaluating anomalous network activity.

INSM of Networks Protected by the Responsible Entity's ESP

It is important to highlight the influence of FERC Order No. 887, which played a significant role in the development of these drafts. FERC Order No. 887 specifically mentioned the term "CIP-network environment" for all its applicability to high impact BES Cyber Systems, including medium impact BES Cyber Systems with external routable connectivity. However, it should be noted that the term "CIP-network environment" remains undefined in both FERC Order No. 887 and the NERC defined terms. Furthermore, the directive of FERC Order No. 887 did not explicitly reference associated EACMS or PACS, which could be located outside of the ESP.

In the initial posting, the DT attempted to incorporate certain types of network data within the INSM requirements, including EACMS and PACS associated with in-scope BES Cyber Systems residing outside the ESP. However, after careful consideration, the DT unanimously decided to change its approach to INSM for networks protected by the Responsible Entity's ESP(s) of high impact BES Cyber Systems (BCS) and medium impact BCS with external routable connectivity.

The decision to revise the approach was influenced by several important factors: first, the lack of a clear definition for the term "CIP-network environment" and the absence of specific reference within FERC Order No. 887 regarding the inclusion of EACMS and PACS outside of the ESP created ambiguity. Second, the feedback from industry received during the initial comment period overwhelmingly demonstrated that industry's broad interpretation of FERC Order No. 887 was that it does not include EACMS and PACS outside of the ESP within the scope. Lastly, it should be noted that Reliability Standard CIP-002 identifies BES Cyber Systems as those systems that have a 15-minute impact on the reliability of the BES, and existing requirements in Reliability Standard CIP-005 already address the detection of known or suspected malicious communications for both inbound and outbound communications via the Electronic Access Points (EAP) to the ESP. In addition, the DT agreed with comments received that focusing on the network data flows within the ESP provides the greatest benefit to reliability of the BES and that requiring inclusion of EACMS and PACS outside of the ESP could ignore more cost-effective alternatives to further protecting

reliability. In consideration of these factors, the revised approach devised by the DT will effectively address the key risks outlined in FERC Order No. 887 with respect to the BES.

System Classification
The Responsible Entity's existing process(es) should be referenced to determine if the INSM system and its components are PCA, EACMS, or exempted from applying protections other than those required for BES Cyber System Information (BCSI) protection.

INSM
The goal of INSM is to detect adversarial activity. INSM technologies are most meaningful and effective when they are built to be industrial control system (ICS) protocol aware and provide detections of network activity that might hamper an industrial process. INSM is commonly implemented as a detective (passive) control that assists in finding and responding to adversarial activity rather than a preventative control that blocks suspicious activity. INSM systems may be combined with other detective controls and may also integrate with preventative controls, such as endpoint detection and response. By itself, INSM is not expected to prevent any network or endpoint activity, and many current products are specifically designed as passive monitors to nearly eliminate the likelihood of negative impact to operational systems. While a Responsible Entity may choose to implement active prevention measures in an INSM system or they may have a Software Defined Network (SDN) that provides this capability, prevention is not required in Reliability Standard CIP-015-1.

Rationale for Requirement R1

Requirement:

> *Each Responsible Entity shall implement one or more documented process(es) for internal network security monitoring of networks protected by the Responsible Entity's Electronic Security Perimeter(s) of high impact BES Cyber Systems and medium impact BES Cyber Systems with External Routable Connectivity to provide methods for detecting and evaluating anomalous network activity.*

Summary
Mature security monitoring programs commonly include the capability of monitoring network traffic to provide a layer of visibility that is not available using endpoint logs and other device logs. Requirement R1 requires Responsible Entities to collect and monitor network communications within ESP environments.

Requirement R1 and Parts 1.1., 1.2., and 1.3. specify that Responsible Entities create a documented process for collecting and analyzing network traffic. This process is expected to result in an INSM system and associated processes that will be used by the Responsible Entity for network monitoring purposes.

Rationale for Requirement R1 Part 1.1

> *Requirement R1, Part 1.1: "*Implement, using a risk-based rationale, network data feed(s) to monitor network activity; including connections, devices, and network communications."

As described in Richard Bejtlich's book, "The Practice of Network Security Monitoring", monitoring is most effective when collection is implemented at strategic network locations (Chapter 2) and utilizes a variety of methods (Chapters 9-11). In "Applied Network Security Monitoring" (Chris Sanders, Jason Smith), the "Applied Collection Framework" is described wherein Responsible Entities first identify broad data feeds and then narrow the focus to collect the data that provides the highest benefit. Requirement R1, Part 1.1. specifies that the Responsible Entity identify possible network data collection locations and then narrow the actual collected data to the data feeds that contain the most cost-effective and relevant data for cyber security monitoring purposes.

A risk-based rationale for excluding collection of some network data could include any method for prioritizing collection of data feeds including: a risk analysis, an impact analysis, an analysis of common adversarial techniques, and more. In addition to risk analysis, a Responsible Entity might evaluate network traffic and exclude some data feeds to reduce duplication of collected network data or to focus collection on network data that is most pertinent to cyber security by excluding network traffic with low value such as network traffic related to backups.

The DT found that it would be untenable to develop detailed and specific requirements that would address data collection for all existing networks and technologies. Instead, Requirement R1, Part 1.1. requires that Responsible Entities evaluate their ESP networks and select and implement one or more INSM network data feed(s) in each ESP. These data feeds provide the necessary data to implement Requirement R1, Parts 1.2. and 1.3. Requirement R1, Part 1.1. allows Responsible Entities latitude to select network data feeds that provide value based on a Responsible Entity's evaluation of the network cyber security risk in their internal networks.

Network Data Feeds

A network data feed is the combination of a data collection location and a data collection method. Collection methods are technologies that provide visibility of network data to an INSM system (examples are provided below). In context of Reliability Standard CIP-015-1, network locations are physical or virtual devices that move data on a network. These devices include switches, virtual switches, firewalls, routers, network interfaces and similar devices.

Data Collection Locations

Data collection locations may be a physical or a logical concept. In a physical context, network data collection locations connote data collection from devices that move data within and between networks such as switches, routers, and firewalls. A physical location might include a network port or a cable. A logical collection location might include a virtual local area network (VLAN), virtual switch, virtual private routed network, or any similar concept in an SDN.

An example collection location is a switch (physical) that utilizes VLANs (logical) to provide network segmentation. The Responsible Entity could connect to a physical port on the switch and configure the switch to mirror traffic from all or some VLANs to a collector. A Responsible Entity may identify a core switch as an ideal physical collection point, and then further narrow traffic collection by excluding VLAN traffic with low cyber security monitoring value from the collection system. In another example, the

Responsible Entity may identify physical traffic to and from a specific operational host, such as a Human Machine Interface (HMI), and then narrow the collection of traffic from that host by filtering out backup traffic so that analysts can focus monitoring on the ICS protocol communication between the HMI and other operational systems.

Data Collection Methods

The following table outlines some considerations for data collection for several common methods:

Method	Comments
Network test access point (TAPs) (physical devices)	Additional Hardware Required. Device failure scenarios are unknown to some vendors. Deployment usually requires outages. Can collect 100% of packets. Good fit in centralized environments. Collects layer 2 and layer 3 communications. Probably doesn't require ERC.
Mirror ports **Switch Port Analyzer (SPAN) ports** **Virtual Mirror ports (in a hypervisor)**	Little hardware required (although Responsible Entities will likely install network aggregators). No outage required to enable. Vendor experience and support varies. Good fit in centralized environments. Will increase processor utilization on layer 2 switches. Some (minimal) packet loss is expected. Collects layer 2 and layer 3 communications. Most mirror/SPAN ports pass data as not ERC and, therefore, may not need to traverse an Electronic Access Point (EAP).
Network Flow (NetFlow, sFlow, IPFIX, jflow, NetStream, Cflowd, etc.)	No hardware costs for forwarding. Good fit in distributed environments. Good fit in low bandwidth environments. Proprietary protocols vary per vendor. Layer 2 collection capabilities differ by vendor. Collects layer 3 communications. Sampled NetFlow may be an option. Does not include payload data. Can be generated by Switches, routers, and firewalls. Probably requires ERC.
RSPAN (remote SPAN)	Collection is similar to Network Flow. Requires higher bandwidth. Can Collect layer 2 traffic. Includes data payload. Probably requires ERC.
Sensor Deployment and management	Usually requires TAPs or Mirror/SPAN ports. Most sensors require external data collection technology to gather data. Hardware costs are high. Relatively fast deployment in centralized environments.

	High cost for distributed environments. Cost of managing sensor hardware can be high.
SDN Networks	Central management capability is often built in. Can deny unauthorized traffic at layer 2. Promising technology, but not widely deployed.
"Bump in the Wire"	Some systems, such as firewalls, have the capability of monitoring network data similar to TAPs.
Endpoint Agents	Some systems allow collection of network data using endpoint software.
Other Technologies	Other technologies exist and may be utilized to provide visibility of network data.

Considerations for selecting Network Data Feeds

The following considerations might inform the decision for collecting data from a network data feed:

Adversary Analysis

The Responsible Entity might perform an assessment of adversary tactics, techniques, and procedures that have been used in previously documented attacks. This analysis might drive network data feeds that focus on targeted uses cases.

ICS Protocols

The network data feeds, as well as the analysis tools used for INSM, should be assessed for their capability to process and analyze ICS specific protocols.

Data Types

The MITRE ATT&CK framework describes three network traffic data sources that are valid sources of INSM data:

1. Network Content Creation.
2. Network Traffic Content.
3. Network Traffic Flow.

While selecting network data feeds, a Responsible Entity may also narrow collection to the appropriate data types needed for specific use cases or detections.

Traffic Duplication

Network data collection can result in duplication of communications data when data is collected from multiple switches on a network. In some network topologies a single Ethernet packet could be collected multiple times by the INSM system. This kind of over collection results in reduced resource efficiency and poor INSM system performance and should be accounted for when selecting network data feeds. Consideration of traffic duplication may be part of a rationale on how network data feeds were selected or excluded for data collection.

Complimentary Monitoring Systems

Many Responsible Entities have existing SIEM systems which provide capability of detecting attack tactics such as Reconnaissance, Initial Access, Execution, Persistence, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, and Exfiltration. The detection capabilities of other installed systems should be considered when narrowing the focus of network data feeds.

Responsible Entities that have mature endpoint collection and detection systems including memory and process logging may properly include this capability as part of a rationale on how network data feeds were selected or excluded for data collection.

A Responsible Entity may choose to include firewall logs to augment INSM data collection.

Aligning Collection and Monitoring with Operations

Operational changes might require temporary or extended removal of INSM collection capability at specific locations. Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and, in the opinion of the DT, does not constitute cause for non-compliance with Requirement R1, Parts 1.2. or 1.3. For example, if a plant is undergoing turbine maintenance and control system upgrades, a Responsible Entity could suppress some or all INSM system components and alerts while that outage is underway to eliminate false positive notifications generated due to the maintenance activities.

Weather events, network outages, and operational upsets may generate a significant number of alerts in some INSM systems. Suppressing alarms or data collection may be warranted for some situations even if those conditions are not CIP exceptional circumstances.

Collection Limitations

Known and expected INSM limitations include:

1. Limited capability to analyze encrypted traffic.
2. High rates of false positive alerts until tuning can be completed.
3. Network traffic volume can overwhelm INSM analysis technology. There will exist situations when network volume reduces the visibility of network traffic. Short periods of reduced visibility are expected and are considered a known limitation of INSM systems. In the opinion of the DT these common situations should not justify a potential non-compliance finding, especially when other cyber security monitoring is in place.

Partner Networks

Transmission Operators have connections to partner networks for the purpose of exchanging Inter-Control Center Communications Protocol (ICCP) data. Some Generator Operators implement connections to external partners for turbine monitoring systems. Communications to and from partner networks frequently traverse an EAP and are visible on ESP networks. Collection of network data feeds that include these partner communications are high value for INSM data collection.

Resilience
While the INSM collection system will likely require some level of additional resource utilization to collect data from existing devices, failure modes of collection devices should be considered. For example, some control systems may have small networks that connect directly to an EAP, router, or firewall without a switch. If collecting INSM traffic at layer 2 requires adding a switch where no switch exists or where very little layer 2 traffic is visible, a focused approach might include a collection of firewall logs or collecting network data at an upstream location rather than creating additional failure points in the ICS system. Requirement R1, Part 1.1. allows a wide range of data collection including TAP devices, Network Flow data, or other methods that would not decrease the reliability of the ICS.

SDN
Use of modern technology, such as SDN, may provide relevant data as part of an INSM data collection system.

Data Filtering
Filtering or elimination of traffic with low cyber security value (backups, replication, virtual machine migration, vSAN, network storage protocols, video, encrypted traffic, etc.) is expected in a focused INSM collection system.

Filtering these data types enhances the ability of an INSM system to analyze traffic and generally results in higher signal to noise ratios and better detection outcomes.

Out of Scope collection
Requirement R1, Part 1.1. does not require collection of data such as:

- Serial communications.
- 4-20ma circuits.
- Wide area network circuits such as multiprotocol label switching (MPLS) (although MPLS and similar technologies may be an effective way of collecting INSM data and may be used).

Vendor Constraints and System Capability
Some ICS vendors have historically stated that their systems do not support cyber security monitoring using either INSM data collection or endpoint logging collection. Rather than add a “per system capability” exclusion, Requirement R1, Part 1.1. allows wide latitude to identify INSM network data feeds appropriate to each Responsible Entity’s ESP networks.

Some networks may not have the capability or capacity to provide network monitoring data to an INSM system. In those situations, the Responsible Entity has several options to provide monitoring data to the INSM including:

- Upgrading hardware and software to systems that do have the capability.
- Installing TAPs to collect network data.

- Collecting flow data.
- Collecting network data feeds from other internal networks that are adjacent to networks that lack modern capabilities or capacity.
- Supplementing network data feeds with other pertinent data feeds such as endpoint logs and firewall logs.
- Selecting the highest value network data feeds from targeted network ports such that the system will not experience capacity issues if all ports on a given device are monitored.

Note that for ESPs that have a high and medium impact rating it would be much more likely that the Responsible Entity would choose options that provide network data feeds such as upgrading hardware. Considerations about placement of monitoring ports are described in "The Practice of Network Security Monitoring" Chapter 2[6].

Reference Architecture

A sample reference architecture for INSM data collection is shown below. This diagram is intended to show a wide variety of possible collection methods. Responsible Entities are not expected to implement all of these, but rather to choose and implement the network data feeds that provide the most value to the Responsible Entity, as determined by the risk-based rationale in Requirement R1, Part 1.1.

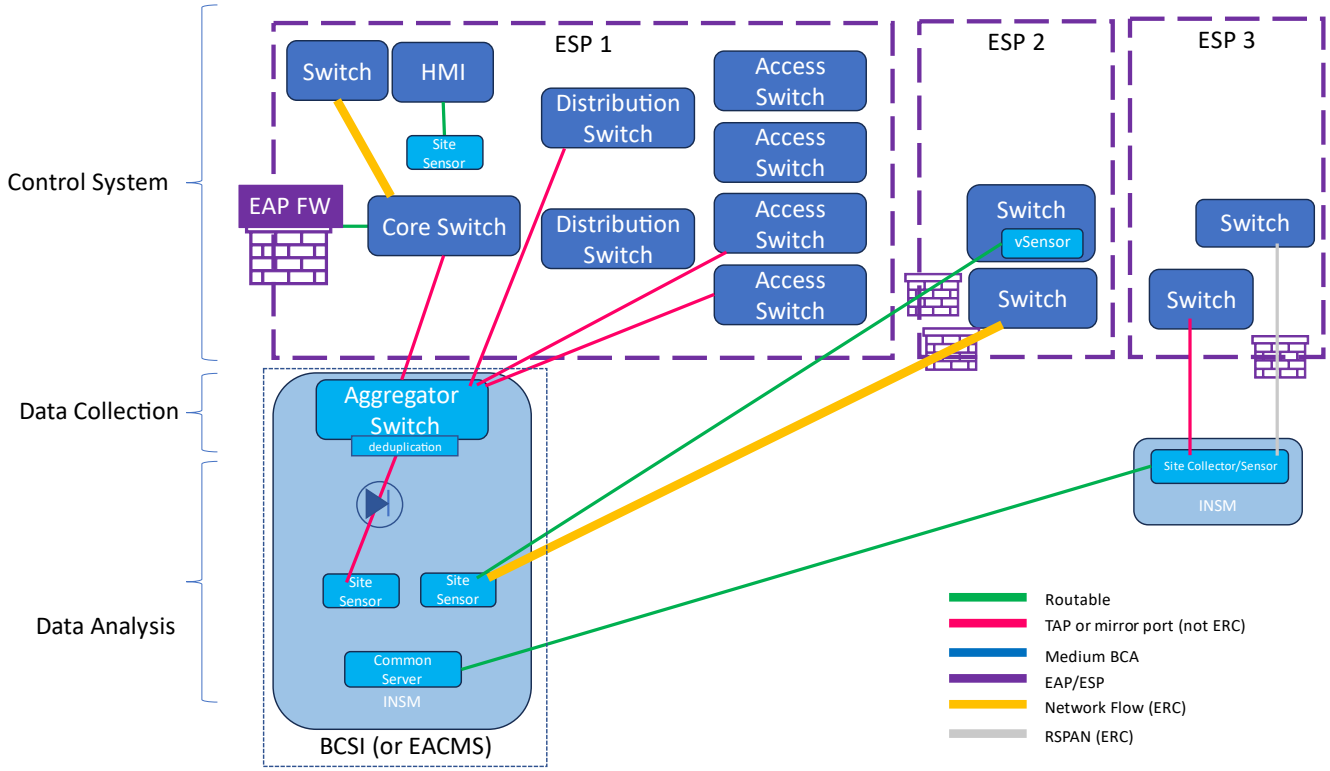

Figure 1

[6] Bejtlich, Richard; The Practice of Network Security Monitoring; published by No Starch press; June 15, 2013.

This reference architecture in Figure 1 has the following features:

ESP1

- Data collection tier is independent of analysis tier avoiding vendor lock in.
- Data collection tier is not connected to applicable systems via ERC. This provides visibility at very low risk.
- Mirror ports are used at appropriate locations to gather data.
- An optional data diode is shown between the analysis tier and the collection tier to provide high levels of segmentation.

ESP2

- A virtual sensor is installed in a switch as a virtual machine.
- Network Flow data is sent to another location for analysis.

ESP3

- RSPAN is configured to send data across a high bandwidth connection.
- A network TAP or SPAN port sends data to a local data collection device.

Emerging Technology

In Order No. 887, FERC also directed NERC to develop new or modified Reliability Standards that are forward-looking. The DT has purposefully tried to create standards that have objectives for Responsible Entities to comply with instead of specifying what technology or methods must be used to accomplish those objectives. The current technology landscape has a number of vendors which in many cases have developed proprietary methods to detect anomalous network behavior. As a result of technology advancements, new anomalous detection products are likely to be introduced. It is not the intent of the DT to dictate what technology a Responsible Entity uses to comply with the requirements. The goal is for Responsible Entities to be able to detect adversaries in ESP networks. Determining what technology each Responsible Entity will use should be part of its identification of methods used for data collection and detection in Requirement R1, Parts 1.2. and 1.3.

Rationale for Requirement R1, Part 1.2.

Requirement R1, Part 1.2.: "Implement one or more method(s) to detect anomalous network activity using the network data feed(s) from Part 1.1."

Summary

Compliance with Requirement R1, Part 1.2. will likely require several steps. Detecting anomalous network activity includes processing collected data, analyzing that data using one or more analysis techniques, and generating notifications regarding traffic or events of interest for evaluation in Requirement R1, Part 1.3.

"Anomalous"

As used in this document and INSM Requirement R1 and Requirement R1, Part 1.2, "anomalous" refers to unexpected, undesired, unusual, or undetermined network traffic. Unless specified, use of the word "anomalous" or "anomaly" in this document and in Reliability Standard CIP-015-1, does not refer to any specific proprietary technology commonly referred to as "anomaly detection." Anomalous traffic by itself does not necessarily indicate adversarial activity in a network, but when combined with analysis and context from other log sources and data, the Responsible Entity might classify communications as benign, suspicious, or other similar evaluations as required in Requirement R1, Part 1.3. The concept of analyzing traffic to select specific network data that will be evaluated is visualized in Figure 2.

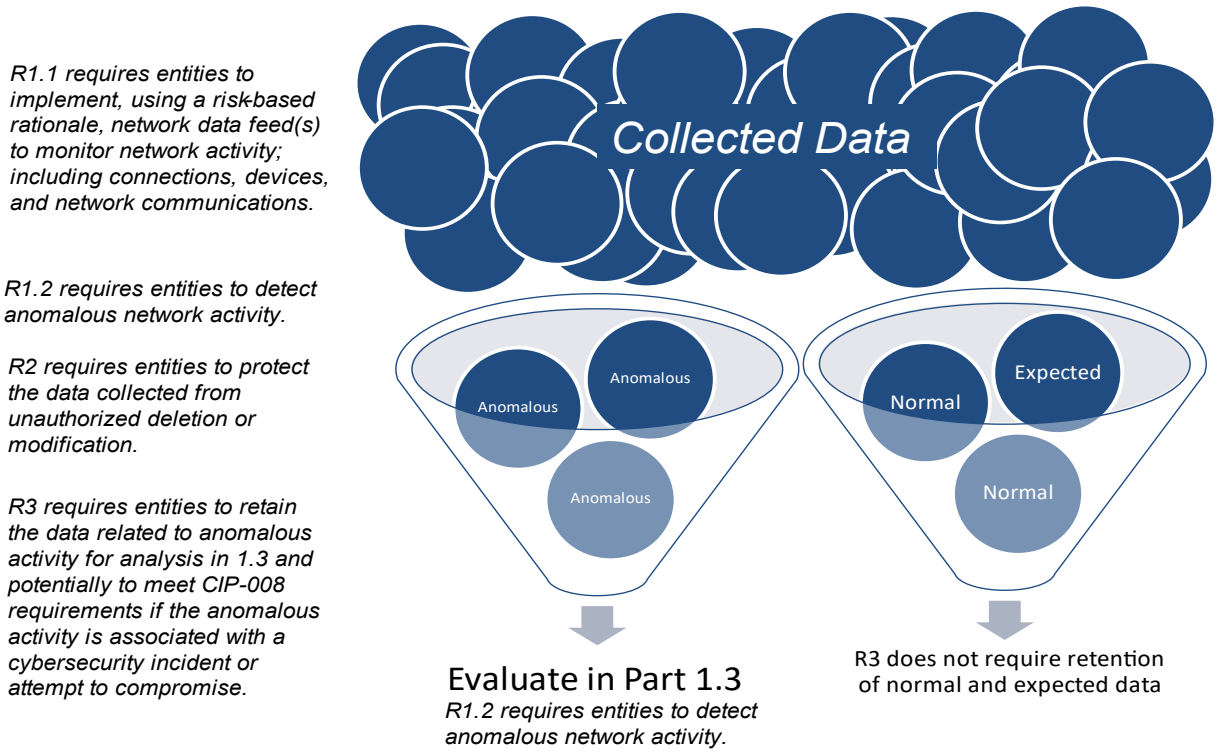

Figure 2

Detection Methods

Anomaly Detection (term used by vendors to refer to a specific technology)

Many vendors use the term "anomaly detection" to refer to specific technology and algorithms used by their software to develop a representation of the normal, expected network traffic seen in the Responsible Entity's collected traffic. Incoming traffic is then compared to that representation of expected

traffic, and this becomes the "baseline" (expected network behavior). Ongoing traffic is then compared against that "baseline" (expected network behavior) to identify traffic patterns with a statistical deviation from the baseline traffic. Anomaly detection is sometimes referred to using other names such as modeling. Some implementations of anomaly detection include machine learning algorithms and other technology to reduce the number of notifications.

Regardless of the algorithm or terminology used, an INSM system using anomaly detection is a valid method for compliance with Requirement R1, Part 1.2.

Signature-based detections
Signature-based detection is a technique used by intrusion detection systems, deep packet inspection, and related tools. These tools and techniques have a long history and a high level of maturity.
When evaluating signature-based methods to be used for compliance with Requirement R1, Part 1.2., attention should be given to existence of signatures that are related to the ICS protocols being analyzed and the need for data retention in Requirement R3.

Behavioral Detections
Some network behaviors are trivially detected by INSM systems. For example, Remote System Information Discovery[7] is a technique used to obtain detailed information about remote systems. INSM systems frequently include capabilities to detect these behaviors, especially if the behaviors have been identified during previous ICS attacks.

Indicators of Compromise (IOC) scanning
After threat actors are detected, Incident Response (IR) teams will frequently share IOCs as part of industry information sharing programs. INSM tools frequently include the ability to search historical network traffic and traffic content such as extracted files to detect similar activity in the analyzed network environment.

Configuration Checking
INSM systems frequently include features to analyze specific protocols in an effort to detect misuse or misconfiguration of the protocol. For example, an INSM system might analyze domain name system (DNS) messages, user agent strings, or x.509 certificates to identify suspicious activity. When evaluating configuration checking methods, attention should be given protocols such as Modbus, DNP3, EGD, ICCP, and other ICS protocols used in the monitored ICS.

Combining Methods
Some INSM systems combine several of the above methods to detect malicious traffic.

Other Methods
As of the publication of this technical rationale document there exist many acceptable methods of detecting anomalous network activity including:

[7] https://attack.mitre.org/techniques/T0888/

- Hygiene-based detections (protocol analysis, certificate analysis, weak cipher detection, use of known vulnerable protocols including SMBv1 and NTLMv1, detecting unauthorized DNS servers, etc.).
- Behavioral based detections (unusual logon times, protocol errors, unexpected protocol volume/size/payload, etc.).
- Proprietary detections.

This document cannot contain an exhaustive list of all possible detection methods. The Responsible Entity should implement detection methods that, as part of an overall INSM program, will provide data necessary for analysts to identify anomalous activity to a high level of confidence.

Tuning
Cyber security detection systems including INSM systems will require ongoing tuning of notifications and alerts. This tuning process could result in notifications and alerts that are suppressed or ignored during maintenance activities or while signatures are being tuned to produce a higher signal to noise ratio. This normal tuning activity is part of a mature INSM program.

Rationale for Requirement R1, Part 1.3.

Requirement R1, Part 1.3. "Implement one or more method(s) to evaluate anomalous network activity detected in Part 1.2. to determine further action(s)."

Evaluation of activity detected in Requirement R1, Part 1.2. is the "analyze" step described in Bejtlich's[8] book. Analyzing the data is an expected part of cyber security operations.

Evaluation
Evaluation of detected anomalous activity is implemented by following an analysis process, implementing steps outlined in a playbook, consulting with operational staff, or similar actions a Responsible Entity has documented as part of their INSM process(es) developed in Requirement R1.

Potential Actions
Resulting actions from the evaluation process might include:

- Escalation following the Responsible Entities Incident Response plan (as required by Reliability Standard CIP-008).
- No action.
- Further investigation.
- Tuning of the INSM system to reduce false positive notifications or adjust severity level.
- Other actions as determined by the Responsible Entity.

[8] Bejtlich, Richard; *The Practice of Network Security Monitoring*; Chapters 3-8, published by No Starch press; June 15, 2013.

Rationale for Requirement R2

Requirement R2: "Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to retain internal network security monitoring data associated with network activity determined to be anomalous by the Responsible Entity, at a minimum until the action is complete, in support of Requirement R1, Part 1.3."

Note: The Responsible Entity is not required to retain internal network security monitoring data that is not relevant to anomalous network activity detected in Requirement R1, Part 1.2.

Requirement R2 allows Responsible Entities to choose which data and data types to discard quickly, which data types to store for short time frames, and which data types to store for longer periods of time. It is expected that a Responsible Entity's data retention process will specify longer retention timeframes for data that has higher cyber security value; while data with low cyber security value is retained for shorter periods of time, if at all. Regardless of the data retention process created, the goal of the process should be to retain data that can support the analysis required in Requirement R1, Part 1.3. and provide evidence needed to meet CIP-008-6 Requirement R2 for data retention related to an actual Cyber Security Incident or attempt to compromise.

An example data retention chart is provided below to outline retention considerations.

Network Communications Data Type	Cyber Security Value over time	Retention Cost	Retention Timeframes or Number of Events to retain
Network Traffic: Full PCAP (payloads) (recording all or most data on the network.)	Value diminishes quickly with time Encrypted payloads have little retention value	High	TBD by Responsible Entity
Targeted PCAP (payloads) generated as part of an analysis or investigation. **Targeted PCAP (payloads) related to or generated from an alert, notification, or event of interest.** **Network traffic records saved as part of an analysis or investigation.**	Value diminishes slowly with time	Low	TBD by Responsible Entity
Network Metadata: **Network Connection data generated from PCAP** **Network flow data** **Network Connection and Session Information**	Value diminishes slowly with time	Low	TBD by Responsible Entity
Carved Files retrieved from PCAP	Malicious files have high value – other files have almost no value	Medium	TBD by Responsible Entity
Hashes of carved files retrieved from PCAP	Maintains high value over time	Low	TBD by Responsible Entity

Data retention is normally specified by the number of events or records of network communications that are stored in an INSM system or by the number of days data is retained. A Responsible Entity might choose to temporarily increase amounts of data collection which might require decreasing the amount of data retained on an INSM system.

Rationale for Requirement R3

Requirement R3: "Each Responsible Entity shall implement, except during CIP Exceptional Circumstances, one or more documented process(es) to protect internal network security monitoring data collected in support of Requirement R1 and data retained in support of Requirement R2 to mitigate the risks of unauthorized deletion or modification."

A common adversary technique is "Indicator Removal" (T1070[9]). The intent of Requirement R3 is to protect the collected INSM data from modification or deletion by an adversary.

Compliance with this requirement includes implementation of protective and detective controls. Examples of controls that could be considered to safeguard INSM data include:

- Granting only authorized personnel electronic and physical access to the INSM system.
- Installing an INSM system with built-in methods that safeguard the integrity of stored data.
- Segmentation of the INSM system into an isolated network separate from the BES Cyber System being monitored.
- Authentication and authorization systems used by the INSM system could be maintained at a higher assurance level than corporate authentication systems or separated from corporate authentication systems.
- Implement two-factor authentication for access to the INSM system.
- Other commonly accepted methods used to protect log data.

Additional Considerations

Information Sharing

Note that no part of Reliability Standard CIP-015-1 or Requirement R3 is intended to limit information sharing. The focus of Requirement R3 is to ensure the data is available and has integrity. Sharing IOCs, threat intelligence, and relevant information about adversary tactics, techniques, and procedures is part of a mature cyber security program. Government agencies expect and encourage Responsible Entities to share information gathered by INSM systems (see NIST 800-150[10], CISA Information Sharing Guidance[11], Cyber security Information Sharing act of 2015[12]). The ERO Enterprise CMEP practice guide titled "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[13]" states that the CIP-011 Requirement R1, Part 1.2. process "should include how the Responsible Entity addresses providing BCSI to third party vendors or other recipients." After implementing an INSM system, Responsible Entities may

[9] https://attack.mitre.org/techniques/T1070/
[10] https://csrc.nist.gov/pubs/sp/800/150/final
[11] https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing
[12] https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance
[13] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf See Page 8

need to review their CIP-011 Requirement R1, Part 1.2. process to ensure that it includes a process for sharing INSM data with third party vendors, government agencies including CISA and law enforcement, and information sharing and analysis organizations such as E-ISAC as outlined in the CMEP practice guide.

Appendix 1 – Example of Selecting Network Data Feeds

Appendix 1 outlines some of the considerations a Responsible Entity might review when determining which network data feeds to implement as part of Requirement R1, Part 1.1.

The table below uses the following simplified diagram of a high impact ESP network.

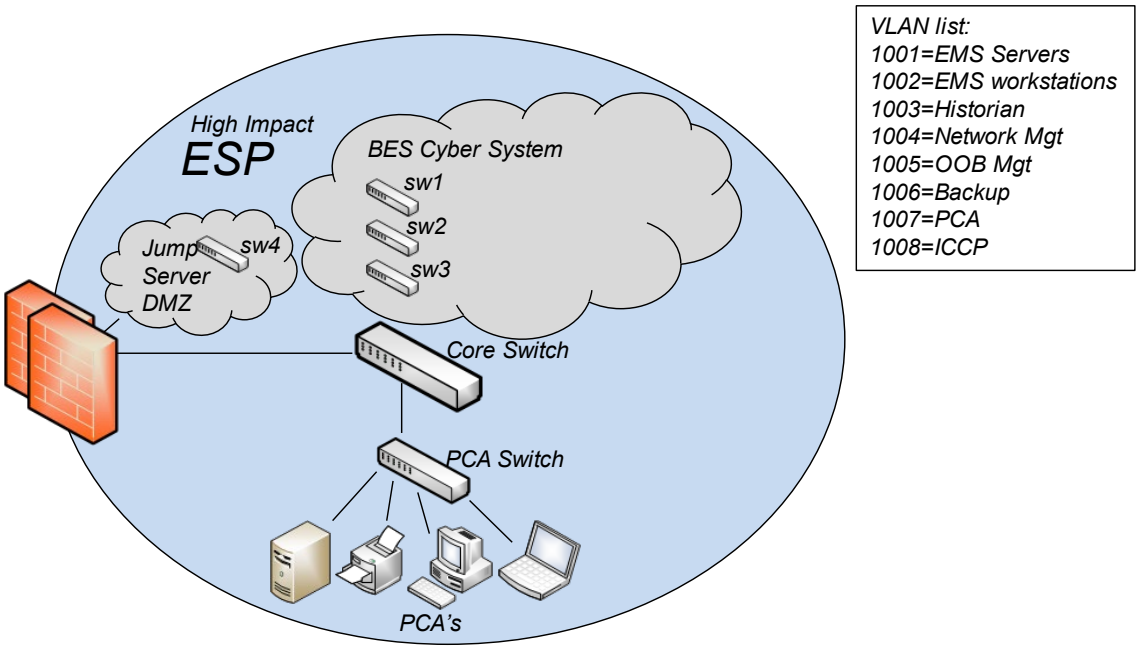

Figure 3

Example rationale for selecting Network Data Feeds:

Network Data Feed	Collection Implemented	Network Location	Collection Method	Rationale
Core PCAP	Yes	Core Switch	Mirror VLANs to physical port	Nearly all data traverses this switch. By collecting at the core switch all data between BCS devices and PCAs will be collected. Collecting based on VLAN allows exclusion of backup traffic.
sw1 PCAP	Yes	sw1 (EMS Server access switch)	Mirror VLAN to physical port	EMS servers communicate frequently with each other and intra-vlan traffic may not cross the core switch. Remote access is allowed to these servers.
	No	sw2 (EMS workstation access switch)		All devices on this switch are EMS workstations which normally do not communicate to each other. All EMS workstations have a high level of endpoint logging including EDR logs (memory and process level logs). Remote access is not allowed to these workstations. All expected traffic will be captured in the Core PCAP data feed. Unauthorized connections are logged by a local firewall enabled on each workstation.
	No	sw3 (DNP3 access switch)		All traffic between these DNP3 front end processors will traverse the core switch. Additional collection from this switch would result in duplication of all traffic.
sw4 PCAP	Yes	sw4 (access switch)	Mirror source ports	IRA to the jump server is a likely attack vector.

			to physical port	
	No	PCA switch		Communication to and from all PCA devices traverses the core switch and will be collected. It is understood that intra-vlan traffic that does not cross the core switch will not be collected. Complementary monitoring of PCA devices is provided by the SIEM system which monitors endpoint logs of all devices including, where possible, memory and process logging. Additional hardening and endpoint controls of all PCAs are implemented. Collecting network data from the PCA switch would result in duplicate data with no assessed improvement to monitoring.
Core PCAP	Yes	VLAN 1001 EMS Servers	VLAN Source	This vlan is critical to the operation of the EMS
Core PCAP	Yes	VLAN 1002 EMS Workstations	VLAN Source	The vlan will collect all communications between VLAN 1002 and other devices.
Core PCAP	Yes	VLAN 1003 Historian	VLAN Source	Historians have been targeted by adversaries that targeted other electric companies. Threat Intel has provided several use cases that require this data.
Core PCAP	Yes	VLAN 1004 Network Mgt	VLAN Source	Management ports were known to be targeted by adversaries in ICS attacks. The INSM system has several use cases that will alert on abuse of management connections.
Core PCAP	Yes	VLAN 1005 OOB Mgt (iDrac/iLO)	VLAN Source	These ports provide elevated access and might be expected

				to be abused by a malicious insider. The OOB cards in use do not provide firewall capabilities so INSM detective controls are added to augment visibility of these ports.
	No	VLAN 1006 Backup		The large volume of backup traffic has very little cyber security value and would increases noise in a data feed
Core PCAP	Yes	VLAN 1007 PCA	VLAN Source	Some PCA devices communicate to external hosts to download patches. This communication traverses the core switch and will be monitored
Core PCAP	Yes	VLAN 1008 ICCP	VLAN Source	Although legitimate ICCP data is already collected in VLAN 1001 (EMS Servers) this VLAN will be collected so that any unexpected requests from the partner network will be logged.
Firewall Log data	Yes	Firewall	API	The INSM tool includes a built-in integration to the firewall which provides information about blocked connection attempts.

This example provides some of the considerations for selecting network data feeds. This example is not exhaustive, but is given primarily to demonstrate a few of the decision points that the Responsible Entity will consider while implementing network data feeds.

The resulting network data feeds to be implemented as a result of this example are depicted in Figure 4.

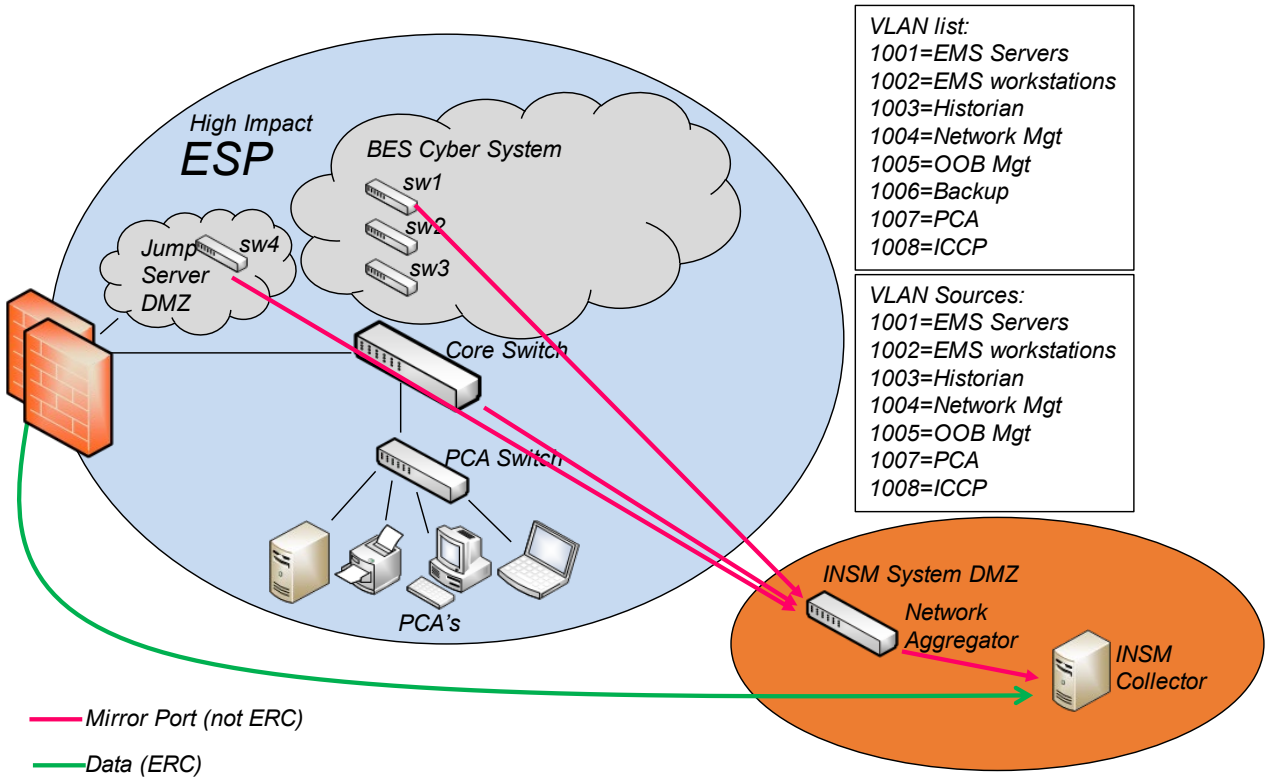
VLAN list:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1006=Backup
1007=PCA
1008=ICCP
VLAN Sources:
1001=EMS Servers
1002=EMS workstations
1003=Historian
1004=Network Mgt
1005=OOB Mgt
1007=PCA
1008=ICCP
High Impact
ESP
BES Cyber System
sw1
sw2
sw3
Jump
Server
DMZ
sw4
Core Switch
PCA Switch
PCA's
INSM System DMZ
Network
Aggregator
INSM
Collector
Mirror Port (not ERC)
Data (ERC)

Figure 4

Revision History

Revision #	Revision Date	Revision Details
V0.1	22 Feb 2024	Initial Draft
V0.2	26 Mar 2024	Changes based on industry comments.
V0.3	24 Apr 2024	Changes based on industry comments.