NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Technical Rationale for Reliability Standard CIP-015-1

CIP-015-1 – 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 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 the three security issues.[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 and incidents. 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 systems that are internal to the operational zones of the entity. While the entities may choose to use NSM systems to monitor other networks, such as corporate internet perimeters, corporate networks, or associated Electronic Access

[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 security issues: (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.

Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS) networks, these requirements apply only to network communications between devices within the ESP of applicable BES Cyber Systems.

The Project 2023-03 DT proposed Reliability Standard CIP-015-1 requires responsible entities to implement INSM processes. Responsible Entities must evaluate their networks within ESPs and identify the collection location(s) and method(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 unexpected, anomalous, or otherwise suspicious network communications within applicable networks. Responsible Entities must evaluate and escalate these anomalous activity occurrences, if appropriate, for further investigation. That could include escalation to an 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.

Responsible Entities must also appropriately protect the collected INSM related network communications data and metadata to prevent unauthorized data manipulation and preserve the data as needed to facilitate additional investigation. In addition, entities must retain relevant data collected from their INSM system(s) with sufficient detail and duration to facilitate the evaluation and further investigation of potential cybersecurity incidents. 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 Drafting Team 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[3], 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].

Based on industry comments, the DT concluded that INSM requirements do not fit cleanly into any existing standard and would be best implemented as a standalone standard. In addition, developing a new standard provides future standard development teams with a framework for potential expansion of INSM to mediums without ERC and low impact BES Cyber Systems, if needed.

[3] *Id.*
[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.

System Classification

The ERO Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[6]" should be referenced to determine if the INSM system and its components are Protected Cyber Asset (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 an 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 expected or required in Reliability Standard CIP-015-1.

Rationale for Requirement R1

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 protected ESP environments.

Rationale for Requirement R1 Part 1.1

> *Requirement R1, Part 1.1: "*Identify network data collection locations and methods, based on the network security risk(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 occurs at strategic network locations and utilizes a variety of methods. In "Applied Network Security Monitoring" (Chris Sanders, Jason Smith), the "Applied Collection Framework" is described wherein 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 requires the Registered Entity to identify many 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 cybersecurity monitoring purposes.

[6] https://www.nerc.com/pa/comp/guidance/CMEPPracticeGuidesDL/CMEP%20Practice%20Guide%20-%20Network%20Monitoring%20Sensors.pdf

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 internal ESP networks and select an INSM data collection location(s) and method(s) that 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 data that provides value based on a Responsible Entity's evaluation of the network cybersecurity risk in their particular system.

Data Collection Locations

In CIP-015-1, "network data collection locations" refers to both a physical and a logical concept. In a physical context, network data collection locations connote data collection from devices that perform technical functions 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 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. An entity may identify a core switch as an ideal physical collection point, and then further narrow traffic collection by excluding VLAN traffic with low cybersecurity monitoring value from the collection system. In another example, an 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.

The entity is responsible for identifying physical and logical communication convergence points that will provide the highest value data for the INSM system.

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. Usually not 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 extensible authentication protocol (EAP).
Network Flow (NetFlow, sFlow, IPFIX, jflow, NetStream, Cflowd, etc.)	No hardware costs for forwarding. Capable of performing in low bandwidth environments. 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.

Optional considerations for selecting or excluding collection locations and methods

As Responsible Entities determine collection locations and methods, the following considerations might inform the decision for including or excluding a collection location or method:

Adversary Analysis

The entity might perform an assessment of adversary tactics, techniques, and procedures that have been used in previously documented attacks. This analysis might drive collection priorities to focus on targeted threats and uses cases that would inform collection locations and exclusions.

ICS Protocols
INSM technologies are most meaningful and effective when they are built to be ICS protocol aware and provide detections of network activity that might hamper an industrial process. The collection locations and methods, as well as the analysis tools used for INSM, should be assessed for their capability to detect ICS specific attacks.

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 data locations and methods, an 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 collection locations and methods. Consideration of traffic duplication may be part of a rationale on how network locations 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 collection locations.

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 locations were selected or excluded for data collection.

A Responsible Entity with mature firewall logging capabilities and extensive segmentation may choose to include firewall logs to augment INSM collection.

Aligning Collection and Monitoring with Operations
Operational changes might require temporary or extended removal of INSM collection at specific locations. Suppressing and enabling alerts in alignment with operational activities is a sign of a mature INSM system and not a cause for potential non-compliance with Requirement R1, Part 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 alarms in some INSM systems. Suppressing alarms or collections 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 should not justify a potential non-compliance finding, especially when other cybersecurity monitoring is in place.

External Networks

External networks, such as turbine monitoring systems, Inter-Control Center Communications protocol (ICCP) connections, etc., are high value networks for INSM data collection of data related to these functions is more likely to be selected than excluded from network 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 cybersecurity 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

Some ICS vendors have historically stated that their systems do not support cybersecurity 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 data collection locations and data collection methods appropriate to each entity's ESP networks.

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. Entities are not expected to implement all of these, but rather to choose and implement the collection locations and methods that provide the most value to the entity.

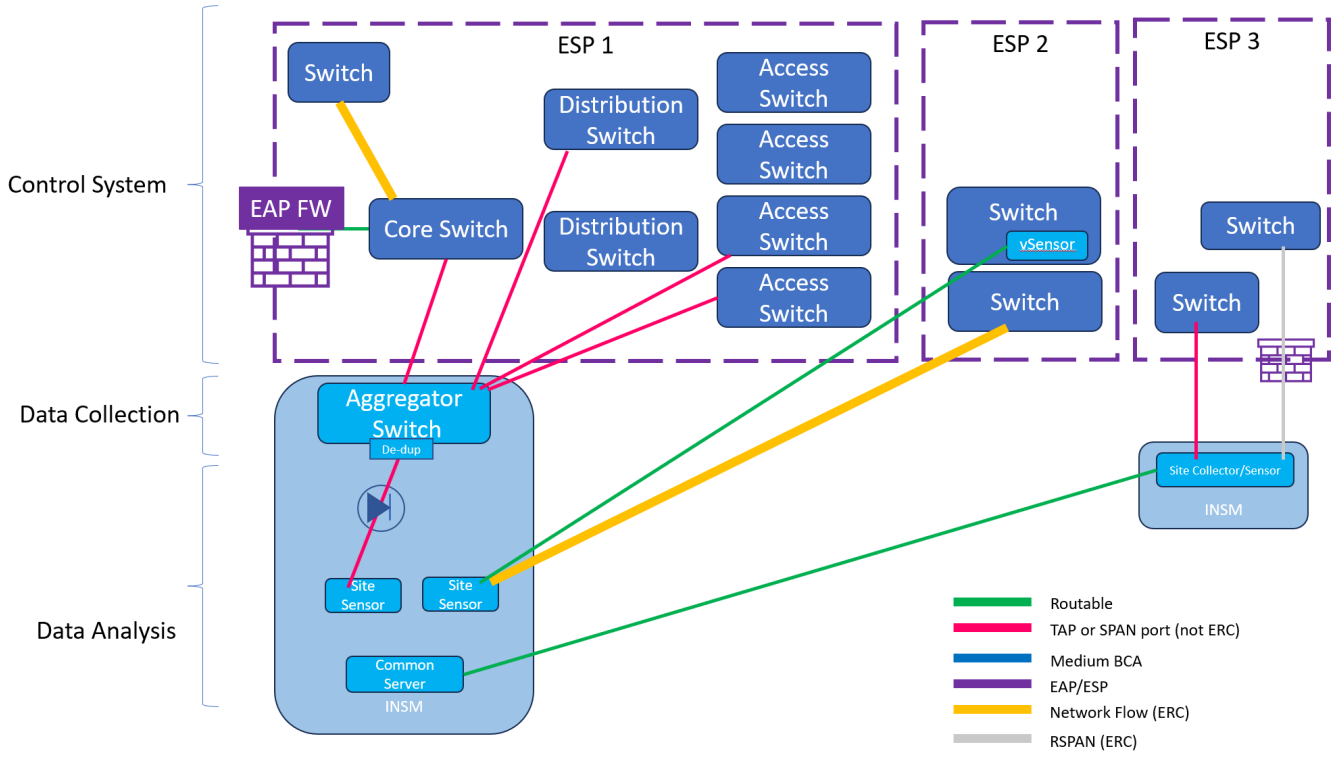

Figure 1

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 Reliability Standards that are forward-looking. The DT has purposefully tried to create standards that have objectives for 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 the rise of AI on the technology landscape, new anomalous detection products that use AI learning models are likely to be introduced. It is not the intent of the DT to dictate what technology an 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 1, 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 data collected at locations identified in 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 the INSM Requirement R1 and Requirement R1, Part R1.2, "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.

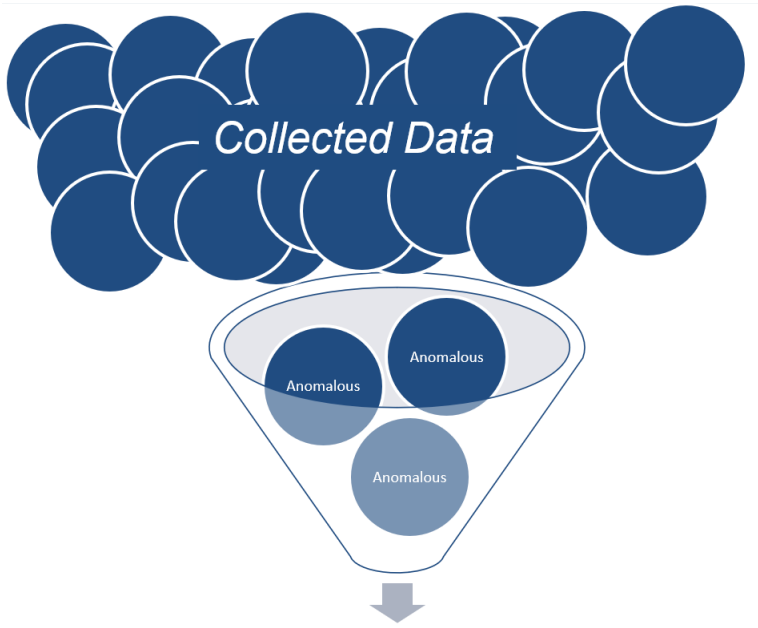

Figure 2

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 that incoming traffic is then compared to determine if any traffic is anomalous or not.

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.

Anomaly detection is sometimes referred to using other names such as modeling. Products may include machine learning algorithms and other technology to reduce the number of notifications.

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 metadata retention in Requirement 2.

Behavioral Detections

Some network behaviors are trivially detected by INSM systems. For example, Remote System Information Discovery 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

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

Cybersecurity 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 activity detected in Part 1.2 to determine appropriate action."

Evaluation of activity detected in Requirement R1, Part 1.2 is the "analyze" step described in Bejtlich's book. Analyzing the data is an expected part of cybersecurity 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 an 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 Registered 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.

Rationale for Requirement R2

*Requirement R2: "*Responsible Entity shall implement one or more documented process(es) to protect INSM data collected in support of Requirement R1 to mitigate the risks of unauthorized deletion or modification, except during CIP Exceptional Circumstances.''

A common adversary technique is "Indicator Removal" (T1070[7]). The intent of Requirement R2 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 like those used to protect BCSI or EACMS. Examples of controls that should be considered to safeguard INSM data include:

- Installing an INSM system with built-in methods that safeguard the integrity of stored data.
- Granting only authorized personnel access to the INSM system.
- Segmentation of the INSM system into an isolated network separate from operational technology (OT) and corporate networks.

[7] https://attack.mitre.org/techniques/T1070/

- 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.

Note that no part of Reliability Standard CIP-015-1 or Requirement R2 is intended to limit information sharing. The focus of Requirement R2 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 cybersecurity program. Government agencies expect and encourage registered entities to share information gathered by INSM systems (see NIST 800-150[8], CISA Information Sharing Guidance[9], Cybersecurity Information Sharing act of 2015[10]).

The ERO Enterprise CMEP practice guide titled "Network Monitoring Sensors, Centralized Collectors, and Information Sharing[11]" states that the CIP-011 Requirement R1, Part 1.2 process "should include how the registered entity addresses providing BCSI to third party vendors or other recipients." After implementing INSM entities may 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.

Rationale for Requirement R3

> *Requirement R3: "*Responsible Entity shall implement one or more documented process(es) to retain network communications data and other metadata collected with sufficient detail and duration to support the analysis in Requirement R1, Part 1.3, except during CIP Exceptional Circumstances.''

Requirement R3 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 R3 for data retention related to an actual cybersecurity incident or attempt to compromise.

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

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

Network Communications Data Type	Cybersecurity 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 Registered 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 Registered 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 Registered 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. Specifying retention timeframes as averages or moving targets rather than absolute values is an acceptable specification in a data retention chart.

Metadata

In the context of Requirement R3, INSM related metadata is a record of past network communication and traffic or a summarization of that traffic.

Metadata retention will vary by protocol. For example, some ICS protocols do not use layer 3, and other ICS protocols are layer 3, but do not create TCP connections. The decision and capabilities of what metadata is retained is frequently configured as part of the INSM system. Registered Entities should consult with vendors to ensure that INSM tools store sufficient data to support necessary analysis of

network activity. The decision of which metadata to store and retention timeframes should enable the entity to accomplish its cybersecurity and operational objectives.

Revision History

Revision #	Revision Date	Revision Details
V0.1	22 Feb 2024	Initial Draft