CYBERSECURITY

Internal Network Security Monitoring (INSM) Implementation Checklist

Schweitzer Engineering Laboratories, Inc.

Introduction

In January 2023, the U.S. Federal Energy Regulatory Commission (FERC) issued Order No. 887. This order directed the North American Reliability Corporation (NERC) to expand the scope of required network monitoring beyond the electronic security perimeter (ESP) and into the LAN. This led to the creation of the Critical Infrastructure Protection (CIP) reliability standard CIP-015-1: Cyber Security — Internal Network Security Monitoring (INSM), which mandates INSM for network traffic inside an ESP. All critical infrastructure industries should consider INSM as a part of their security monitoring within trusted zones, such as ESPs, to effectively detect malicious activity and intrusions.

To comply with this directive, it is necessary to implement a dedicated network monitoring solution. There are many intrusion detection system (IDS) manufacturers, and while each possesses a unique set of strengths and weaknesses, a successful INSM implementation strategy requires far more than the selection of a product. The technology must be holistically integrated with existing infrastructure, governance, and workforce. This can include the identification of stakeholders, updates to policies and standards, technical modifications to existing infrastructure, and increasing the skill levels of the current workforce. This document is provided to assist in the early planning stages of INSM implementation.

In each section of this document, corresponding checklists and descriptions can be found, which guide and inform an implementation strategy for INSM deployed at scale. While the items contained in each checklist are typical for most organizations, each organization is unique and will need to tailor their strategy accordingly. Schweitzer Engineering Laboratories, Inc. (SEL) Cyber Services is uniquely qualified to assist in your INSM initiative. Our network and security engineers can help you at the initial phase of your project by providing a comprehensive front-end engineering design (FEED) study during implementation and long-term maintenance and monitoring.

Governance

Policy and Standards

As is necessary for the introduction of all new technological enterprises, governing policies and organizational standards must be reviewed and revised to ensure that a new solution is properly integrated into the overarching governance's structure of the organization. This review process often consists of manufacturer risk reviews, data classification efforts, data owner and custodian involvement, and system ownership designation.

NERC CIP Compliance

Regulatory compliance provides the base level for what is required from a security perspective. Per NERC CIP-015, only medium-impact facilities with external routable connectivity and high-impact facilities are initially required to implement INSM. However, it may be valuable to consider a broader deployment of INSM to realize the security and visibility benefit across all critical networks.

While an IDS solution may be implemented to comply with NERC CIP-015 requirements, it is important to remember that the system itself must be included in the existing compliance program. Compliance mandates, such as inventory management, asset classification, vulnerability management, and data classification, must be carefully considered throughout design and implementation.

Governance Checklist

Table 1 Governance Checklist

Item	Description	Complete (Yes/No)
Policies	Existing policies are reviewed and updated to accommodate the new technology.	
Processes	Existing processes are updated to accommodate new technologies, including but not limited to, NERC CIP-010 Cyber Security — Configuration Change Management and Vulnerability Assessments process, NERC CIP-007 Cyber Security — Systems Security Management process, and NERC CIP-013 Cyber Security — Supply Chain Risk Management process.	
Plans	Existing plans are updated to accommodate new technology, including but not limited to, NERC CIP-008 Cyber Security — Incident Reporting and Response Planning, NERC CIP-009 Cyber Security — Recovery Plans for Bulk Electric Systems (BES) Cyber Systems, and NERC CIP-011 Cyber Security — Information Protection.	
Standards	Existing standards are reviewed and updated to include new technology.	
Data Classification	Data are classified and infrastructure is allocated for storage and management. The Electric Reliability Organization (ERO) Enterprise Compliance Monitoring and Enforcement Program (CMEP) Practice Guide provides guidance to ERO Enterprise CMEP staff when assessing a registered entity's process to authorize access to designated BES Cyber System Information (BCSI) storage locations and any access controls the registered entity implemented. The Monitoring Sensors, Centralized Collectors, and Information Sharing Practice Guide should be referenced to determine if the INSM system and its components are Protected Cyber Assets, electronic access controls, or monitoring systems, or if they are exempted from applying protections other than those required for BCSI protection.	
Data Ownership	Data owner and custodian are identified.	
Compliance	New technologies are completely integrated with the compliance program (asset classification, patch management, etc.).	

Infrastructure

Firewalls

Except in the case of an isolated local deployment, firewall rules will need to be revised to allow the passage of metadata and alerts from the IDS platform or anomaly detection solution, to a central location. This may include metadata sent from the sensor to a central management console or data from the central management console to a Security Information and Event Manager (SIEM). It is critical to identify what updates to the firewall are going to be required and ensure that the firewall administrators are consulted about the required updates and given adequate time for review and implementation.

WAN

Prior to installation of a monitoring system, the WAN transport infrastructure should be assessed to validate that it can adequately support the increased traffic load. Traffic that will need to traverse the WAN can be minimal in the case of SIEM alerts or metadata traffic feeds; however, maintenance activities, such as remote patching to the platform and engineering access, should also be considered.

LAN

LAN analysis and updates are fundamental to determining a monitoring strategy. Multiple methods of capturing traffic from the LAN can be utilized, but the best option is often dependent on the network architecture and types of technology being monitored. For instance, in the case of virtual infrastructure, we may opt to use a remote collector to transport data from the virtual cluster to our monitoring solution. In other cases, we can leverage the switches themselves to deploy an endpoint agent on the switch to monitor and forward traffic. However, the most common method of capturing traffic is the use of a dedicated switched port analyzer (SPAN) or mirror port on the switch through which the traffic passes. This method requires a modification to the configuration on each switch, which instructs the switch to copy ingress or egress traffic from a specified port or range of ports, before sending this traffic out to a dedicated monitoring port. If using this method, it is important to analyze the capabilities, current processor used, and switch fabric throughput of the current network switch. Some switches do not support a full switch port mirror, and if mirroring is turned on, overused switch network traffic can be interrupted or dropped.

If a SPAN or mirror port cannot be leveraged for monitoring, a valid alternative method is to use a network traffic access point (TAP). A network TAP is physically placed between the switch and the host it is connected to and makes copies of the traffic passing through it, before sending that traffic to the IDS.

The most efficient method of copying traffic to an IDS sensor is the use of operational technology (OT) software-defined networking (SDN). OT SDN enforces dataflow baselines, which translates to granular control of network traffic. This approach also allows for precise definition of network data feeds for monitoring, while ensuring that explicitly authorized traffic is permitted to traverse the network. The logical nature of OT SDN optimizes IDS sensor deployment as data feeds do not need to be physically connected to each switch. This type of network infrastructure can drastically decrease the number of sensors needed to monitor the network; OT SDN enables complete network visibility without packet duplication through a single OT SDN switch port.

Asset Risk Profiling

Often referred to as crown jewel analysis in enterprise environments, asset risk profiling informs the monitoring strategy of an organization by identifying the most critical devices, systems, and resources, ensuring priority in maintaining the availability and visibility of these assets. Additionally, with the outcome of this analysis, operational playbooks can be developed to prioritize incident response (IR) activities prescribed to ensure the availability and integrity of these devices. The concept of high-value data feeds supports this approach of maximizing monitoring effectiveness. The technical rationale for NERC CIP-015-1 supports this concept by explaining that R1 Part 1.1 is intended to require entities to identify and monitor critical data feeds.

Infrastructure Checklist

Table 2 Infrastructure Checklist

Item	Description	Complete (Yes/No)
Firewall Rules	Required ports and protocols are identified to support INSM, and firewall rule sets are updated.	
WAN Transport	Network traffic that will traverse the WAN has been identified. WAN transport network infrastructure has been analyzed and can support the increased network traffic load.	
LAN Monitoring Strategy	The method of moving traffic from the switches to the INSM sensor has been identified, and network changes and upgrades have been completed.	
Asset Risk Profiling	Crown jewel assets have been identified.	
Critical Data Feeds	Critical data feeds have been identified, and network monitoring points have been updated appropriately.	

Technology

IDS

The fundamental requirement for an IDS tasked with monitoring a control system is that it has protocol dissectors for the industrial protocols used in the system. Secondly, the platform should provide industrial-focused rule sets that alert when deviations from established baseline communications occur. Manufacturers of IDS for industrial control systems (ICSs) typically have broad protocol support; however, it is beneficial to confirm that your systems' protocols are included. Follow-on considerations, which can be useful when selecting a manufacturer, should include deployment strategies that align with specific answers to the following questions:

- Does this deployment require cloud connectivity? Is it capable of operating in an isolated environment?
- How many sensors are required? What is the expected volume of ingress traffic for each sensor? Are there concerns with the bandwidth limitations of the sensors?
- How are alerts, notifications, and findings surfaced by the IDS viewed, investigated, and addressed? Does this solution integrate with existing tools or systems?

Deployment Strategy and Field Installations

Once the network monitoring requirements have been established and a comprehensive deployment strategy has been developed, the deployment of the solution can begin. Deployment will likely involve numerous stakeholders from a variety of teams, including IT infrastructure teams, substation and field technicians, and OT systems integrators. It is critical to develop a systematic plan for deployment to minimize the impact on teams with vast responsibility sets, as they may be under preexisting strain. This burden can also be offset by utilizing resource augmentation from an expert manufacturer, like SEL Cyber Services, that has checklist development capabilities, planning experience, and IDS configuration expertise. A field deployment strategy may be dependent on onsite surveys to help answer the following questions:

- Is there existing panel or cabinet rack space for new technology?
- Will new power and communications cabling be required?
- What are the available power supply voltages?
- Is a union labor force required for the support of the installation? Does a collective bargaining agreement need to be reviewed?

Technology Checklist

Table 3 Technology Checklist

Item	Description	Complete (Yes/No)
IDS	A manufacturer for IDS platform is selected, and a deployment architecture is defined.	
Deployment Strategy	The deployment strategy is fully defined, and all stakeholders are informed of the plan.	
System Integrator	If required, a system integrator is identified to develop system-specific plans.	
Stakeholder Agreement	All relevant stakeholders have been given the opportunity to review, comment on, and approve deployment plans.	

Operationalization

Monitoring and Investigation

Having and equipping adequate staff with the ability to monitor and triage alerts is critical to the long-term success and value of implementing INSM. This task requires personnel who are knowledgeable in the areas of network security and protocols found in OT environments. If hiring for this position is necessary, it may be beneficial to begin during the system design phase to ensure that the team is involved with the development of the solution. If such an initiative is to be supported by current IT-focused staff, it is advisable to provide specialized training in protocols and processes that may be unique to the OT and ICS sector.

Dependent on the organizational structure, it may be beneficial to create an OT security operations center, if one does not exist already. If OT-specific security analysts are hired as part of this initiative, they should be identified at an early stage so that system-specific training can be provided for a successful postdeployment operational posture.

Complementary Systems

As part of the overall monitoring strategy of the organization, complementary systems that support the overall aggregation and presentation of data to the security analyst should be considered. The most common complementary system is a SIEM system. The SIEM takes in data from multiple sources and presents those data to an analyst in a “single pane of glass” view. This view of events, from multiple sources across the system, helps provide context and visibility of potentially related events.

Other considerations for supporting the ongoing maturation of the INSM program include the augmentation of staff through services such as IR retainers, threat intelligence reports, and threat hunts using the data that INSM has made available.

Stakeholder Communication

IR plans should be updated to acknowledge and leverage the new technology, and the existing IR contact list should be updated to reflect ICS network monitoring stakeholders. The extension of new capabilities to networks, which previously lacked visibility, should allow rapid communication between stakeholders across multiple teams and improve situational awareness in the event of an incident.

Maintenance and Updates

Like other solutions, the components of any selected IDS platform will require periodic updates. These updates include the replacement of hardware deemed to be end of life, solution components found to be susceptible to newly discovered vulnerabilities, and updates to threat signatures and indicators of compromise.

Operationalization Checklist

Table 4 Operationalization Checklist

Item	Description	Complete (Yes/No)
Monitoring and Triage	Qualified monitoring and triage staff are in place.	
Investigation	Qualified investigation staff are identified.	
Complementary Systems	Complementary systems are identified and integrated.	
Stakeholder Communication	Stakeholders are identified and plans, call lists, and procedures are updated.	
Maintenance and Updates	Vulnerability management procedures are defined, and maintenance update cadence is established.	

Conclusion

The successful implementation of INSM involves far more than the initial installation of an appliance. Realization of the full value offered by such a solution is contingent of a holistic, project-focused approach that can be scaled to benefit the organization rather than merely focusing on supporting technology and individual components. SEL Cyber Services is well positioned to assist you in your journey to implement INSM by providing expert assistance at every step of the process. From a FEED study to deployment-focused staff augmentation, and even postdeployment monitoring and tuning, SEL Cyber Services engineers are prepared to assist you in closing existing gaps and achieving your goals.