Deloitte.

5x5 series: Insights and actions

Internal Network Security Monitoring (INSM)

North American Electric Reliability Corporation (NERC) has created the Critical Infrastructure Protection (CIP) Reliability Standard CIP-015-1 to enhance the detection of malicious activity within internal networks of Responsible Entities by implementing INSM processes. INSM focuses on the collection and analysis of network communications within a trusted zone. The requirements apply to network communications between devices protected by the Electronic Security Perimeter (ESP), Electronic Access Control or Monitoring Systems (EACMS), and Physical Access Control Systems (PACS) of high and medium impact Bulk Electric System (BES) Cyber Systems with External Routable Connectivity (ERC).

5 updates you should know	*5 actions you can take*
Within protected ESP environments, organizations should define criteria to identify and evaluate anomalous activity. This will necessitate **the collection of additional data sources** and the development of new baselines for network traffic. ***CIP-015*** builds upon network monitoring introduced in CIP-005 R1.5 by requiring INSM implementation. As a reminder, ***CIP-005*** R1.5 focuses on traffic passing through the Electronic Access Points (EAP) and does not require monitoring of traffic that is only passing between cyber assets within the defined ESP.	1 **Identify and evaluate network data feeds** (data location collection) that provide relevant data to establish network baselines. **Prioritize data collection based on risk**, focusing on critical and vulnerable areas, and implement a playbook for analyzing anomalies in collaboration with relevant stakeholders.
Organizations should explore INSM solutions to monitor and detect anomalous activity and generate alerts. ***CIP-015*** builds upon monitoring introduced in ***CIP-007*** by requiring monitoring and logging of internal ESP traffic for malicious activity. As a reminder, ***CIP-007*** R3.1 is focused on the implementation of traditional signature-based technologies on cyber assets and does not require monitoring the network traffic in the ESP. In addition, ***CIP-007*** R4 requires logging events at the Cyber Asset level.	2 **Evaluate existing INSM capabilities** against requirements and identify gaps; **implement an INSM solution that addresses gaps;** and establish targeted monitoring capabilities to detect anomalies, as well as develop incident response plans to contain and mitigate security incidents. **Detection technologies,** for example, could be anomaly-based detection, signature-based detection, behavioral detection, configuration checking, etc.
Organizations should define INSM solutions, then develop internal procedures, guidelines, and a streamlined process for meeting compliance. Documentation of process that support ***CIP-015*** can include escalation processes that are defined within ***CIP-008*** Cyber Security Incident Response Plans.	3 Create **Organization Change Management** program to account for new system design and training the teams on new requirements. INSM solutions may require **ongoing tuning of alerts and notifications** for effective management and response.
Organizations should develop a comprehensive **process to collect INSM data,** including capturing details associated with to anomalous network activity to evaluate and determine appropriate actions, including escalation.	4 Assess specific needs and regulatory requirements to **define retention periods** for different types of data, retaining critical security analysis data longer for investigations. **Define security controls for the data** to maintain their integrity and confidentiality by **leveraging existing security controls**, such as limiting system access, network segmentation, and multi-factor authentication (MFA) to maintain data integrity and protect sensitive information.
To decrease the risk of attackers removing or modifying evidence of their tactics, techniques, and procedures (TTPs) from compromised devices, organizations should **establish strategies** that include retaining data, continuous monitoring, logging network traffic, maintaining logs and other data regarding network traffic.	5 **Integrate policies for data retention** and implement centralized logging solutions to collect and store logs. **Deploy continuous monitoring tools** to aggregate and analyze host event logs, network traffic, resource access, and other security events in real-time, thereby reducing the risk of attackers removing or modifying evidence on the network.

Connect with us:

Samuel Icasiano
Managing Director | Deloitte & Touche LLP
saicasiano@deloitte.com

James Sample
Managing Director | Deloitte & Touche LLP
jwsample@deloitte.com

Ali Rizvi
Senior Manager | Deloitte & Touche LLP
alrizvi@deloitte.com