OPERATIONAL TECHNOLOGY MONITORING FUNCTIONAL CONSIDERATIONS FOR NATURAL GAS TRANSMISSION PIPELINE OPERATORS

Purpose

The CEO Task Group of the Oil and Natural Gas Subsector Coordinating Council (ONG SCC) has created a Functional Considerations document to support critical natural gas transmission pipeline owners and operators in evaluating Industrial Control System (ICS) monitoring and detection technologies that meet characteristics that the U.S. government has identified as supportive to national security of critical natural gas transmission pipelines. This information can enable broader private sector participation in the U.S. government's 100-day voluntary ICS Initiative to increase visibility and sharing of Operational Technology (OT) threats in critical natural gas transmission pipelines. Additional information may be included from technology suppliers to further identify strengths or weaknesses of ICS technology.

The Functional Considerations are guidelines and not requirements, and the list should not be considered a fully comprehensive requirements list for use in selecting or developing an OT Monitoring and Detection solution. Individual companies should develop their own individual requirements as well as use these considerations as part of their evaluation of solutions if they are so inclined.

Feedback

On October 29th, we will poll industry companies to see what companies are interested in participating in this voluntary effort, and to get an update on their progress of vetting and identifying a solution that will enhance OT Monitoring/Detection and information sharing with the appropriate government agencies. The communication on the 29th will provide details to companies on how they can provide their feedback. In an effort to ensure companies are comfortable with the feedback process, there will be several options available for providing the information.

Notice

This OT Monitoring Functional Considerations document and any related amendment(s) and notices will be posted on the ONG SCC website (ONGSubsector.com) and will be distributed by AGA and INGAA.

Disclaimers

The United States Government, the ONG SCC and the participating natural gas transmission pipeline industry does not and will not select, endorse, or recommend any specific technology or provider as part of the 100-day ICS Initiative for Natural Gas Transmission Pipelines. All entities are encouraged to deploy technology to improve visibility on their systems and share those outputs with government partners. Each entity must assess and select the technology or provider that is best for it. The evaluation considerations listed below are recommendations, not requirements. The government intends to work with entities to integrate, to the maximum extent possible, information-sharing with any ICS monitoring technology.

SECTION 1
FUNCTIONAL CONSIDERATIONS

Consideration	Meets (Yes / No/ Partially)	Comments
Technologies built for ICS networks with integration compatibility with ICS protocols and communications.		
Technologies that provide sensor-based continuous network cybersecurity monitoring, detection, and facilitate response capabilities for ICS/OT (i.e., the technology is ICS focused and already understands ICS communications, such as deep packet inspection capabilities for ICS protocols).		
Technology software that has a collective-defense capability/framework to allow the sharing of insights and detections rapidly with the Federal government, participants, and trusted organizations such as relevant information sharing and analysis centers (ISACs)/information sharing and analysis organizations (ISAOs). Data and insights collected must be sharable across the Federal government, to the greatest extent possible, and should be compatible with other sector sensing partnerships.		
Data collected should be formatted and compatible with industry standard data formats to enable sharing between agencies		
Technologies that do not collect or store sensitive data off the participants' site (e.g., perform analysis at the edge); however, certain insights or analysis outputs, such as whether a threat was present and relevant indicators of compromise, may be stored off premises.		
Technologies must protect or anonymize participant identity and ensure that risks and vulnerability information is not inadvertently disclosed between participants unless explicitly authorized by the participating entity.		
The technology allows for centralized queries and correlation. Sensitive information that contextualizes anomalies that may indicate adversary presence may be stored off premises for analysis.		
The technology allows for short-term (minimum of one year) on-site storage of raw data so new insights or detections can be retroactively applied to full data sets as needed.		
The technology is passive in its deployment, using isolation technologies to ensure that the technology itself cannot be used as a vector for adversaries to gain access into or impact operations of sensitive ICS networks		

Consideration	Meets (Yes / No/ Partially)	Comments
The ICS sensing technology is capable of working with correlation and aggregation technologies to allow for OT/IT sensing cross correlation and analysis.		
Technology has the capability of baselining normal ICS operations and can compare/detect abnormal operations from a known good baseline.		
Data at rest should be cryptographically protected (e.g., leverage NIST FIPS 140-3 certified cryptology to protect the data)		
Technology has the capability to detect known unauthorized remote access operations.		
Technology has the capability to detect unauthorized movement from the IT to the OT environment including via non-Internet Protocol (IP) communication pathways.		
Technology has the capability to detect unauthorized network activity and actions consistent with the MITRE ATT&CK for ICS framework including detecting potential tactics that may be used for disruptive or destructive actions.		
Technology has analytic and detection capabilities, which are dynamically updatable leveraging timely, validated, and trusted external or internal threat intelligence.		
Technology has the capability to detect access credential misuse.		
Does the Technology require any proprietary hardware or interoperable devices.		
Does the solution provider account for changes in the regulatory environment in their solution.		
Technology to identify violations of implemented application allow listing policies enforced on IT and OT systems.		
Technologies has the capability of passive monitoring with the option of a safe mode of scanning for asset inventory and the baselining of normal communication patterns between validated/approved detected devices.		
The technology requires the capability to add/augment additional data points to improve and augment the quality of discovered devices.		