DRAGOS

INDUSTRIAL CONTROL SYSTEM CYBERSECURITY INITIATIVE

OT MONITORING FUNCTIONAL CONSIDERATIONS FOR NATURAL GAS TRANSMISSION PIPELINE OPERATORS

MAPPING DRAGOS SOLUTIONS AGAINST THE CONSIDERATIONS

As threats to critical infrastructure become more frequent and sophisticated, cybersecurity leaders in the industry must improve visibility into their OT networks, effectively manage vulnerabilities, and leverage a collective defense approach to protect the connected supply chain to deliver products reliably and efficiently. Dragos, backed by the largest team of ICS/OT cybersecurity practitioners, is your ally and can meet you at any point on your journey with a set of comprehensive solutions positioned to help you meet government recommendations.

This guide was put together based on our understanding of the Functional Guide issued by the Oil and Natural Gas Subsector Coordinating Council (ONG SCC) in October 2021 to help pipeline owners and operators identify technologies to improve visibility of OT threats in pipeline systems. It maps certain Dragos solutions, in this case the Dragos Platform with Neighborhood Keeper, to the ICS Cybersecurity Initiative considerations – enabling critical infrastructure owners and operators to improve visibility into their systems and optionally share those insights securely and anonymously with specific government partners and other Neighborhood Keeper participants.

	OT Monitoring Functional Considerations For Natural Gas Transmission Pipeline Operators	Dragos Platform w/ Neighborhood Keeper	Notes
1	Technologies built for ICS networks with integration compatibility with ICS protocols and communications.	✓	The Dragos Platform was purpose built for ICS/OT environments with native support for both standard and proprietary ICS protocols for asset inventory, visibility, and threat detection.
2	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).	✓	Dragos Platform sensors provide deep packet inspection of ICS/OT protocols for continuous network monitoring, asset identification, analysis, threat detection, and actionable response playbooks designed for ICS/OT environments with correlation between cyber and physical events.
3	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.	✓	Neighborhood Keeper was designed specifically to address the need for collective defense in ICS/OT. Dragos Platform customers can opt-in to participate in Neighborhood Keeper, anonymously contributing aggregated analytics of threats in their own environment for visibility to other participants.
4	Data collected should be formatted and compatible with industry standard data formats to enable sharing between agencies.	✓	Dragos Platform supports industry standard data formats for data sharing including SYSLOG (CSV and CEF), SMTP, JSON, REST. Support exists for sharing analytics and summarized data with common SIEM and network security tools like next generation firewalls (NGFW).
5	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.	✓	Any directly or derived identifying information is removed but cryptographically secure mechanisms will be available for participants to ask for and respond to mutual aid requests.
6	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.	✓	Participants are able to centrally query and filter collective insights to determine frequency and occurrence of adversary activity in other participant environments.
7	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.	✓	Yes, based on Dragos Platform data retention configuration and storage capacity.
8	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 sensitive ICS networks.	✓	Secure architecture, software development, and system configuration standards are regularly reviewed and updated by design and deployment teams to reduce the likelihood of compromise within customer environments.
9	The ICS sensing technology is capable of working with correlation and aggregation technologies to allow for OT/IT sensing cross correlation and analysis.	✓	The Dragos Platform is able to ingest Windows host log files in addition to passive sensor-based network collection for asset and threat visibility. Support exists for sharing analytics and summarized data with common SIEM and network security tools like next generation firewalls (NGFW).

	OT Monitoring Functional Considerations For Natural Gas Transmission Pipeline Operators	DRAGOS Dragos Platform w/ Neighborhood Keeper	Notes
10	Technology has the capability of baselining normal ICS operations and can compare/detect abnormal operations from a known good baseline.	✓	Achieved through customer baselines as monitored within the Dragos Platform to show changes over time that indicate abnormalities that may require investigation.
11	Data at rest should be cryptographically protected (e.g., leverage NIST FIPS 140-3 certified cryptology to protect the data).	✓	FIPS 140-3 certified encryption algorithms used throughout Dragos technologies.
12	Technology has the capability to detect known unauthorized remote access operations.	✓	Communication between devices and Zones can be monitored so security teams can see and investigate potential unauthorized activity.
13	Technology has the capability to detect unauthorized movement from the IT to the OT environment including via non-Internet Protocol (IP) communication pathways.	✓	Communication between OT and other network environments (including IT or internet) can be monitored and analyzed depending on specific protocol(s), network architecture and sensor placement.
14	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.	✓	Detections in the Dragos Platform are mapped against tactics, techniques, and procedures (TTPs) as identified by the MITRE ATT&CK for ICS framework with clear guidance for practitioners.
15	Technology has analytic and detection capabilities, which are dynamically updatable leveraging timely, validated, and trusted external or internal threat intelligence.	✓	Dragos Threat Intelligence is dynamically added to Platform Knowledge Packs (KPs). KPs are manually assigned to Platform (not dynamic). Neighborhood Keeper participants get dynamic detections.
16	Technology has the capability to detect access credential misuse.	✓	Multiple detections exist for credential misuse in the Dragos Platform with prescriptive guidance through playbooks for investigation and response teams.
17	Technology to identify violations of implemented application allow listing policies enforced on IT and OT systems.	✓	Custom analytics and dashboards can be configured to detect and notify against application allow policy violations depending on customer requirements.
18	Does the Technology require any proprietary hardware or interoperable devices.	✓	No, the Dragos Platform and Neighborhood Keeper do not require proprietary technology. Dragos Platform can optionally be deployed in a virtualized environment, and Neighborhood Keeper is deployed in Amazon Web Services (AWS).

	OT Monitoring Functional Considerations For Natural Gas Transmission Pipeline Operators	DRAGOS Dragos Platform w/ Neighborhood Keeper	Notes
19	Does the solution provider account for changes in the regulatory environment in their solution.	✓	Dragos Platform is deployed and configured to meet regulatory requirements.
20	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.	✓	Dragos Platform delivers passive monitoring of ICS and IT protocols used for industrial operations, including baseline of assets, protocols, and function codes between approved, unknown, and transient assets.
21	The technology requires the capability to add/augment additional data points to improve and augment the quality of discovered devices.	✓	Dragos Platform supports user edit, user upload, API integration, and CMDB integration to improve and augment the quality of discovered devices.

About Dragos, Inc.

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, VISIT WWW.DRAGOS.COM.

THANK YOU