DRAGOS PLATFORM 2.X
SUPPLEMENTAL PROCEDURES

Version 1, Release 2

30 January 2025

Developed by Dragos and DISA for the DOD

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

Page

Dragos Platform 2.x Supplemental Procedures, V1R2
30 January 2025

DISA
Developed by Dragos and DISA for the DOD

iii

UNCLASSIFIED

LIST OF TABLES

Page

1. TECHNOLOGY IMPLEMENTATION CONSIDERATIONS

1.1 Security Assessment Information – Kibana

Dragos integrates Kibana as part of its platform to enhance data visualization and analysis capabilities. Kibana is a highly scalable interface for Log Stash and Elasticsearch that allows users to efficiently search, graph, analyze, and most importantly, understand a mountain of log data. Kibana is an open-source data visualization and exploration platform from Elastic that specializes in large volumes of streaming and real-time data. It is an analytics and visualization platform that builds on Elasticsearch to give users a better understanding of data.

By integrating Kibana into its platform, Dragos enhances its ability to provide comprehensive visibility, advanced analytics, and effective incident response tools tailored specifically for ICS and OT environments. This integration empowers organizations to protect their critical infrastructure more effectively by leveraging powerful data visualization and analysis capabilities.

1.2 Security Assessment Information – External Identity and Access Management

This STIG delegates certain security controls to an external Identity and Access Management system; delegated controls are out of scope of this STIG. Security controls in this STIG ensure the correct integration of this external system but thereafter rely on the security capabilities of this system. Security assessors should ensure the choice of Identity and Access Management system that the Dragos Platform is integrated with provides the following capabilities:

- **Identification of temporary or inactive users:** Users who have not logged in to the Dragos Platform within a designated, organizationally defined period must be identified by the external Identity and Access Management system, and organizationally defined remedial actions must be taken. Typical actions include removal of users from the authorized user's group or list maintained by the external Identity and Access Management system such that subsequent attempts to access the Dragos Platform are denied and appropriate logs, system events, and other tracking information is generated by the Identity and Access Management system.
- **Auditing of user accounts:** Users with access to the Dragos Platform must be audited via the external Identity and Access Management system for creation of new accounts, modification of existing accounts, or deletion/removal of user accounts.
- **Enforcement of invalid login attempt limits:** User attempts to log in to the Dragos Platform that fail must be managed by the external Identity and Access Management system and organizationally defined remedial actions must be taken. Typical actions include temporary account disablement, deprivileging of the user account, additional user monitoring, or broader account management actions.
- **Notice and consent:** The external Identity and Access Management system must present all users accessing the Dragos Platform with organizationally defined notice and consent notices on login events and deny access if the notice and consent is not accepted by the user.
- **Multifactor Authentication:** The external Identity and Access Management system must require all users accessing the Dragos Platform in normal operations, except as exceptional

DR and COOP processes require, to present multiple independent authentication factors, verify these factors, and deny access if any factors are not deemed verified in accordance with organizationally defined policy.

- **Password Policy Enforcement:** The external Identity and Access Management system must enforce organizationally defined password usage policies, including the reuse of passwords, minimum length requirements, complexity requirements, and expiration rules.

- **PKI user identity mapping:** The external Identity and Access Management system must map the authenticated identity extracted from a user's PKI certification credential to the individual user or group account provided during PKI-based authentication to the Dragos Platform.

- **Role and Privilege Changes:** When a device, host, user, or other roles or security-relevant attributes change, the external Identity and Access Management system must remove, delete, or render inoperable all associated and currently active authorizations to the Dragos Platform.

The Dragos Platform allows the use of a number of supported providers, including Active Directory, LDAP, and others. This STIG was tested and validated using LDAP.

1.3 Security Assessment Information – Jupyter

The Dragos Platform integrates Jupyter to enhance its data analysis, visualization, and reporting capabilities, providing users with tools for conducting detailed security investigations and analyses. By incorporating Jupyter Notebooks, the Dragos Platform empowers its users with advanced data analysis and visualization tools, enhancing their ability to investigate and respond to cybersecurity threats in industrial environments effectively. This integration supports a collaborative, transparent, and reproducible approach to cybersecurity analysis and reporting.

1.4 Security Assessment Information – Nginx

The Dragos Platform uses Nginx for several purposes related to web server and reverse proxy functionalities. By leveraging Nginx, the Dragos Platform enhances its ability to provide a robust, secure, and scalable environment for its ICS and OT security solutions. Nginx plays a crucial role in managing network traffic, ensuring high performance, and maintaining the security and availability of the platform.

1.5 Third-Party Services

The key third-party services used in the Dragos Platform are listed in the table below and accompanied by a description of the function the service performs.

Table 1-1: Third-Party Services

Service	Description
Platform Ui Logger (AFAIK)	Receives errors from UI JavaScript code to monitor for problems with UI code.
Asset inventory	Manages database of observed and imported assets.

Service	Description
Asset Map	Manages database of aggregate asset communication.
Baseline Service	Tracks baseline and deviations from normal network activity.
Detection Management Service	Maintains and distributes active state detections in the platform. File Service File repository for packet captures tasked to: - Sensors. - Knowledge packs. - Dragos Platform Package (DPP) files. - Files of interest extracted by sensors.
Gateway Service	Authentication gateway between users of the SiteStore and other services.
Midpoint Inventory Service	Keeps track of Sensors and is responsible for pairing Sensors to SiteStore.
Notification Service	Stores notifications created via sensor events and triggers.
Push Gateway	Component of Prometheus used for pushing metrics.
Report Service	Backs "Reports" panel in UI.
SiteStore Data Flow Service	Ingests events from sensors and performs data enrichment before data is indexed in Elasticsearch. Also creates notifications and sends updates to asset-inventory-service based on Sensor data.
Tasking Service	Sends task requests to Sensors, including: - Capturing packets based on BPF expression. - Installing DPP on Sensor.
Analytic Engine Service	Returns analytic metadata about characterizations and detection in the Platform. Also provides analytic metadata to additional services, such as Notification service.
Baseline Operator	Performs the detection logic to determine if a given type of traffic is a deviation from the baseline.
Baseline Stream Processor	Consumes and batches the data used for each type of baseline detection and sends the batches to the Baseline Operator.
Rabbitmq	Proxies some of the traffic between SiteStore and Sensors.
Legacy Sensor Adapter	Ingests Sensor data for the SiteStore and tasks Knowledge Packs to Sensors.