

UNCLASSIFIED



# **DRAGOS PLATFORM 2.X SECURITY TECHNICAL IMPLEMENTATION (STIG) OVERVIEW**

**Version 1, Release 1**

**26 September 2024**

**Developed by Dragos and DISA for the DOD**

UNCLASSIFIED

## 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
<b>1. INTRODUCTION.....</b>	<b>1</b>
1.1 Executive Summary.....	1
1.2 Authority.....	1
1.3 Vulnerability Severity Category Code Definitions.....	1
1.4 STIG Distribution.....	2
1.5 Document Revisions.....	2
1.6 Other Considerations.....	2
1.7 Product Approval Disclaimer.....	3
<b>2. ASSESSMENT CONSIDERATIONS.....</b>	<b>4</b>
2.1 Security Assessment Information - Applicability.....	4
<b>3. CONCEPTS AND TERMINOLOGY CONVENTIONS.....</b>	<b>5</b>
3.1 SiteStore – Elasticsearch.....	5
3.2 Authentications, Authorizations, and Access Interaction.....	6
3.3 Dragos Architecture.....	7
<b>4. GENERAL SECURITY REQUIREMENTS.....</b>	<b>10</b>
4.1 Hardening of Integrated External Services.....	10

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions .....	2

LIST OF FIGURES

	<b>Page</b>
Figure 3-1: SiteStore Components .....	5
Figure 3-3: Dragos Architecture .....	9

## 1. INTRODUCTION

### 1.1 Executive Summary

The Dragos Platform Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DOD) information systems. This document is meant for use in conjunction with other STIGs and appropriate operating system STIGs.

This STIG applies to the Dragos Platform 2.x. It assumes this product is installed and configured in accordance with the documented installation instructions provided by Dragos. This STIG also assumes delegation of certain security control implementation to external, integrated enterprise systems including a central identity and access management system, central logging management system, and others as noted below.

### 1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that “all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be [...] configured [...] consistent with applicable DOD cybersecurity policies, standards, and architectures.” The instruction tasks that DISA “develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible.” This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

### 1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will <b>directly and immediately</b> result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which <b>has a potential</b> to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which <b>degrades measures</b> to protect against loss of Confidentiality, Availability, or Integrity.

## 1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at <https://cyber.mil/>. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from <https://public.cyber.mil/>.

## 1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: [disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil). DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

## 1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

## 1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from [disa.stig\\_spt@mail.mil](mailto:disa.stig_spt@mail.mil). This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (<https://www.niap-ccevs.org/>) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<https://csrc.nist.gov/groups/STM/cmvp/>) IAW federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (<https://www.disa.mil/network-services/ucco>) IAW DODI 8100.04.



## **2. ASSESSMENT CONSIDERATIONS**

### **2.1 Security Assessment Information - Applicability**

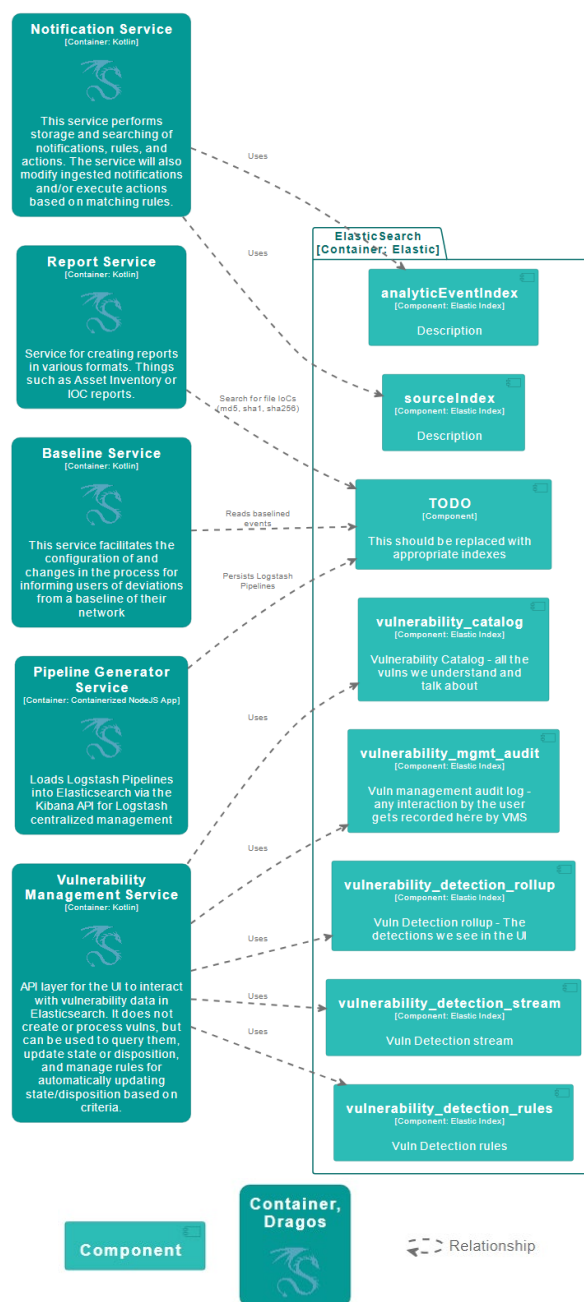
This STIG is not intended to provide technical guidance for all portions of the Dragos Platform. The Dragos Platform is a complex software system, and this STIG is applicable to only a subset of the potential set of components available for use in and with the Dragos Platform. All applicable subcomponents are part of default installation per the installation instructions provided with the platform.

### 3. CONCEPTS AND TERMINOLOGY CONVENTIONS

#### 3.1 SiteStore – Elasticsearch

The Dragos Platform uses several components from the Elastic Stack (also known as the ELK Stack) to store, search, analyze, and visualize data. These components include Elasticsearch, Logstash, and Kibana. By leveraging the Elastic Stack, the Dragos Platform enhances its capabilities in data collection, storage, search, and visualization, providing a comprehensive solution for ICS and OT cybersecurity.

**Figure 3-1: SiteStore Components**



### 3.2 Authentications, Authorizations, and Access Interaction

- **User's device to Nginx:** HTTP requests sent to the SiteStore are first received by Nginx as a reverse proxy. If the request is not over HTTPS, a redirect is returned.
- **Nginx to Dragos IdP:** Nginx (ngx\_http\_auth\_request\_module) calls IdP's request verification endpoint to verify authentication and authorization for requests destined for applications that do not handle auth tokens. The request may include parameters such as whether that route should allow cookie-based authentication, ignore API keys, or require certain permissions. If successful, responses include setting the dragos-auth-token cookie and legacy auth token headers to send downstream with the routed request. For routes to applications that handle server-signed auth tokens themselves, this interaction is skipped. For routes to applications that handle server-signed and API key auth tokens themselves, this interaction is skipped. The goal is for this interaction to decrease over time as more internal applications are upgraded; however, this interaction is still needed to continue to support third-party web UIs (such as Grafana).
- **Dragos IdP to an LDAP server:** When a user's device requests an auth token (a.k.a. logging in) using an LDAP authentication provider, the IdP binds to the LDAP server to authenticate the credentials and retrieve user and group information.
- **To an OIDC provider:** When a user's device requests an auth token (a.k.a. logging in) using an OIDC authentication provider, the IdP sends a few requests to the provider both before the user device is redirected to the provider and after the user device is redirected back from the provider to the SiteStore.
- **An updated, in-house API application (ex. Asset Inventory Service) to IdP:** Upon receiving a request with a server-signed auth token, the application will attempt to verify the JWT's signature by fetching the JWKS (JSON Web Key Set) from the Dragos IdP's API. After using the appropriate public key from the JWKS and if the subject is an identity type, the application will fetch the identity from the IdP. The fetched identity information will include permissions and allow the application to determine if the request has sufficient authorization.
  - Additionally, applications may also request an auth token with an application subject type to make requests to other application APIs. This application-subject auth token is fetched from the Dragos IdP's API using a shared secret.
- **To another updated, in-house API application:** When making a request to another application's API on behalf of the requester who does not have permissions to perform the request directly themselves, the application's auth token can be accompanied by an X-On-Behalf-Of HTTP header with the original requester's identity ID.
- **To a legacy-auth, in-house API application:** If an application has not been updated to handle server-signed auth tokens, a legacy auth token can be manufactured and sent. The legacy-auth application trusts that the legacy auth token is accurate and was not manufactured by a malicious party that gained internal access to the cluster.
- **Data Broker to Filter Service:** Upon a request to Data Broker with an auth token that resolves to an identity with an assigned scope, Data Broker will attempt to fetch any needed scoping filters from Filter Service.

### 3.3 Dragos Architecture

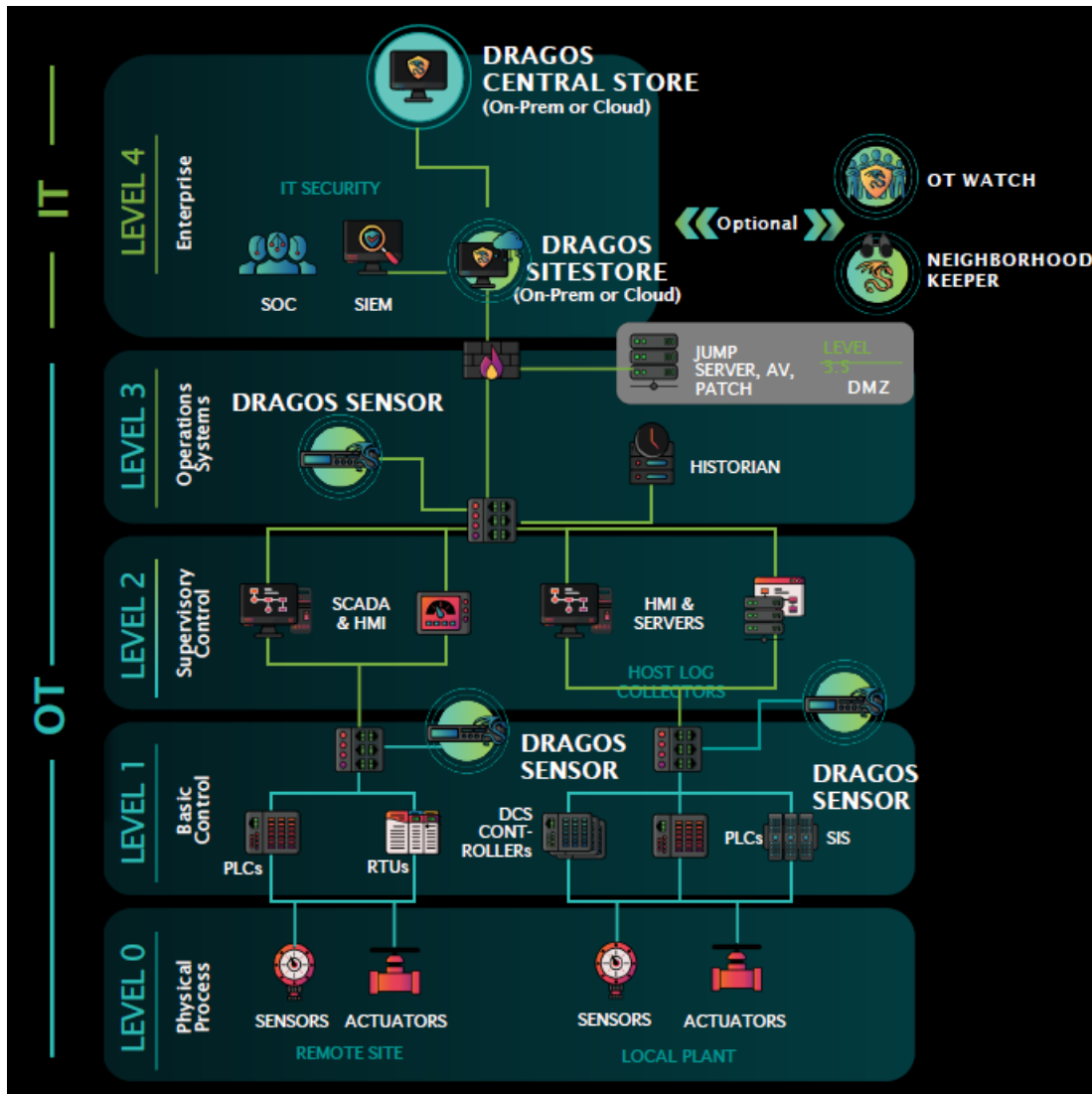
The Dragos Platform architecture is designed to provide a comprehensive cybersecurity solution tailored for industrial control systems (ICS) and operational technology (OT) environments. It integrates various components to ensure effective data collection, processing, storage, analysis, and visualization.

#### Summary of the Dragos Platform Architecture:

1. Data Collection:
  - Beats:
    - Filebeat: Collects and forwards log files from ICS and OT devices.
    - Metricbeat: Gathers system and service metrics to monitor device performance and health.
    - Packetbeat: Captures network traffic, providing insights into communication patterns and detecting anomalies.
    - Winlogbeat: Collects Windows event logs, crucial for monitoring and forensic analysis.
  - Dragos Agents:
    - Endpoint Agents: Deployed on ICS/OT endpoints to gather telemetry, logs, and other relevant data, ensuring comprehensive visibility into the operational environment.
2. Data Ingestion and Processing:
  - Logstash:
    - Data Parsing and Transformation: Logstash processes raw data, transforming and enriching it with additional context such as geolocation and threat intelligence.
    - Pipeline Management: Manages multiple data pipelines to ensure data from various sources is processed and forwarded correctly.
3. Data Storage and Indexing:
  - Elasticsearch:
    - Centralized Data Repository: Acts as the core data store, holding all collected logs, events, and telemetry data.
    - Indexing: Structures data in an indexed format, allowing for fast and efficient searches and queries.
    - Scalability: The distributed nature allows horizontal scaling, accommodating increasing data volumes.
4. Data Analysis and Correlation:
  - Analytics Engine:
    - Rule-Based Detection: Uses predefined rules to detect known threats and anomalies within the data.
    - Machine Learning: Employs machine learning algorithms to identify patterns and anomalies that may indicate emerging threats.
    - Event Correlation: Correlates events from multiple sources to identify coordinated attacks or security incidents.
5. Data Visualization and Reporting:
  - Kibana:

- Custom Dashboards: Provides interactive dashboards and visualizations to help users interpret and analyze data.
  - Visual Analysis: Enables security analysts to explore data trends, detect anomalies, and gain insights through visual representations.
  - Reporting: Facilitates the creation of detailed reports for stakeholders, enhancing transparency and communication.
6. Threat Intelligence
- Dragos Threat Intelligence:
    - Threat Database: Integrates with a comprehensive threat intelligence database, providing context on known threats, adversaries, and tactics.
    - Automatic Updates: Regularly updates with the latest threat intelligence, ensuring the platform remains current with evolving threats.
    - Contextual Analysis: Provides contextual information about detected threats, helping analysts understand the significance and potential impact.
7. Incident Response and Forensics:
- Incident Response Tools:
    - Timeline Reconstruction: Allows analysts to reconstruct the sequence of events leading up to and during an incident, aiding in root cause analysis.
    - Detailed Forensics: Provides tools for deep forensic analysis, helping to understand the scope and impact of security incidents.
8. Integration and Extensibility:
- APIs and Integrations:
    - API Access: Offers APIs for integrating with other security tools and platforms, enhancing overall security posture.
    - Third-Party Integrations: Supports integrations with various third-party tools and services, allowing organizations to leverage existing investments in security infrastructure.
9. Security and Compliance:
- Security Features:
    - Access Controls: Implements robust access control mechanisms to ensure only authorized users can access sensitive data.
    - Encryption: Uses encryption to protect data in transit and at rest, ensuring data integrity and confidentiality.
    - Compliance: Helps organizations meet regulatory compliance requirements by providing detailed logs, reports, and audit trails.

Figure 3-3: Dragos Architecture



## **4. GENERAL SECURITY REQUIREMENTS**

### **4.1 Hardening of Integrated External Services**

Dragos Platform must use external services (refer to the Supplemental document). The deployment and management of these services is outside the scope of this STIG. All services that are used by Dragos Platform must be hardened to an appropriate level via a well-defined RMF, including the use of associated STIGs as applicable. Failure to do so may allow compromise of data, managed systems, user operations, or other impacts via lateral attacks from these integrated systems.