ADVISORY

The Dragos Platform Enables Federal Agencies to Secure Operations and Meet Mission Requirements

THE U.S. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) issued a Binding Operational Directive regarding asset discovery, vulnerability detection, and reporting practices for Federal Civilian Executive Branch (FCEB) agencies.

Operational technology (OT) and industrial control systems are critical to the functions of both our federal government and Defense Department. CISA's 23-01 BOD emphasizes the importance of asset and vulnerability management across both IT and OT.

The Dragos Platform, along with our threat intelligence and managed services programs, are specifically designed and continuously updated to secure the world's most critical infrastructures. The Dragos Platform enables our customers and partners to meet (and exceed) regulatory requirements and best security practices. Our intelligence and services teams ensure network defenders have the most up-to-date information and capabilities available to triage and respond to threats.

CISA BOD Requirement	How Dragos Helps Agencies Meet the Requirement
Automated asset discovery every 7 days	The Dragos Platform analyzes multiple data sources including protocols, network traffic, data historians, host logs, asset characterizations, and anomalies to provide visibility of your ICS/OT environment. Asset discovery is **continuous** — exceeding the requirements of this BOD.
Vulnerability enumeration across all discovered assets every 14 days	Dragos is the only ICS/OT cybersecurity company to provide corrected, enriched, prioritized vulnerability guidance that allows customers to manage the full lifecycle of specific vulnerabilities in their environment through continuous, automated collection and analysis. Organizations that have segregated OT/ICS networks will benefit from the vulnerability disposition tracking built-in to the Dragos Platform, alongside both remediation and mitigation guidance.
Update vulnerability detection signatures within 24 hours	The Dragos Platform was built for heavily regulated environments here any change must be validated, tested, and documented — even on a passive platform such as Dragos. Today, vulnerability information is published in knowledge packs; these knowledge packs deliver new protocol classifications, threat detections, and vulnerability information at once to minimize the amount of regulatory-required testing.
Initiate automated ingestion of detected vulnerabilities into the CDM Agency Dashboard within 72 hours of discovery completion	The Dragos Platform CentralStore provides consistent, centralized risk management and reporting — so you can easily transfer the information to the CDM Agency Dashboard. Both the Dragos Platform and CentralStore provide users with data visually, and through a robust API, allowing for ease of integration into existing workflows and processes.
Develop and maintain the operational capacity to initiate on-demand asset discovery and vulnerability enumeration	The Dragos Platform exceeds this requirement, while ensuring that the discovery of assets and the enumeration of vulnerabilities does not impact OT/ICS environments that cannot tolerate asset discovery scanning or active vulnerability enumeration. The Dragos Platform provides continuous monitoring and vulnerability identification — all while not impacting processes and assets under control.

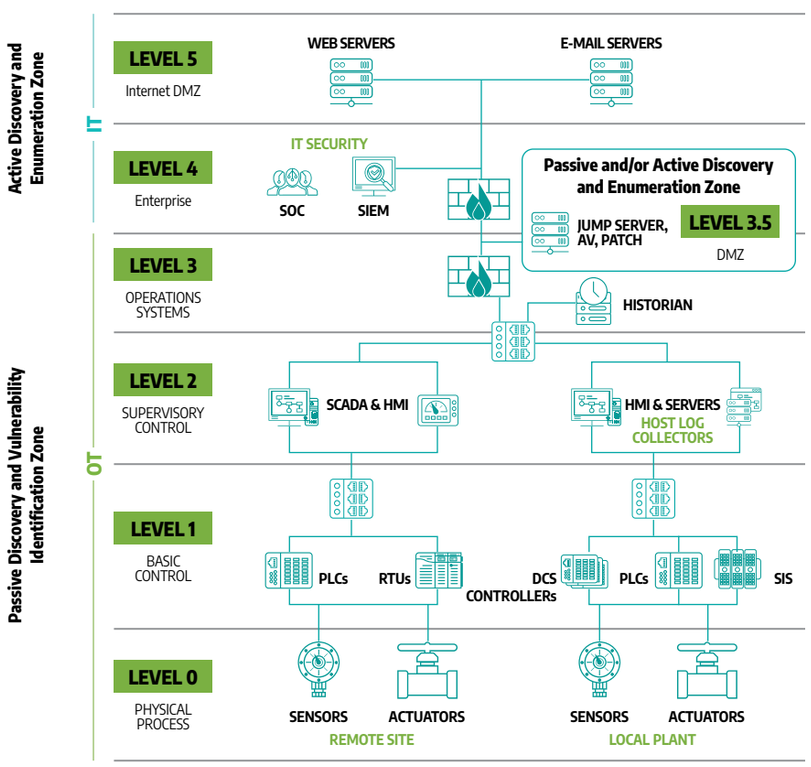
EXPERT GUIDANCE AND KEY CONSIDERATIONS

Implementing a Blended Active/Passive Asset Discovery and Vulnerability Detection Program Across IT and OT Networks

This BOD highlights two methods that can be used to perform asset discovery and vulnerability enumeration:

- **Active:** communications between a discovery tool and the target device across the network space
- **Passive:** monitoring traffic and analyzing it for assets, communications protocols, and vulnerabilities

Active and passive methods can achieve the goals of this BOD on enterprise IT networks, but OT/ICS systems require a more nuanced approach. Especially in more modern systems where the ethernet network is part of the control system, care must be taken not to alter the OT/ICS environment. The risk of introducing technologies that can interact with OT/ICS systems must be carefully managed, both to prevent accidental outages and to avoid providing adversaries with a means by which to interact with the OT/ICS system directly.



IMPORTANT QUESTIONS TO CONSIDER

Ask yourself these questions as you work toward meeting these requirements:

DO I HAVE AN INDUSTRIAL DMZ THAT SEPARATES MY IT FROM OT NETWORKS?
If not, limit any active scanning only to subnets that are 100% known to only contain IT assets; use passive monitoring to validate the rest of the network space.

DO I HAVE IT ASSETS THAT ARE DUAL USE FOR BOTH IT AND OT?
If so, separate these functions to separate physical machines if possible.

DO MY IT AND OT ENVIRONMENTS SHARE IDENTITY MANAGEMENT/ AUTHENTICATION SERVICES?
If so, separate these services, one for IT and one for OT. In 2021, 100% of threat actor compromises leverages a shared authentication ecosystem to cross from IT into OT.

Once assets are properly segregated, the process of building a blended program is much simpler. By creating scanning boundaries that align with the IT/OT DMZ, not only is process safety and integrity maintained, but lines of effort and responsibility remain clear-cut between IT and OT teams.

A common question as work progresses will be "Can't I actively interact with at least SOME assets in the OT environment?" The answer is "it depends." Always talk with your on-site asset operators who can guide you in making risk-informed decisions.

CLICK OR TAP BELOW TO DOWNLOAD ADDITIONAL RESOURCES

For more information or to schedule a demo of the Dragos Platform, visit www.dragos.com