SOLUTION BRIEF

DRAGOS
SAFEGUARDING CIVILIZATION

# Level Up: CMMC 2.0 Cybersecurity Practices

## Leverage Dragos technology and services to align with CMMC guidance

Cyber threat actors continue to target the Defense Industrial Base (DIB) and the supply chain of the Department of Defense (DoD). The DIB sector consists of more than 300,000 companies that contribute toward the operations of DoD. In concert with the DoD, the Office of the Under Secretary of Defense for Acquisition and Sustainment launched the Cybersecurity Maturity Model Certification (CMMC) to safeguard sensitive information and operations from increasingly frequent and sophisticated cyberattacks.

This document summarizes how Dragos helps minimize barriers to compliance with CMMC 2.0 requirements and accelerate cyber maturity for ICS/OT asset owners under contract with the DoD.

## How Dragos Can Help OT Security Environments Leveraging CMMC 2.0

Dragos is on a mission to safeguard civilization. To that end, Dragos delivers critical elements for implementing CMMC 2.0 practices, with a focus on improving the success rate of cybersecurity programs for ICS environments and OT networks. Dragos provides unmatched visibility of assets, coverage of OT cybersecurity threats, and expert support through a combination of the Dragos Platform, Threat Intelligence, and Professional Services.

| SOLUTION | HOW IT HELPS |
|---|---|
| **Dragos Platform** | **Automate Key CMMC Security Controls at Scale with Intelligence Driven Software.**<br>• Visibility into asset inventory, key vulnerabilities & mitigation, analysis of network traffic, and forensic records<br>• Detection of OT cyber threats that integrates threat intelligence research into adversary TTPs to deliver high-fidelity detection with low noise ratio<br>• Response information to simplify investigation, with expert playbooks to automate and streamline incident resolution |
| **Professional Services** | **Establish CMMC 2.0 Practices and OT Cybersecurity with Expert Resources**<br>• Dragos has the largest and most experienced private team of OT security practitioners<br>• From architecture assessments and program evaluations to incident response resources, we are here to help you win the fight |
| **Threat Intelligence** | **Maintain Situational Awareness into New Threats, Attacks, & Vulnerabilities**<br>• Timely insight into OT adversary campaigns, detailed TTP info, and practical vulnerability mitigation advice, with key insights from attacks and incidents |
| **Success Focus** | **Training, Resources, & Community Connection to Increase Your Success**<br>• OT security is a specialized domain Dragos helps you navigate the issues, build expertise, and engage with professionals beyond your organization to strengthen the collective defense of the ICS/OT community |

## Mapping CMMC 2.0 Domains to Dragos Solutions

CMMC 2.0 launched in November 2021 to streamline requirements to the interim rules established in 2020. The CMMC 2.0 model consists of 14 domains, with required practices related to each of them.

The following is a summary of the ways we can help the DIB meet CMMC 2.0 compliance objectives:

| CMMC 2.0 DOMAIN | DOMAIN DESCRIPTION | DRAGOS CAPABILITIES - DETAILED |
|---|---|---|
| Access Control (AC) | Establish access requirements, controls, and authorizations for system users and processes. | Dragos Platform integrates with firewalls to provide insights into access control policies and monitors OT network traffic to help validate the effectiveness of Access Controls. Baseline and behavioral threat detection will alert about unauthorized assets, users, or communication paths. This includes documenting network logon attempts and analyzing traffic to detect potential attacks and threat behaviors.<br>Dragos is not an Identity Access Management (IAM) solution, but it can be configured to conform with CMMC 2.0 Access Control practices. |

| CMMC 2.0 DOMAIN | DOMAIN DESCRIPTION | DRAGOS CAPABILITIES - DETAILED |
|---|---|---|
| Access Control (AC) *continued* | | Dragos Professional Services support the development and assessment of ICS/OT IAM processes. Our team conducts comprehensive architecture reviews to identify remote access connections used by third parties, evaluate the policies and controls used to manage connectivity, and recommend changes to secure access. |
| Asset Management (AM) | Identify and document assets. | Dragos Platform automatically generates an asset inventory and asset profiles, including software versions, and map assets to zones to simplify visualization of traffic between them.<br>Dragos Platform links vulnerabilities to assets for faster response and prioritized by their corrected CVSS scores through the lens of ICS/OT from Dragos Threat Intelligence.<br>Dragos Platform monitors OT network activity and changes to log communication sessions, command execution, network telemetry, and more. The system analyzes the data for anomalies and threats, preserving artifacts for use in forensics and root cause analysis.<br>OT Watch supports management of the Dragos platform, with expert-led support to enable customers to ramp up operations of asset and change management procedures quickly. Dragos OT Watch proactively monitors changes and triages detection alerts.<br>Dragos Professional Services can help with the design and validation of CMMC 2.0 compliant asset management practices and initial assets inventories by conducting thorough architecture reviews, compromise assessments, and vulnerability assessments. |
| Awareness & Training (AT) | Conduct security awareness activities and conduct training. | Dragos Academy 5-Day ICS Training course provides skills and knowledge required to develop an internal ICS/OT focused awareness program.<br>Dragos Threat Intelligence can be used for awareness Threat Groups, campaigns, and attacks targeting critical infrastructure industrial operations. Expert technical analysis and guidance on malware, exploits, and vulnerabilities train security professionals to assess and hunt for similar activity in their facilities.<br>Dragos is a leader in the ICS/OT security community and delivers regular public briefings, educational resources, and guidance. |

| CMMC 2.0 DOMAIN | DOMAIN DESCRIPTION | DRAGOS CAPABILITIES - DETAILED |
|---|---|---|
| Audit & Accountability (AU) | Define audit requirements, perform auditing, and review logs. Identify, manage, and protect audit information. | Dragos Platform enables the performance of audits of ICS/OT network architecture, vulnerability/patch management procedures, and compliance to change management practices.<br>Dragos Professional Services provides incident response planning, collection management framework optimization, and helps teams identify potential areas for remediation prior to an audit. |
| Configuration Management (CM) | Establish configuration baselines, perform configuration, and change management. | Dragos Platform tracks and reports certain baseline deviations in asset configuration to support configuration management monitoring.<br>Dragos Professional Services support the design and assessment of configuration management procedures in ICS/OT environments. |
| Identification & Authentication (IA) | Grant access to authenticated entities. | Dragos Platform notifies on new or unauthorized devices detected and monitors traffic to help validate security controls. Baseline and behavioral threat detection will alert about unauthorized assets, users, or communication paths. This includes documenting network logon attempts and analyzing traffic to detect potential attacks and threat behaviors.<br>Dragos Professional Services helps customers develop and modify policies and procedures during architecture and program reviews. |
| Incident Response (IR) | Develop, implement, and test an incident response plan. Detect and report events, and perform post-incident reviews. | Dragos Platform monitors activity in ICS/OT environments, alerting on events that may pose a risk, and providing context and forensic information to aid in the rapid prioritization and investigation of incidents.<br>Dragos Platform integrates with firewalls and endpoint security platforms for rapid isolation of infected systems and termination of connections. Integrations with popular SOC automation tools such as a SIEM enable rapid investigation<br>To develop an incident response process, Dragos provides guidance in the form of playbooks. Written by senior incident responders with experience responding to threat events in ICS/OT environments, these built-in playbooks are available for turnkey use or as a starting point to create your own.<br>Dragos OT Watch service is available to support the day-to-day incident response process by triaging high severity alerts and assisting with insights from the platform in an event of an incident.<br>Dragos Professional Services helps customers prepare for, respond to, and recover from cyber incidents. Architecture reviews, incident response planning, tabletop exercises, and incident response retainers help to ensure comprehensive response capabilities. |

| CMMC 2.0 DOMAIN | DOMAIN DESCRIPTION | DRAGOS CAPABILITIES - DETAILED |
|---|---|---|
| Maintenance (MA) | Manage maintenance. | Dragos Professional Services supports the design and assessment of change management procedures, vendor management programs, and patching and updating procedures. |
| Media Protection (MP) | Protect and control media at rest at rest and in transit. | Dragos Professional Services conducts architecture reviews and compromise assessments to help with the design and validation of CMMC 2.0 compliant media protection controls. |
| Personnel Security (PS) | Screen personnel and protect confidential user information during personnel actions. | Dragos Professional Services can help evaluate and recommend steps to mature plans, procedures, technologies, and controls that improve the culture of cyber security. Objectives for workforce development include implementing workforce controls, increasing cybersecurity awareness, assigning cybersecurity responsibilities, developing the cybersecurity workforce, and related management activities.<br>Dragos employees are screened and appropriate due diligence including background checks, and clearance, when necessary, are conducted. |
| Physical Protection (PE) | Limit physical access. | Dragos Professional Services provides proactive risk analysis, architecture reviews, and incident response planning including physical security plans.<br>Dragos does not offer any physical security controls. |
| Risk Assessment (RA) | Identify, evaluate, and manage risk. | Dragos Platform actively monitors and evaluates network traffic to identify indicators of compromise and threat behaviors that may indicate an attack, including remote access connections from third parties, one of the common attack methodologies used by adversaries.<br>Dragos Professional Services helps customers assess risk comprehensively, evaluating the business consequences of threats and vulnerabilities and analyzing how resilience measures can mitigate risks. The team evaluates different scenarios, such as ransomware, insider threats, business system compromises that pivot to the ICS/OT network, third party risks that impact critical functions, and more. |
| Security Assessment (SA) | Develop and manage a system security plan and security controls. Perform a code review where necessary. | Dragos Platform actively monitors and evaluates network traffic to identify indicators of compromise and threat behaviors that may indicate an attack, including remote access connections from third parties, one of the common attack methodologies used by adversaries.<br>Dragos Platform can assist with identifying insecure architectures and protocols across OT environments including testing environments. |

| CMMC 2.0 DOMAIN | DOMAIN DESCRIPTION | DRAGOS CAPABILITIES - DETAILED |
|---|---|---|
| Security Assessment (SA) *continued* | | Dragos Threat Intelligence is leveraged as a component of cybersecurity project life cycles to inform best practices and provide alternate mitigations where needed.<br>Dragos Professional Services are available to help you assess and build your cybersecurity program. Our team can conduct in-depth reviews and recommendations on your policies and procedures, roles and responsibilities, and critical controls.<br>Dragos Professional Services are available to support the development and assessment of cybersecurity requirements across all phases of ICS Cybersecurity project management. |
| Systems & Communications Protection (SC) | Define security requirements and controls for systems and communications. | Dragos Platform provides asset visibility & threat detection, vulnerability management, and response playbooks – all of which are critical to protecting against cyber risk.<br>✓ Detect certain configuration changes<br>✓ Identify ICS assets and firmware versions.<br>✓ Validate network segmentation<br>✓ Monitor remote and external network communication<br>Dragos Professional Services are available to assist in the instruction, development, evaluation, and assessment of controls to protect OT/ICS systems against cyber risks. |
| System & Information Integrity (SI) | Identify and manage information system flaws and identify malicious content. Perform network and system monitoring along with advanced email protections. | Dragos Platform provides logical segmentation maps, network communication and asset visibility, and integrates with firewalls. Dragos informs on unauthorized users or devices that transfer of data over unencrypted protocols.<br>Dragos Professional Services can evaluate architecture and network design and recommend changes to be in accordance with best practices and CMMC 2.0. |


## About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. 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 our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.

info@dragos.com @DragosInc @Dragos, Inc.