SOLUTION BRIEF

OT Cybersecurity Solutions for the Cybersecurity Capability Maturity Model (C2M2)

How Dragos Supports OT Environments Leveraging C2M2

The expansive coverage and level of detail in cybersecurity frameworks like the Cybersecurity Capability Maturity Model (C2M2) can be challenging for teams evaluating their maturity and risk exposure. Dragos is uniquely positioned to help operational technology (OT) teams understand their current cybersecurity posture, identify gaps, and provide guidance towards maturity goals.

Our comprehensive approach for industrial cybersecurity environments enables teams to implement the controls required to meet the security demands that OT environments require. The Dragos Platform is a technology platform that provides in-depth visibility of industrial assets, coverage of OT cybersecurity threats enabled by Dragos Threat Intelligence, as well as expert support through our Professional Services team.

Dragos Platform

Automate Key C2M2 Security Controls at Scale

- Visibility into asset inventory, key vulnerabilities & mitigation, analysis of network traffic, and forensic records
- Detection of OT cyber threats that integrates threat intelligence research into adversary TTPs to deliver high-fidelity detection
- Response capabilities to automate and streamline incident investigation and resolution

OT Expert Services

Build Your OT Security Program & Architecture

Dragos operates a deep bench of the most elite OT security practitioners—including those that helped create and evolve C2M2—ready to evaluate your cyber capabilities and bolster your program resources

OT Threat Intelligence

Maintain Situational Awareness into New Threats, Attacks, & Vulnerabilities

Dragos analysts work around the clock offer timely insight into OT adversary activities based on real-world OT attacks and incidents

Community Defense

Connect with Other OT Security Experts & Grow Your Skills

Dragos helps connect OT operators and cyber defenders with insights and intelligence from across the community, collaborative training, and facilitation of information sharing to strengthen the collective defense

Cybersecurity Capability Maturity Model (C2M2)

C2M2 provides a structured way to evaluate cybersecurity capabilities based on a graduated scale of maturity. The capabilities are divided into 10 main domains, with several sub-domains each. Maturity is broken into four Maturity Indicator Levels (MILs), MIL0 through MIL3, which apply independently to each domain and are judged on a dual progression of maturity. The framework evaluates maturity against both an approach progression and a management progression.

Below is a summary of each domain, along with a detailed summary of Dragos capabilities that can help organizations improve their maturity levels in each domain.

C2M2 DOMAIN	DOMAIN DESCRIPTION	DRAGOS CAPABILITY - DETAILED
Asset, Change and Configuration Management (ASSET)	Manage the organization's IT and OT assets, including both hardware and software, and information assets commensurate with the risk to critical infrastructure and organizational objective	Dragos Platform provides the ability to: • Create an asset inventory and asset profiles, including software versions, • Monitor OT network activity, analyzing traffic to identify changes to the environment, • Organize assets into zones to simplify visualization of assets and traffic, • Map vulnerabilities to the assets, • Monitor asset changes, communication sessions, command execution, and network telemetry, and • Analyze that data to identify irregularities and detect threats. The information logged by the system can also be used for in-depth forensics and root cause analysis. The optional OT Watch program provides additional asset and change management operational support, with Dragos-led management of the platform, including regular monitoring and reporting. Additionally, Dragos Services offers a suite of Architecture Review services to help create asset inventories and identify the riskiest vulnerabilities and threats within them.

C2M2 DOMAIN	DOMAIN DESCRIPTION	DRAGOS CAPABILITY - DETAILED
Threat and Vulnerability Management (THREAT)	Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (such as critical, IT, and operational) and organizational objectives	The Dragos Platform provides real-time views into threats and vulnerabilities, with threat intelligence-driven insights that help you prioritize incidents and effectively manage vulnerabilities. The Dragos Platform monitors traffic and provides real-time alerts in a detection dashboard that breaks alerts into four quadrants based on the type of detection mechanism: Configuration, Modeling, Indicator, or Threat Behavior. Alerts include contextual details like asset information, detection specifics, mapping to the MITRE ATT&CK for ICS Framework, and links to both the event data and raw traffic data in the database. Additionally, the platform supplies investigative playbooks to enable rapid analysis and investigation of alert information. Dragos Platform also maps vulnerabilities against asset inventories. The platform layers timely threat intelligence into vulnerability management capabilities, adding context based on adversary behavior and exploits found in the wild. This intelligence provides access to newly discovered vulnerabilities, corrected severity scores, prioritization (Now, Next, Never), impact guidance, recommendations, mitigating recommendations, and information about how attackers are exploiting certain flaws. This vulnerability intelligence can also be delivered as a WorldView threat intelligence subscription via email, portal, API and other methods. • Additionally, the platform can be used to move beyond vulnerability assessment to manage the disposition of the assessed vulnerability and audit any changes to its state. Finally, Dragos Services offers experts available to conduct Vulnerability Assessments, Compromise Assessments, and Threat Hunts as part of its retainer services.

C2M2 DOMAIN	DOMAIN DESCRIPTION	DRAGOS CAPABILITY - DETAILED
Risk Management (RISK)	Establish, operate, and maintain an enterprise cyber risk management program to identify, analyze, and respond to cyber risk the organization is subject to, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.	The Dragos Platform provides critical controls to identify, manage, and reduce OT Risk. Key programmatic elements supported include: • Asset management, • ICS network monitoring, • Vulnerability management, • And threat detection. Dragos Professional Services runs a team of elite OT risk managers who can evaluate OT risk and review architectures and processes to assess risk and current C2M2 status. Many experts on the services team had a hand in the development of C2M2 standards and are perfectly positioned to guide a program's maturity progression. Dragos risk management consultants focus on identifying, mitigating, monitoring and controlling operational risks.
Identity and Access Management (ACCESS)	Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.	Dragos Platform does not directly manage identities or access management policies. However, Dragos technology can validate access management policies and controls and Dragos professional services can provide risk-based assessment of access control architectures and roadmaps to facilitate advancing maturity. Dragos Platform integrates with firewalls to provide insights into access control policies. The platform's monitoring of OT network traffic can help validate the effectiveness of access controls by documenting network logon attempts and analyzing traffic to detect potential attacks and threat behaviors. Dragos Professional Services can help to review access architectures and processes in the context of C2M2 to plan advances in maturity. Experienced OT security practitioners on the services team can guide improvements to access control policies, network segmentation, multi-factor authentication (MFA), use of jump hosts, and active monitoring of OT networks and traffic.

C2M2 DOMAIN	DOMAIN DESCRIPTION	DRAGOS CAPABILITY - DETAILED
Situational Awareness (SITUATION)	Establish and maintain activities and technologies to collect, monitor, analyze, alarm, report, and use operational, security, and threat information, including status and summary information from the other model domains, to establish situational awareness for both the organization's operational state and cybersecurity state.	Dragos provides situational awareness into OT Security threats via the Dragos Platform, Neighborhood Keeper, OT Watch, and Threat Intelligence. The Dragos Platform delivers real-time situational awareness with threat and vulnerability dashboards based on in-depth logging and analysis of OT network activity, including: • traffic, • connectivity attempts, • user behavior, • file downloads, and • device commands. The platform analyzes OT traffic to detect potential threats and create alerts that can be sent to SIEM, SOAR and other SECOPS process tools. External to the platform and customer operations, the Dragos OT Threat Intelligence group conducts in-depth research into and analysis of OT adversaries, threat activity groups, vulnerabilities, and incidents worldwide. Dragos Threat Intelligence powers advanced detection and risk management features in Dragos Platform, including automated intelligence-based threat detections, vulnerability prioritization and mitigation recommendations, and response playbooks. Threat intelligence can also be consumed through the Dragos WorldView subscription service in human readable formats or API-delivered feeds. The free, opt-in Neighborhood Keeper program extends situational awareness to include asset, threat, and vulnerability analysis shared across OT environments leveraging the Dragos Platform. It delivers pooled intelligence insights that strengthen the collective defense. The optional addition of OT WATCH provides services to proactively triage incidents, escalate alert, and handoff context to Incident Response teams. Staffed by our team of expert hunters and responders, the Dragos Platform delivers that added insight from seasoned OT security practitioners.

C2M2 DOMAIN	DOMAIN DESCRIPTION	DRAGOS CAPABILITY - DETAILED
Event & Incident Response, Continuity of Operations (RESPONSE)	Establish and maintain plans, procedures, and technologies to detect, analyze, mitigate, respond to, and recover from cybersecurity events and incidents and to sustain operations during cybersecurity incidents, commensurate with the risk to critical infrastructure and organizational objectives.	Dragos Platform monitors traffic and provides real-time detection and alerting of potential security events. The platform then provides the forensic information base, workflows, and integrations to facilitate rapid investigation and response to incidents. Integrations with SIEM and SOC automation tools forward Dragos Platform information to SOC analysts in the dashboards they use most. Integrations with firewalls and endpoint security platforms make it easier for incident responders to rapidly isolate problematic endpoints. Meantime, the platform delivers incident response playbooks that provide specific best practice guidance to dealing with incidents. These playbooks distill information about adversary TTPs researched by Dragos Threat Intelligence analysts and guidance written by senior incident responders from the Dragos Professional Services team based upon their experience of investigating and responding to events in OT environments. They are written to guide your staff through the investigation process as if they were sitting next to the authors. Customers' security teams can choose to leverage these in-built playbooks as-is, or they can modify them or even create custom playbooks. Additionally, customers can bolster in-house response resources with the optional OT Watch service, which offers Dragos-led triage of high-severity alerts delivered by the platform. In addition, the Dragos Incident Response (IR) Service helps organizations prepare for, respond to, and recover from cyber incidents in industrial environments. Our team of experienced ICS incident responders–backed by Dragos' ICS threat intelligence and the industrial-specific technology of the Dragos Platform–offers both rapid response availability and retainers to help ICS security personnel resolve crisis situations as quickly as possible.

C2M2 DOMAIN	DOMAIN DESCRIPTION	DRAGOS CAPABILITY - DETAILED
Third-Party Risk Management (THIRD-PARTIES)	Establish and maintain controls to manage the cyber risks arising from suppliers and other third parties, commensurate with the risk to critical infrastructure and organizational objectives.	The Dragos Platform actively monitors network traffic, including remote access connections from third parties, which stands as one of the most common attack methodologies used by adversaries. The platform can be used to evaluate traffic to identify indicators of compromise and threat behaviors that may indicate an attack. Through Dragos Professional Services Architecture Review Suite, Dragos OT security experts can identify remote access connections used by third parties, evaluate the policies and controls used to manage that connectivity, and can recommend changes to technologies, policies, and procedures to make that access more secure. Additionally, the Dragos services team can help evaluate third parties in the context of critical OT operations through independent testing, code reviews, vulnerability discovery and secure software development processes. The Dragos team can also work with customers to identify steps that can reduce assessed third-party risks and mature the cybersecurity posture of an organization, including establishing a methodology for third-party selection and maintaining comprehensive risk management procedures.
Workforce Management (WORKFORCE)	Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.	Dragos provides training resources for ICS cyber security professionals through Dragos Academy, as well as ongoing briefings on new threat intelligence findings. Dragos Program Assessment and Capability Maturity Assessment 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. Dragos does not provide broader organizational cybersecurity awareness training.

C2M2 DOMAIN	DOMAIN DESCRIPTION	DRAGOS CAPABILITY - DETAILED
Cybersecurity Architecture (ARCHITECTURE)	Establish and maintain the structure and behavior of the organization's cybersecurity architecture, including controls, processes, technologies, and other elements, commensurate with the risk to critical infrastructure and organizational objectives.	Dragos provides both the controls to augment OT security architecture as well as expert services to help evaluate and improve risk posture of the architecture. Dragos Platform bolsters critical controls to around the OT architecture, including asset management, threat monitoring, vulnerability management, and incident response. Through Dragos Services, the Architecture Review Suite evaluates OT architectures to provide an understanding to the most critical ICS systems in a given environment, and the potential consequences of a cyber-attack on those systems. These reviews can be used to shape and prioritize protection, detection, and response efforts. Dragos also offers compromise assessments to look for common indicators of an ongoing or prior network compromise, threat behaviors, and vulnerable assets and protocols, vulnerability assessments to identify vulnerabilities within network, hosts, field devices, and applications, and a suite of penetration testing services helps you evaluate the effectiveness of controls for networks, devices, and applications.
Cybersecurity Program Management (PROGRAM)	Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner that aligns cybersecurity objectives with both the organization's strategic objectives and the risk to critical infrastructure.	Dragos Professional Services provides expert ICS security practitioners and educators that can help organizations assess and mature their cybersecurity programs. The range of offerings include a review of program maturity and specific recommendations to advance that maturity. Additionally, the Dragos OT Cybersecurity Journey and Five Critical Controls can provide a simplified, high-level framework to guide build of effective OT security programs.

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.