SOLUTION BRIEF

DRAGOS
SAFEGUARDING CIVILIZATION

Cyber Assessment Framework, Version 3.1

How Dragos Can Help You Align to CAF Principles

It has been over five years since the UK's National Cyber Security Centre (NCSC) introduced the Cyber Assessment Framework (CAF) in response to the implementation of the Network and Information Systems (NIS) Regulations. Currently in its 4th iteration, version 3.1 includes several clarifications and updates. Originally designed for organisations responsible for Critical National Infrastructure designated Operators of Essential Services (OESs) as defined by the NIS Regulations, the CAF has been updated to have broader applicability and is now at the core of the government's cybersecurity strategy. It is being used by a wider range of public sector organisations.

The CAF collection consists of four high-level objectives that are further broken down into 14 cyber security and resilience principles. It also provides guidance on their application and includes 39 Indicators of Good Practice (IGP). Unlike many generic cybersecurity practices, the CAF collection is suitable for both Information Technology (IT) and Operational Technology (OT) environments, covering various organisations that operate OT systems, ranging from power generation to pharmaceutical production.

The primary focus of the CAF is on "Cyber Resilience," which refers to an organisation's ability to maintain the proper functioning of its essential operations even in the face of adverse cyber events. This emphasis on cyber resilience closely aligns with Dragos' approach to OT cybersecurity. It is the reason why Dragos offers a range of products and services in addition to the Dragos Platform.

Which industrial sectors are covered by Dragos technology and services?

- **Transport**
- **Manufacturing of Critical Products** (such as Pharmaceuticals, Medical Devices, Chemicals)
- **Digital Infrastructure, including Data Centers**
- **Space**
- **Food**
- **Public Administration**
- **Water Supply**
- **Wastewater and Waste Management**
- **Energy**
- **Digital Service Providers**

Cyber Assessment Framework (CAF) Principles and Guidance

Objectives in the Framework and How Dragos Can Help You Meet Them

Objective A: Managing security risk

Appropriate organisational structures, policies, and processes are in place to understand, assess and systematically manage security risks to the network and information systems supporting essential functions.

A1 Governance	Putting in place the policies and processes which govern your organisation's approach to the security of network and information systems.
A2 Risk management	Identification, assessment and understanding of security risks. And the establishment of an overall organisational approach to risk management.
A3 Asset management	Determining and understanding all systems and/or services required to maintain or support essential functions.
A4 Supply chain	Understanding and managing the security risks to networks and information systems which arise from dependencies on external suppliers.

How Dragos Can Help You Achieve Objective A: Managing Security Risk

OT Cybersecurity Assessment

The OT Cybersecurity Assessment is a comprehensive assessment of an ICS/OT cybersecurity program, examining cybersecurity policies and procedures, network topology, standards and regulations, and identifies those assets with most impactful risks – the "Crown Jewels". An OT Cybersecurity Assessment also assesses threat behaviours and groups of interest and includes recommendations for building a Collection Management Framework to support an ICS/OT incident response plan.

Dragos Platform: Asset Inventory Use Case

A comprehensive and real-time understanding of all assets in your environment is essential for network monitoring, threat correlation, and effective vulnerability management. Our customers use the Dragos Platform to identify crown jewel assets, create asset inventories, and identify unusual activity across thousands of devices. The Dragos Platform's asset inventory and visibility capabilities provide the industry's most comprehensive and in-depth understanding of OT environments, including:

- Comprehensive inventory of all assets, devices, and details
- Faster triage of incidents through timeline analysis
- Group assets by zone to identify unexpected traffic

Dragos Professional Services: Collection Management Frameworks

A Collection Management Framework (CMF) documents and institutionalises data sources that are available to defenders, including what information is available and how long that data is retained. CMFs allow defenders to understand the visibility and lack of visibility in their industrial environments, so they can more effectively prepare for and respond to cyber threats within their organisations. The Dragos Professional Services team can guide your organisation through this process.

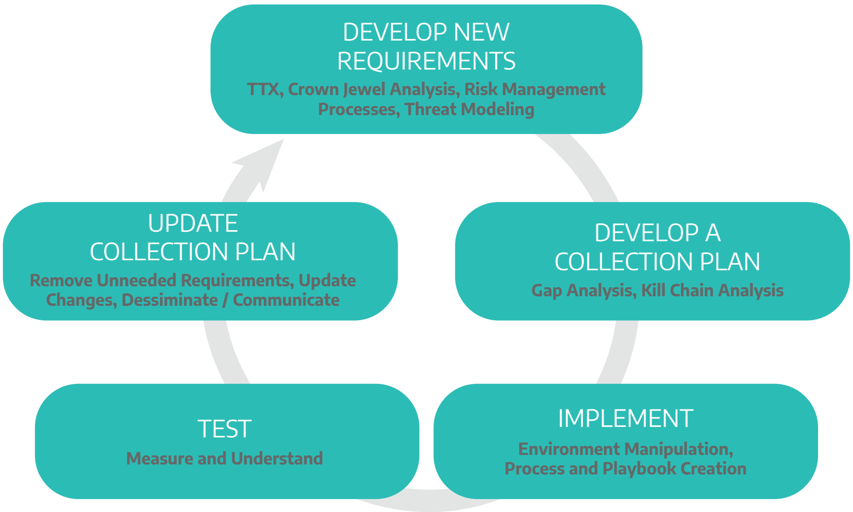
DEVELOP NEW REQUIREMENTS
TTX, Crown Jewel Analysis, Risk Management Processes, Threat Modeling
DEVELOP A COLLECTION PLAN
Gap Analysis, Kill Chain Analysis
IMPLEMENT
Environment Manipulation, Process and Playbook Creation
TEST
Measure and Understand
UPDATE COLLECTION PLAN
Remove Unneeded Requirements, Update Changes, Dessiminate / Communicate

Figure 1: CMF Development and Improvement Model

Dragos WorldView Threat Intelligence

Dragos WorldView, industrial threat intelligence, provides actionable information and recommendations on threats to OT environments. It provides security teams with in-depth visibility of the tactics, techniques, and procedures (TTPs) of sophisticated adversaries targeting industrial networks globally, so your organisation can better prepare for, detect, and respond to potential attacks.

Objective B: Protecting against cyber attack

Proportionate security measures are in place to protect the network and information systems supporting essential functions from cyber attack.

B1 Service protection policies and processes	Defining and communicating appropriate organisational policies and processes to secure systems and data that support the operation of essential functions.
B2 Identity and access control	Understanding, documenting and controlling access to networks and information systems supporting essential functions.
B3 Data security	Protecting stored or electronically transmitted data from actions that may cause an adverse impact on essential functions.
B4 System securit	Protecting critical network and information systems and technology from cyber attack.
B5 Resilient networks and systems	Building resilience against cyber attack.
B6 Staff awareness and training	Appropriately supporting staff to ensure they make a positive contribution to the cyber security of essential functions.

How Dragos Can Help You Achieve Objective B: Protecting Against Cyber Attack

OT Cybersecurity Assessment

The OT Cybersecurity Assessment includes a full program review, creation of a collection management framework, crown jewel analysis, topology review, standards and regulations review, indicators of compromise sweep, threat discovery, asset inventory, network vulnerability assessment, and asset vulnerability assessment.

OT Network Vulnerability Assessment

An OT Network Vulnerability Assessment helps your company close gaps in network defence by evaluating protection, detection, and response capabilities that currently exist in your environment. The assessment identifies exploitable vulnerabilities and provides action items to strengthen OT cybersecurity posture.

Dragos Platform: Vulnerability Management Use Case

OT cybersecurity teams are overwhelmed by hundreds of vulnerabilities that potentially need to be remediated. Dragos customers use the platform to simplify compliance and reporting, prioritise vulnerabilities that matter most, and maximise remediation resources.

Dragos ICS-OT Cybersecurity Training

Training builds a better shared understanding of the terminologies, purpose, security goals, and technologies deployed in OT environments and security programs. Training operations staff in cybersecurity fundamentals is an important part of business continuity – cybersecurity is everyone's job, and the operations team are the front lines for identifying and mitigating issues.

Dragos Neighborhood Keeper

Neighbourhood Keeper is a collective defence and community-wide visibility solution that provides a more effective industrial cyber defence by sharing aggregated and anonymised asset, threat, and vulnerability intelligence at machine-speed across industries and geographic regions. By participating, each organisation's defensive capability is made stronger than what they can achieve on their own.

OT Penetration Testing

OT Penetration Testing prevents severe breaches by leveraging real-world attacker tactics, techniques, and procedures (TTPs) gained from intelligence. Penetration testing identifies devices that could allow unauthorised access to critical OT assets and demonstrates how attackers can move through OT environments.

Objective C: Detecting cyber security events

Capabilities exist to ensure security defences remain effective and to detect cyber security events affecting, or with the potential to affect, essential functions.

C1 Security monitoring	Monitoring to detect potential security problems and track the effectiveness of existing security measures.
C2 Proactive security event discovery	Detecting anomalous events in relevant network and information systems.

How Dragos Can Help You Achieve Objective C: Detecting Cyber Security Events

OT Watch

With Dragos OT Watch, our OT cybersecurity experts become part of your team, performing high severity notification triage and proactive threat hunting with the Dragos Platform to ensure threats don't get overlooked. Our elite team of analysts proactively hunt for and report on threat activity in your OT environment using the latest threat intelligence exclusive to Dragos customers. We work alongside your team to triage and investigate high severity notifications to reduce the burden on internal resources.

Dragos Platform: Detection Use Case

Adversaries evolve their tactics, techniques, and procedures with subtle behaviours that are easily lost in the noise of your environment. Our platform customers immediately see any unauthorised IT-OT traffic across complex networks, analyse file downloads quickly and easily, and detect potential adversaries in the environment in real-time.

Objective D: Minimising the impact of cyber security incidents

Capabilities exist to minimise the adverse impact of a cyber security incident on the operation of essential functions, including the restoration of those functions where necessary.

D1 Response and recovery planning	Putting suitable incident management and mitigation processes in place.
D2 Lessons learned	Learning from incidents and implementing these lessons to improve the resilience of essential functions.

How Dragos Can Help You Achieve Objective D: Minimising the Impact of Cyber Security Incidents

Rapid Response Retainer

An OT-specific Rapid Response Retainer is essential for any industrial environment. Since the potential impact of a cyber attack can vary based on visibility, the ability to respond, and your organisational security posture, a dedicated OT incident response plan accounting for your needs is crucial to quickly scope, investigate, and respond to incidents. As the cornerstone of your OT cyber program, an OT-specific incident response retainer ensures you can respond quickly and recover confidently.

Tabletop Exercises

The Dragos Tabletop Exercise (TTX) Service is a step-by-step method that demonstrates how a realistic attack may occur within your unique OT environment based on your organisation's most concerning risks. Dragos TTXs include collaboration between all stakeholders, including IT and OT security teams, to strengthen internal communication strategies and develop relationships.

Dragos Platform: Incident Investigation Use Case
Dragos Platform users can analyse changes and forensic records, efficiently manage response and recovery, and leverage prescriptive playbooks with proven, tested response protocols.

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**.