SOLUTION BRIEF

DRAGOS

Cyber Assessment Framework, Version 4.0

How Dragos Can Help You Align to CAF Principles

CAF v4.0 sets the UK's latest expectations for resilience across four objectives: managing risk, protecting against attack, detecting events, and minimizing impact. At Dragos, our mission to safeguard civilization directly supports these goals with OT-native technology, intelligence, and services recognized as a Leader in the 2025 Gartner® Magic Quadrant™ for Cyber-Physical Systems (CPS) Protection Platforms. Here's how Dragos maps to CAF v4.0:

- **Objective A - Managing Security Risk:** Real-time asset visibility, risk-based vulnerability management, OT cyber threat intelligence, and expert-led cybersecurity assessments help organizations identify crown-jewel assets and anticipate adversary behaviors.
- **Objective B – Protecting Against Cyber Attack:** Platform-based vulnerability management, collective defense, penetration testing, and ongoing platform tuning and enrichment ensure defenses remain aligned with CAF expectations.
- **Objective C – Detecting Cyber Security Events:** Intelligence-driven detections that combine behavior analysis mapped to MITRE ATT&CK for ICS, anomaly monitoring, and threat hunting to surface adversary activity before essential functions are disrupted.
- **Objective D – Minimizing Impact:** Frontline incident response retainers, prescriptive playbooks, and intelligence-driven tabletop exercises help organizations recover quickly, apply lessons learned, and strengthen resilience.

CAF v4.0 demands proactive, intelligence-driven resilience. Dragos uniquely provides the OT-native cybersecurity platform, services, and intelligence to help organisations not only comply, but build operational resilience against capable and opportunistic adversaries.

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	Policies and processes governing the security of network and information systems.
A2 Risk management	Identification, assessment, and understanding of security risks. **NEW** A2.b Threat Understanding – Maintain current knowledge of adversary methods and risks.
A3 Asset management	Determine and document systems/services essential to operations.
A4 Supply chain	Manage security risks from external suppliers. **NEW** A4.b Secure Development – Ensure software and systems are developed and maintained securely throughout their lifecycle.

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

Dragos Platform Asset Visibility & Inventory

Provides passive OT-native discovery across OT/IT/IoT assets, complemented by an active collection agent for deeper validation. It delivers real-time visibility, automated asset inventory, and deep packet inspection. Customers gain:

- A unified, continuously updated inventory across all industrial assets
- Identification of crown-jewel systems and visibility into their communication pathways
- Rapid anomaly detection through traffic analysis and asset grouping by zones
- Actionable context for remediation and improved response readiness

WorldView Threat Intelligence

Technical and strategic research covering OT-specific adversary TTPs, malware analysis, vulnerability insights, and risk context.

Neighborhood Keeper

Community defense program for Dragos Platform customers that shares anonymized, real-time threat and vulnerability intelligence across industries.

NP-View

Map and validate network configurations to identify segmentation gaps, verify firewall rules, and provide assurance around asset inventories and supply chain dependencies.

OT Cybersecurity Assessment

Guide policies, risk management, and crown jewels, with threat modeling aligned to adversary behaviors.

Professional Services

Development of Collection Management Frameworks and secure-by-design practices for industrial environments.

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	Define and communicate organizational policies for securing systems and data.
B2 Identity and access control	Document and control access to critical networks and information systems.

B3 Data security	Protect stored and transmitted data from unauthorized access or damage.
B4 System securit	Protect critical technology and networks against attacks.
B5 Resilient networks and systems	Build resilience into systems to withstand cyber threats.
B6 Staff awareness and training	Ensure staff are trained to make positive contributions to cybersecurity.

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

Dragos Platform Vulnerability Management

Simplifies compliance and remediation by applying OT context to vulnerability assessments and prioritization. Customers benefit from:

- Automated correlation of vulnerabilities to asset inventories
- Recalculated risk scoring factors in exploitability, active exploitation, and criticality
- "Now, Next, Never" guidance for prioritization and resource allocation
- Integrated workflows to streamline patching, mitigation, and reporting

OT Watch Complete

Provides continuous support in tuning zones, enriching asset inventories, and configuring detections to ensure the best security outcomes from the Dragos Platform.

Network Vulnerability Assessment

Identifies exploitable security weaknesses through systematic information gathering and configuration review.

Network Penetration Testing

Demonstrates adversary pathways with intelligence-driven scenarios to improve defenses.

OT/ICS Cybersecurity Training

Builds staff awareness, improving resilience across IT and OT teams.

Objective C: Detecting cyber security events

Capabilities exist to ensure defenses remain effective and to detect events that could affect essential functions.

C1 Security monitoring	Monitor networks and systems to detect potential security problems and measure the effectiveness of defenses. **NEW** C1.f User and system monitoring & threat intelligence – Monitor patterns of activity to establish behavioral baselines, implement anomaly detection, and integrate threat intelligence to understand behavior context.
C2 Proactive security event discovery	**NEW** Replaces "Proactive attack discovery" - Structured, intelligence-driven threat hunting to actively search for adversary presence, detecting hidden or stealthy threats.

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

Dragos Platform Threat Detection

Provides OT-native detections mapped to MITRE ATT&CK for ICS, delivering precise alerts without noise. Built on frontline OT incident response and adversary research, the platform enables:

- Immediate visibility into unauthorized IT-OT crossover, malicious file transfers, anomalous traffic patterns and communication
- Continuous Knowledge Pack updates from Dragos threat intelligence, ensuring detection logic evolves with adversary tradecraft
- Integrated playbooks and case workflows that help teams move from alert to action with confidence
- Flexible deployment with passive monitoring at scale, complemented by active collection for targeted checks

OT Watch

Dragos experts triage high-severity alerts and perform proactive threat hunts to detect the presence of hidden or stealthy threats.

OT Watch Complete

Extends the OT Watch service with 24/7 security monitoring, triage, and investigations fully managed by Dragos analysts, threat hunters, and incident responders.

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	Put suitable incident management and mitigation processes in place.
D2 Lessons learned	Learn from incidents and apply improvements to strengthen resilience.

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

Dragos Platform Incident Investigation

Empowers defenders to detect, investigate, and respond to incidents using OT-native workflows. The platform provides:

- Forensic timelines built from both passive and active data sources
- Prescriptive, expert-authored playbooks tested in real-world incident response
- Investigations explicitly designed for OT environments, not retrofitted from IT
- Integration with Dragos services to accelerate coordinated response and recovery

Rapid Response Retainer

OT-specific expertise for scoping, containment, and recovery, ensuring quick return to operations.

Tabletop Exercises (TTXs)

Realistic attack simulations to test plans, improve coordination, and apply lessons learned from incident response.

In Summary

CAF v4.0 raises expectations for resilience, moving beyond compliance to anticipate, detect, and recover from threats. Backed by recognition as a Leader in Gartner's 2025 CPS Protection Platforms Magic Quadrant, Dragos delivers OT-native monitoring, intelligence, and expert services so you can meet these standards with confidence and strengthen defenses against adversary threats.

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. Learn more about our technology, services, and threat intelligence offerings: **request a demo** or **contact us**.