# MOSAICS-Compatible Solution to Real-Time Operational Technology (OT) Monitoring and Mitigation

## Critical infrastructure is at risk

Adversaries have demonstrated non-kinetic means to disrupt critical warfighting infrastructure, denying the United States and its Allies the ability to project force.

This threat was recently highlighted in a DHS technical alert detailing an ongoing Russian government cyber intrusion campaign targeting U.S. government and commercial critical infrastructure. **DoD currently lacks adequate cyber situational awareness and response capabilities to address this challenge.**

## Dragos / Sentar / Siemens solution

In 2021, the successful Joint Capability Technology Demonstration (JCTD) of MOSAICS created a call to industry to develop a commercially-viable solution with MOSAICS ("technologies associated" in the NDAA).

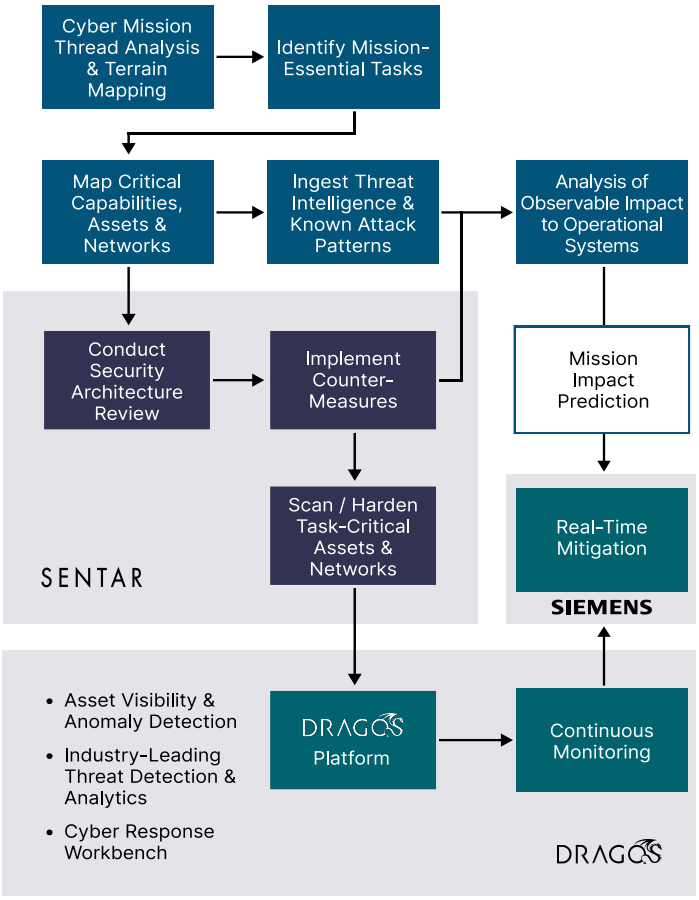
The Dragos / Sentar / Siemens solution for Defense Critical OT Networks and Assets is compatible with MOSAICS and includes key extensions to meet the requirements of the 2022 NDAA while also providing real-time mitigation in a contested operating environment.

This solution also addresses the NDAA's call for the complete mapping of mission-relevant terrain in cyberspace for Defense Critical Assets and Task Critical Assets at sufficient granularity to enable mission thread analysis and situational awareness.

## Congress and Pentagon take action

The 2022 National Defense Authorization Act (NDAA) prioritizes the need to mitigate such threats. The NDAA directs military departments to invest in the cyber-defense of operational technology (OT).

More recently (April 2022), the DoD CIO released an addendum to DoD's Cyber Defense Reference Architecture to include components of **More Situational Awareness for Industrial Control Systems (MOSAICS)** reference architecture.




01 **INL & MDA-Inspired Mission Thread Analysis**

02 **Hardened & Secured Control Systems**

03 **MOSAICS-Based Continuous Monitoring**

04 **Real-Time CS Detections & Mitigations**

# MOSAICS-Compatible Solution to Real-Time Operational Technology (OT) Monitoring and Mitigation (Continued)

01

## INL & MDA-Inspired Mission Thread Analysis

The first layer in the solution leverages the industry-leading Consequence-Driven, Cyber-Enabled Engineering (CCE) methodology pioneered by Idaho National Labs (INL) to provide the foundation for Cyber Mission Thread Analysis and Relevant Terrain Mapping and Identification. The INL CCE process identifies Mission-Essential Tasks and maps critical OT capabilities, assets, and networks. The INL process also serves as a front-end for Mission Valor, the Missile Defense Agency Small Business Innovation Research (SBIR) investment which ingests threat intelligence and known attack patterns for operational networks and assets. Mission Valor integrates with Digital Twins and Model-Based Systems Engineering principles and performs an analysis of observable impacts to OT networks and assets to predict mission impact. **Mission Valor Phase 3 extensions automatically qualify for sole source justification and small business credit.**

02

## Hardened & Secured Control Systems

The Defense of Critical Assets relies upon hardened, secured, and rigorously monitored operational technology. Sentar implements these best practices at critical National Security sites including those associated with the Missile Defense Agency and serves in this role within our integrated solution. **The Dragos / Sentar / Siemens solution goes beyond NIST's Risk Management Framework and is strengthened by a robust security architecture review, the implementation of countermeasures, and a continuous ATO enabled by regular security, vulnerability, and configuration scans.** We also provide detailed system security planning and a mature program complete with a plan of action and a milestones-based remediation program.

03

## MOSAICS-Based Continuous Monitoring

The foundational element of MOSAICS is its ability to provide continuous monitoring for Defense-Critical OT Networks and Assets. The Dragos Platform performs this function in our solution architecture and is the commercial industry-leading OT Threat Monitoring Platform. **The Dragos Platform is developed entirely in the United States — by U.S. entities and experts trusted by some of the largest asset owners in the world to investigate and respond to the most significant ICS cyberattacks in history.** The Dragos OT Platform aligns with the MOSAICS architecture and provides asset visibility and anomaly detection, industry-leading threat detection and analytics, and a cyber response workbench to accelerate incident response.

04

## Real-Time CS Detections & Mitigation

The real-time mitigations layer is provided by Siemens SIBERprotect. This capability within our solution goes beyond the envisioned operational and functional requirements of MOSAICS by providing a secure enclave and out-of-band communications and digital signaling capabilities during the most critical operations of Defense-Critical OT Networks and Assets. **Siemens SIBERprotect can accommodate any OT security architecture and is tailored to a client's unique operating environment.** SIBERprotect operates at the control systems level within OT networks (typically Purdue Level 1-3) and serves as a technology-independent solution that integrates and protects any commercially available control system to provide real-time mitigation at the speed of the adversary.