SOLUTION BRIEF

# Dragos OT Security Solutions to Align with NIST SP 800-82r3 Guidelines

## How to Secure Operational Technology to Meet NIST Standards for Industrial Control Systems

NIST Special Publication 800-82 Revision 3 (NIST SP 800-82r3) sets the gold standard for operational technology (OT) security, providing crucial guidance for protecting industrial control systems across various sectors.

Dragos, a leader in industrial cybersecurity, offers a suite of solutions designed to help organizations meet and exceed these stringent requirements. The Dragos Platform, coupled with Dragos Services, Intelligence, Academy, and Neighborhood Keeper, provides a holistic approach to OT security. From asset discovery and threat detection to incident response and training, Dragos equips organizations with the tools and expertise needed to safeguard their critical infrastructure in alignment with NIST SP 800-82r3 guidelines.

This solution brief outlines how Dragos offerings map to the key control families of NIST SP 800-82r3, enabling organizations to enhance their OT security posture effectively and efficiently.

# The Relationship Between NIST SP 800-82r3 and NIST SP 800-53r5 (Risk Management Framework - RMF)

NIST SP 800-82r3 provides an OT overlay for NIST SP 800-53 Rev. 5, which provides tailored security control baselines for low-, moderate-, and high-impact OT systems. This overlay adapts the general security controls from SP 800-53 to address the unique performance, reliability, and safety requirements of OT environments. By incorporating this tailored approach, SP 800-82r3 ensures that organizations can apply appropriate security measures to their OT systems while maintaining alignment with the broader information security framework established in SP 800-53. This integration allows for a more cohesive and comprehensive approach to securing both IT and OT systems within an organization's overall cybersecurity strategy.

## Dragos Capabilities Mapped to NIST SP 800-82r3 Guidelines

### 1 ACCESS CONTROL (AC)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| The Access Control family contains controls that cover access to systems, networks, and devices. It provides guidance on implementing access policies, account management, and user privileges to lower the risk of unauthorized access. | In OT environments, proper access control is crucial to prevent unauthorized individuals from interfering with critical industrial processes or accessing sensitive operational data. | • **Dragos Platform:** Provides passive monitoring of OT networks, helping identify unauthorized access attempts.<br>• **NP-View:** Validates remote access through path analysis and segmentation policy. |

### 2 AWARENESS AND TRAINING (AT)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family focuses on ensuring that system users are aware of security risks and have received appropriate training to carry out their duties securely. | OT environments often require specialized knowledge. Proper training ensures that personnel can operate and maintain systems securely, reducing the risk of accidental incidents. | • **Dragos Academy:** Offers comprehensive training programs on OT security, including courses on the Dragos Platform and general ICS security practices.<br>• **Dragos Threat Intelligence:** Provides real-world threat intelligence on OT attacks.<br>• **Dragos Services:** Provides tabletop exercises and program reviews to enhance organizational awareness and preparedness. |

## 3 AUDIT AND ACCOUNTABILITY (AU)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family deals with the creation, protection, and retention of system audit records and the tools to analyze them. | Auditing is crucial in OT environments to track system changes, detect anomalies, and investigate incidents while maintaining operational integrity. | • **Dragos Platform:** Offers extensive logging and auditing capabilities for OT networks, including asset inventory changes and real-time threat detections.<br>• **NP-View:** Provides evidence for network configuration changes and potentially overly permissive access. |

## 4 ASSESSMENT, AUTHORIZATION, AND MONITORING (CA)Z

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family focuses on assessing the security controls in organizational systems, authorizing system operation, and ongoing system monitoring. | Regular assessment and monitoring are essential in OT environments to ensure that security controls remain effective as systems and threats evolve. | • **Dragos Platform:** Offers continuous monitoring of OT networks, providing real-time visibility into system status and potential security issues.<br>• **Dragos Services:** Provides assessment services to evaluate the security posture of OT environments and test security controls.<br>• **NP-View:** Enables ongoing monitoring of network segmentation and access policies. |

## 5 CONFIGURATION MANAGEMENT (CM)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family addresses the establishment and maintenance of the integrity of organizational systems throughout their life cycles. | Proper configuration management in OT environments ensures that systems remain secure and operational, minimizing vulnerabilities and unplanned downtime. | • **Dragos Platform:** Provides visibility into asset configurations and can detect unauthorized changes.<br>• **NP-View:** Offers configuration analysis for network devices through system level segmentation analysis and device level segmentation analysis. |

## 6 CONTINGENCY PLANNING (CP)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family focuses on the preparation, testing, and maintenance of plans for emergency response, backup operations, and post-disaster recovery. | In OT environments, contingency planning is crucial to ensure continuity of critical operations in the face of disruptions or cyber incidents. | • **Dragos Services:** Offers incident response planning and tabletop exercises to enhance organizational preparedness. |

## 7 IDENTIFICATION AND AUTHENTICATION (IA)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family addresses the verification of users, processes, or devices as a prerequisite to allowing access to organizational systems. | Proper identification and authentication in OT environments prevent unauthorized access to critical systems and help maintain the integrity of industrial processes. | • **Dragos Platform:** While primarily passive, it can detect anomalies in authentication patterns and cleartext authentications. |

## 8 INCIDENT RESPONSE (IR)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family focuses on the development and maintenance of an organizational incident handling capability. | Effective incident response in OT environments is crucial to minimize the impact of security incidents on critical infrastructure and industrial processes. | • **Dragos Platform:** Provides threat detection, necessary network forensic evidence, and investigation capabilities to support incident response.<br>• **Dragos Services:** Offers incident response support and planning services.<br>• **NP-View:** Enables comparison of last known good configuration to current configuration as part of validation in IR and provides network context to the host being investigated.<br>• **Neighborhood Keeper:** Enables anonymous threat information sharing to improve collective defense. |

## 9 MAINTENANCE (MA)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family addresses the maintenance of organizational systems, and the tools used to maintain them. | Proper maintenance of OT systems is crucial to ensure their continued secure operation and to prevent vulnerabilities introduced through maintenance activities. | • **Dragos Platform:** Provides visibility into system changes that may occur during maintenance activities.<br>• **NP-View:** Enables comparison of last known configuration to current configuration as part of maintenance validation. |

## 10 MEDIA PROTECTION (MP)

| Description | Relevance to OT Security |
|---|---|
| This family focuses on the protection of system media, both digital and non-digital. | In OT environments, media protection is important to prevent unauthorized disclosure of sensitive operational data or introduction of malware through removable media. Dragos encourages strong policies against using removable media. |

## 11 PHYSICAL AND ENVIRONMENTAL PROTECTION (PE)

| Description | Relevance to OT Security |
|---|---|
| This family addresses the physical and environmental protection of systems, equipment, and supporting infrastructure. | Physical security is crucial in OT environments to prevent unauthorized physical access to critical systems and to protect against environmental threats. Dragos focuses on cybersecurity, not physical security, but encourages a robust physical security program. |

## 12 PLANNING (PL)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family focuses on the development, documentation, and updating of security and privacy plans. | Comprehensive planning is essential in OT environments to ensure that security measures are aligned with operational requirements and regulatory obligations. | • **Dragos Intelligence:** Provides threat intelligence to inform security planning. |

## 13 PROGRAM MANAGEMENT (PM)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family provides controls for information security program management at the organizational level. | Effective program management ensures that OT security efforts are coordinated, resourced, and aligned with organizational objectives. | • **Dragos Platform and NP-View**: Offer tools and insights that support informed program management decisions.<br>• **Dragos Intelligence:** Dragos Intelligence provides in-depth visibility of threats targeting industrial environments globally and offers defensive recommendations to combat them.<br>• **Dragos Services:** Can provide strategic guidance on OT security program management. |

## 14 PERSONNEL SECURITY (PS)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family addresses the controls for personnel screening, termination, and transfer. | Personnel security is crucial in OT environments to ensure that individuals with access to critical systems are trustworthy and properly vetted. | • **Dragos Platform:** Dragos Platform can monitor remote access into the OT network and provide validation that provider access and change management follows the organizational requirements. |

## 15 RISK ASSESSMENT (RA)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family focuses on the assessment of risk to organizational operations, assets, and individuals. | Regular risk assessment in OT environments is crucial to identify and prioritize security risks to critical infrastructure and industrial processes. | • **Dragos Platform:** Provides asset visibility, vulnerability management, and threat detection capabilities that inform risk assessments.<br>• **NP-View:** Supports network risk assessment through its policy analysis capabilities to identify configuration vulnerabilities.<br>• **Dragos Services:** Conducts Crown Jewel Analysis to identify critical systems and components as part of an OT Cybersecurity Assessment. |

## 16 SYSTEM AND SERVICES ACQUISITION (SA)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family addresses the allocation of resources for information system security and the integration of security into system development life cycles. | Proper acquisition practices ensure that security is built into OT systems from the start, reducing vulnerabilities and lifecycle costs. | • **Dragos Platform**: Helps identify and manage risks associated with acquired systems once deployed.<br>• **NP-View:** Helps identify and manage configuration and segmentation risks. |

## 17 SYSTEM AND COMMUNICATIONS PROTECTION (SC)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family focuses on the protection of system communications and architectures. | Protecting communications in OT environments is crucial to maintain the integrity and confidentiality of control data and prevent unauthorized system manipulation. | • **Dragos Platform:** Provides baselining, threat detection, deep packet inspection, and protocol analysis for OT networks.<br>• **NP-View:** Offers network segmentation and policy analysis to ensure proper communication protections are in place for (as an example) interactive remote access. |

## 18 SYSTEM AND INFORMATION INTEGRITY (SI)

| Description | Relevance to OT Security | Dragos Capabilities |
|---|---|---|
| This family addresses the identification, reporting, and correction of system flaws, protection from malicious code, and monitoring of system security alerts and advisories. | Maintaining system and information integrity is critical in OT environments to ensure the reliability and safety of industrial processes. | • **Dragos Platform:** Offers continuous monitoring, threat detection, and vulnerability management for OT systems.<br>• **Dragos Intelligence:** Provides timely information on new vulnerabilities and threats.<br>• **Neighborhood Keeper:** Enables anonymous sharing of threat information to enhance collective defense. |

## 19 SUPPLY CHAIN RISK MANAGEMENT (SR)

| Description | Relevance to OT Security |
|---|---|
| This family focuses on the management of risks associated with the global supply chain. | Supply chain risks in OT environments can introduce vulnerabilities through hardware, software, or services, potentially compromising critical infrastructure. |

**This mapping demonstrates how the Dragos suite of offerings and NP-View software provide comprehensive coverage across the NIST SP 800-82r3 control families, offering robust support for OT security requirements.**

### 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    Contact Us