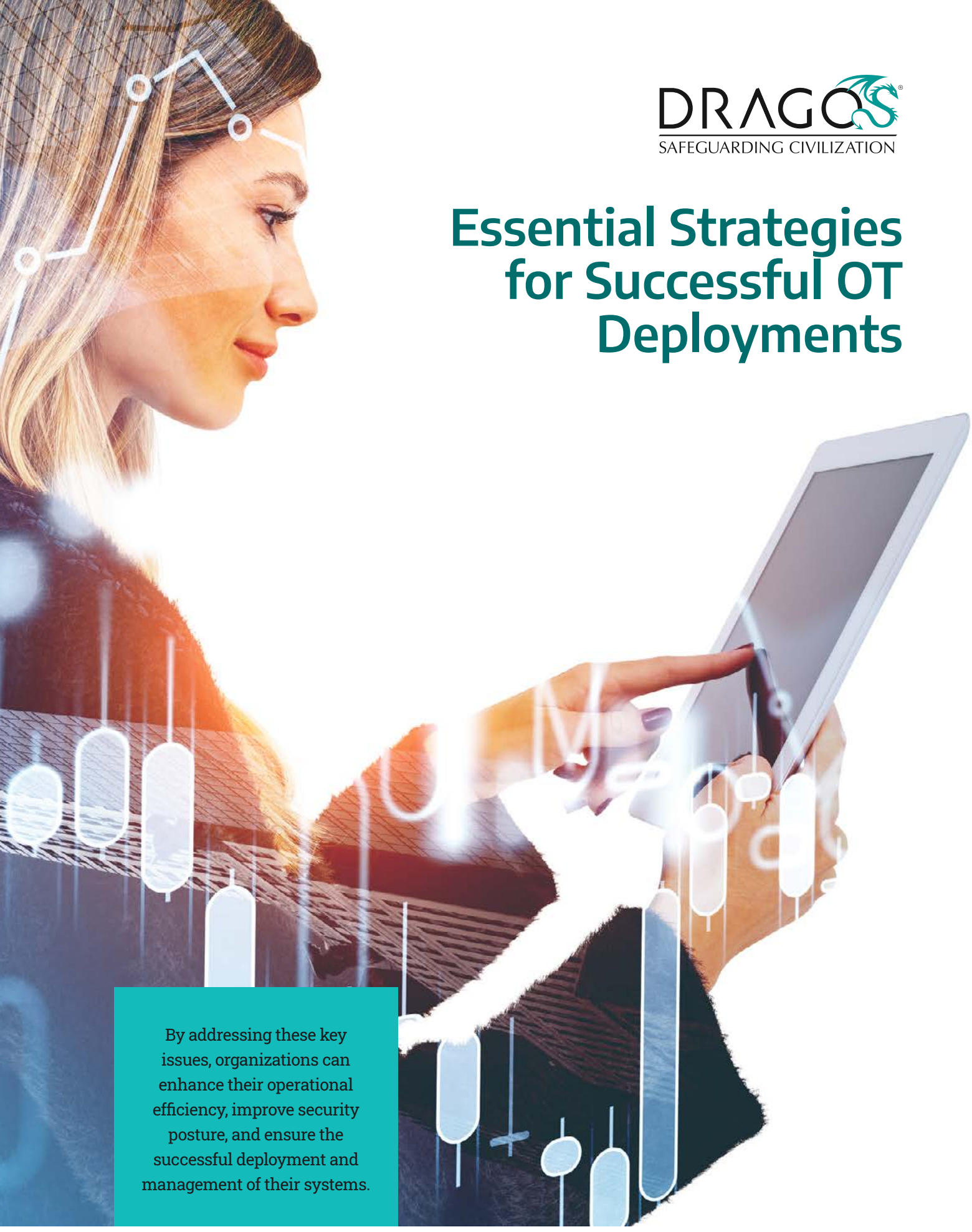
DRAGOS
SAFEGUARDING CIVILIZATION

# Essential Strategies for Successful OT Deployments



By addressing these key issues, organizations can enhance their operational efficiency, improve security posture, and ensure the successful deployment and management of their systems.

# Essential Strategies for Successful OT Deployments

## COMMUNICATION WITH KEY STAKEHOLDERS & GROUPS

**Effective communication is vital for the successful deployment and operation of any system. To manage this issue:**

- ☐ Make sure the right stakeholders are included from the start: You'll need IT security teams, network administrators responsible for OT switching fabric, OT security teams, plant operations and management, corporate leadership, and procurement. Identify a single point of contact as a project manager.
- ☐ Establish clear communication channels: Ensure there are well-defined channels for regular updates and feedback between stakeholders. Consider a quarterly business review, ensuring executive visibility to challenges and progress.
- ☐ Document and share information: Keep detailed records to ensure transparency and accountability.

## EARLY & FREQUENT COLLABORATION WITH OT TO AVOID DEPLOYMENT DELAYS

**Operational Technology (OT) teams play a crucial role in deployments. To avoid delays:**

- ☐ Engage OT early: Involve OT teams from the planning phase to ensure their requirements and constraints are considered.
- ☐ Maintain continuous dialogue: Regularly update OT teams on progress and seek their input to preempt potential issues.
- ☐ Collaborate on timelines: Work together to account for OT constraints and availability.

## IMPROVE NOTIFICATION TUNING BASED ON KNOWLEDGE OF ASSETS/IMPACT

**Effective notification systems are essential for prompt response and mitigation. To enhance notification tuning:**

- ☐ Understand asset criticality: Identify and prioritize notifications based on the criticality and impact of different assets.
- ☐ Regularly review and adjust: Continuously assess the effectiveness of notifications and adjust as needed.
- ☐ Leverage historical data: Use past incident data to refine notification settings and improve accuracy.

## IDENTIFY AND UNDERSTAND YOUR CROWN JEWEL ASSETS (CJAs)

**Knowing your most critical assets is essential for effective risk management. To address this:**

- ☐ Conduct a thorough assessment: Identify and document all assets, focusing on those critical to operations.
- ☐ Engage stakeholders: Collaborate with key stakeholders to validate and refine the list of crown jewel assets.
- ☐ Regular updates: Periodically review and update the list to reflect changes in the operational environment.

## Our Team's Expertise Improves Your Deployment Experience

"Dragos, Inc. has been absolutely fantastic to work with through every step of this journey and continues to surpass my expectations on all fronts."
**— OT Cybersecurity & Automation Specialist, Oil and Gas Operator**

"The Dragos team has been very helpful managing our deployment in our compliance-related environments. The team has been great to work with and I know if we have any challenges, you're just a phone call away. Thank you for everything!"
**– Electric Utility Customer**

## RISK-BASED MITIGATION AGAINST OPERATIONAL IMPACT (SAFETY, QUALITY, PRODUCTIVITY)

**Identifying crown jewel assets (CJAs) is the first step towards targeted risk mitigation. To manage this:**

- ☐ Develop risk-based strategies: Create mitigation plans that prioritize CJAs based on their potential impact on safety, quality, and productivity.
- ☐ Implement monitoring systems: Set up systems to continuously monitor the health and security of CJAs.
- ☐ Regular training: Provide ongoing training to staff on the importance of CJAs and how to protect them.

## INCORPORATE OT EXPERTISE IN YOUR SOC

**A lack of OT expertise in the Security Operations Center (SOC) can hinder effective incident response. To mitigate this issue:**

- ☐ Hire or train OT specialists: Include OT experts in your SOC. If skill gaps or staff shortages are a problem, consider leveraging proactive threat hunting, resident engineers, concierge analysts, etc.
- ☐ Foster cross-functional collaboration: Encourage collaboration between IT and OT teams. Cross-training can enhance the SOC's capability to handle OT-related incidents.

## IDENTIFY SITE/FACILITY LEVEL CONTACTS TO CONSULT ON DETECTIONS ANALYSIS

**Local expertise is invaluable for accurate detection analysis. To leverage this:**

- ☐ Identify key contacts: Determine who at each site or facility can provide insights into detections.
- ☐ Establish communication protocols: Set up clear protocols for when and how to contact these individuals.
- ☐ Incorporate local feedback: Use the insights from site-level contacts to refine detection and analysis processes.

# The Dragos Platform Pre-Deployment Task List

## Streamlining Installation of Dragos Platform Sensors for OT Visibility

The Dragos Platform provides visibility and monitoring of OT networks. It provides asset discovery and inventory, vulnerability management, and cyber threat detection, as well as forensic data capture to aid in investigations. Dragos provides the most effective cyber threat protection for OT, which is typically a shared responsibility between IT Security and the Operations organizations that run industrial systems. We provide added value to aid operational efficiency and resilience as well.

### Building Resilience and Improving Efficiency for Operations

The rise of cyber threats poses significant risks to industrial operations, including ransomware, malware, and targeted attacks. Disruption to OT environments from cyber events can result in impacts to safety, environment, and lead to interruption of production processes.

And there are other issues that disrupt operations – networking issues, system misconfiguration, faults or errors.

Dragos detailed logging and analysis across OT systems fills a key gap in many OT environments. The forensic data is used to identify misconfigurations and find root cause to operational problems. Our ability to monitor networks without disruption, to mitigate vulnerabilities without system shutdown, and to understand the complexities of the environment earns the respect of Operations.

### Elements of Sensor Operation

Dragos Platform Sensors operate as passive devices deployed in key aggregation points of the OT network, using network spans, port mirroring, or traffic aggregators to direct copies of network traffic to the sensors. This passive approach is to avoid any issues with active scans and tools, though you can use Dragos Extended Visibility tool to augment device inventories and profiles.

As the sensor sees traffic, it builds asset inventories, logs key activities, analyzes the data. This results in threat detections dashboard, vulnerability dashboard, asset inventory and communications visualization, along with a number of other views on the OT system and network activity.

Sensors connect to SiteStores which aggregate information across all connected sensors. SiteStore operates either on-premises or in the cloud. Both sensors and SiteStores can be deployed virtually, on your approved hardware models vis ESXi or HyperV; they are also delivered on Dragos hardware platforms, with multiple options to meet capacity, form factor, and environmental needs.

## Before You Begin

Look to the following key information for planning your deployment:

- Follow the Quick Start guides to deploy sensors (available via the Dragos Customer Portal at: portal.dragos.com)
- Engage with your identified Dragos Field Operations Engineer for any deployment guidance or questions
- Are there specialized environmental standards needed to be met (e.g. electrical immunity standards, ruggedization requirements, mounting requirements such as DIN rails)?
- Is equipment compatibility and validation testing required? With what vendors?

## Step 1: Prepare Key Change Control Processes

- ☐ Identify key parties involved. Send a message that outlines the project including key reasons and benefits to the organization
- ☐ Review Quick Start Guide(s) applicable to your deployment
- ☐ Initiate change management procedures to allow for the deployment of Dragos Sensors
- ☐ Document key parties required for change management – site personnel, IT personnel, third party management & operations (e.g. equipment OEM, external management company or contractor)
- ☐ Evaluate any dependencies on OEM equipment vendors
- ☐ Create necessary tickets to initiate change management process
- ☐ Ensure an outage or maintenance window has been identified where required
- ☐ Prepare and submit firewall modifications. Note the timelines required for completion of tickets. See Dragos Platform Rules Guide for specific requirements available via the Dragos Customer Portal at: portal.dragos.com
- ☐ Evaluate resources with required skills, competencies, and access to perform installation
- ☐ Prepare sites for rack and stack procedures and instruct teams on how sensors will be delivered, if applicable
- ☐ Make updates to compliance policies, procedures, evidence, and evaluations

## Step 2: Evaluate & Document Site Specific Network Environment - Operations Site(s)

- ☐ Identify network aggregation points where Sensors are to be placed
- ☐ Evaluate the capability of the aggregation point/switches for a) SPAN (RSPAN, Remote SPAN, Local SPAN) and b) VLANs
- ☐ Identify interfaces / available ports
- ☐ Validate dataflows, network architecture, sensor placementand connection to OT Watch / Neighborhood Keeper for optimal functionality
- ☐ Ensure power, space, cooling, and connectivity exists for all hardware, including Out-of-Band management
- ☐ Ensure virtual resources available in full to allocate to Dragos Virtual machines according to the Dragos Virtual System Requirements
- ☐ Identify interfaces / available ports
- ☐ Configure managed switches for both management and monitor traffic, and identify interfaces
- ☐ Ensure cabling is pre-routed between switches and sensors
- ☐ Identify and document static IP addresses for sensor management, NTP server address(es), DNS address(es), etc.
- ☐ Identify rack space, mounting (e.g. standard or DIN rails), and power requirements
- ☐ Verify network backhaul capacity
- ☐ Update network diagrams in anticipation of the modifications
- ☐ Attend the Dragos Pre-Deployment Kickoff meeting (if appropriate)

## Step 3: Review and complete the steps in the Dragos Technical Guide: OT Network Traffic Validation Steps.

Click here to download



### 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