



RISK-BASED VULNERABILITY MANAGEMENT FOR **OPERATIONAL TECHNOLOGY**

**A FRAMEWORK FOR
PRIORITIZING RISKS
TO INDUSTRIAL
CONTROL SYSTEMS**

DRAGO
SAFEGUARDING CIVILIZATION



Introduction

Operational technology (OT) environments are critical to industrial operations but face unique cybersecurity challenges. From insecure-by-design devices to interconnected OT, IT, and IoT systems, these environments require a tailored approach to vulnerability management. Unlike IT networks, OT systems demand solutions prioritizing operational continuity, safety, and uptime while minimizing risks.

This guide offers a comprehensive framework for managing vulnerabilities across the OT environment. It outlines the foundational steps—asset inventory and network mapping to centralized tracking, prioritization, and risk-based mitigation—all driven by threat intelligence. The Dragos Platform ties these components together, providing a robust system that empowers organizations to proactively protect critical systems, mitigate risks, and maintain operational resilience without disruptions.

Asset Inventory and Network Mapping: The Foundation of OT Cybersecurity

Effective vulnerability management starts with knowing what devices are in your environment and how they communicate. An **asset inventory** provides visibility into every device, from PLCs and SCADA systems to IoT sensors and engineering workstations. It captures the data needed to identify specific CVEs (Common Vulnerabilities and Exposures) that apply to them. **Network mapping** adds context by visualizing communication paths and data flows, revealing where vulnerabilities may expose critical systems to attack paths. An asset inventory and network mapping create the foundation for efficiently tracking, prioritizing, and mitigating vulnerabilities.

Key Challenges in OT Environments

- **Legacy Systems and Insecure by Design:** Many OT systems were built before cybersecurity became a priority. These legacy devices often lack essential protections like encryption, authentication, and secure communication protocols, making them vulnerable to modern threats.
- **Continuous Operations:** 24/7 uptime requirements make active scanning or intrusive asset discovery impossible without disrupting critical processes.
- **Mixed Environments:** The interconnection of OT, IT, and IoT systems bring together the vulnerabilities of each domain and expand the attack surface.

What it Takes to Secure OT

- **OT-Native Passive Monitoring:** OT systems prioritize availability, uptime, and safety. Passive monitoring allows operators to detect threats and anomalies without risking disruptions. In contrast, active scanning sends queries to assets that can overwhelm sensitive OT systems or trigger unintended behaviors, particularly in legacy OT equipment.
- **Asset Profiles Linked to CVEs:** Knowing a device's make, model, and firmware version allows for direct correlation with known CVEs. This ensures each vulnerability is identified and addressed with precision.
- **Network Mapping Exposes Impact:** Mapping communication flows shows where CVEs on less critical devices might still enable lateral movement toward high-value assets. This insight ensures vulnerabilities are assessed in the context of their severity and operational impact.
- **Comprehensive Coverage of Assets:** IT and IoT devices may serve as potential attack vectors and should be embedded in the broader context of protecting OT assets responsible for critical operations.



How Dragos Helps

The Dragos Platform profiles each asset and correlates it with relevant CVEs, ensuring up-to-date visibility of risks. Visualizing communication paths helps identify how CVEs could be exploited within the network, allowing for preemptive segmentation. As new vulnerabilities emerge, the Platform updates asset inventories and network maps, ensuring organizations stay ahead of evolving threats.

Connecting **asset inventory and network mapping** to CVEs ensures organizations know what vulnerabilities exist and their impact across the network. The Dragos Platform provides the tools to continuously identify, track, and mitigate these risks, ensuring security while maintaining operational continuity.

Scenario

A **wastewater treatment plant** relies on legacy PLCs that lack authentication, encryption, and firmware update capabilities – making them insecure by design. Through the asset inventory in the Dragos Platform, these devices are identified and linked to CVEs. Network mapping shows that these PLCs communicate with IoT flow sensors over insecure protocols, creating a potential attack path. The team segments the PLCs within the network and restricts external access while monitoring for unusual activity until a long-term solution can be identified.





A Centralized Process for Managing Vulnerabilities

Given the complexity of OT environments, managing vulnerabilities effectively requires a **centralized process** that tracks vulnerabilities from identification through resolution. This approach ensures all teams—security, operations, and engineering—are aligned and address vulnerabilities without operational disruption. A centralized management system prevents vulnerabilities from slipping through the cracks by providing **visibility across departments and assets** throughout the lifecycle of each issue.

Key Challenges in OT Environments

- **Extended Resolution Timelines:** Patch deployments are delayed due to operational constraints, requiring vulnerabilities to be managed over extended periods.
- **Communications Across Teams:** Security, operations, and engineering teams often operate in silos, leading to misaligned priorities or duplicated efforts.
- **Compliance Pressures:** Regulatory frameworks like NERC CIP and ISA/IEC 62443 require detailed documentation of vulnerability management activities, which adds an administrative burden.

What it Takes to Secure OT

- **Unified Ticketing and Tracking System:** A single platform for all teams to log, update, and track vulnerabilities affecting OT from discovery to closure.
- **Collaboration Tools:** Role-based access for each team ensures efficient coordination without disrupting workflows.
- **Lifecycle Visibility with Continuous Updates:** Maintain real-time status of vulnerabilities, including threat intelligence updates, mitigation strategies, and patch schedules.
- **Automated Reporting:** Generate compliance-ready reports that track vulnerability status and risk management efforts.

How Dragos Helps

The Dragos Platform tracks **every step of the vulnerability lifecycle**, from discovery to mitigation and resolution, with a unified system. Teams work together seamlessly, with the ability to share insights, schedule patching windows, and align mitigation strategies. Integrated Dragos threat intelligence updates ensure tickets reflect the latest risks and mitigation priorities. Automated dashboards help ensure compliance with regulatory frameworks like NERC CIP and ISA/IEC 62443. They provide visibility into vulnerability status, mitigation efforts, and outstanding risks, saving time and reducing administrative overhead.

The Dragos Platform ensures vulnerabilities are managed seamlessly across departments by providing a **centralized tracking system** that aligns security, operations, and engineering teams. With integrated threat intelligence, real-time updates, and automated compliance reporting, organizations can stay ahead of vulnerabilities without disrupting critical operations.

Scenario

A **renewable energy facility** identifies a vulnerability in a wind turbine controller. The Dragos Platform identifies the CVE associated with the asset in a centralized tracking system. Security initiates temporary segmentation to reduce risk, and operations schedules a maintenance window for firmware updates. The platform ensures teams stay coordinated with automated notifications and status updates throughout the process. A final report is generated to meet regulatory requirements.



Prioritizing & Mitigating Vulnerabilities in Complex OT Environments

With vulnerabilities identified and processes in place to track them, the next challenge is deciding **which vulnerabilities to address first**. Not every issue can be patched immediately, especially in OT environments where uptime is critical. Here, priorities based on operational impact and mitigation strategies like segmentation and monitoring are essential. The focus shifts from simply identifying risks to efficiently managing them without disrupting industrial processes.

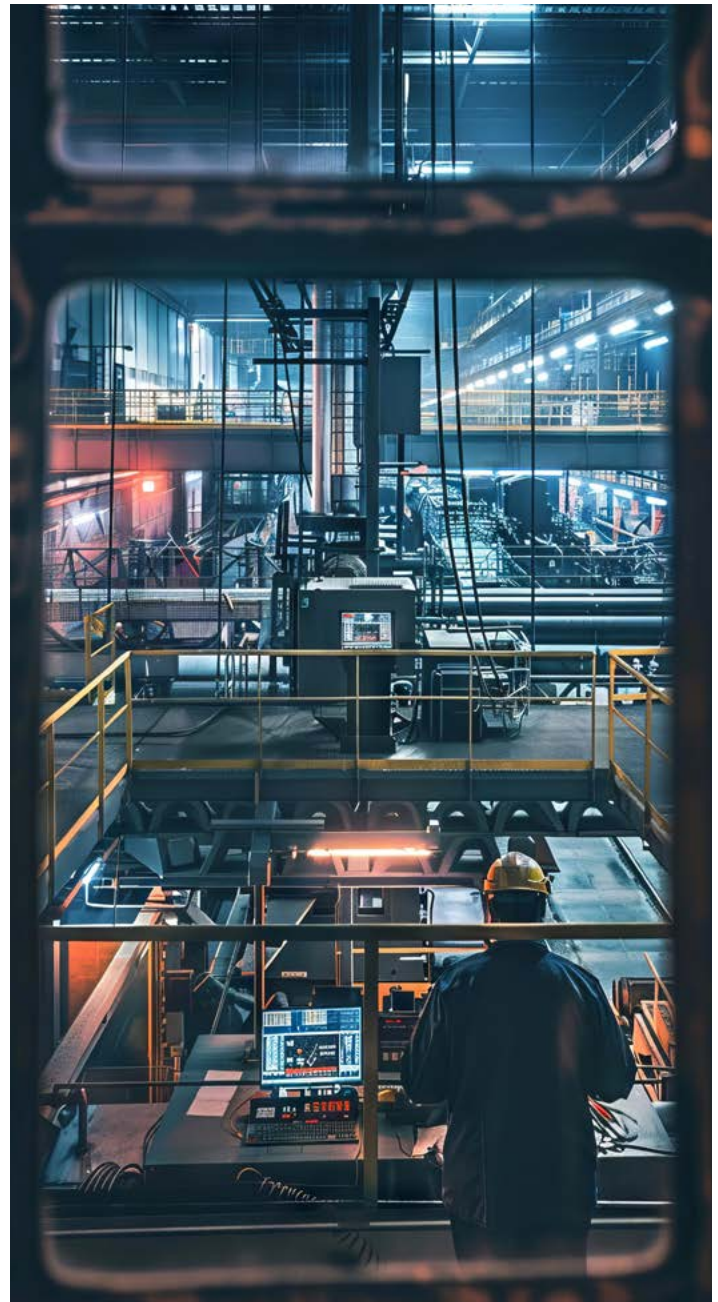
Key Challenges in OT Environments

- **Operational Constraints:** Continuous uptime limits the ability to apply patches or take systems offline.
- **Insecure-By-Design Equipment:** Many devices can't be patched or require vendor involvement, prolonging resolution timelines.
- **Lateral Movement Risks:** Vulnerabilities in low-priority systems can be exploited to reach high-value targets through interconnected networks.

What it Takes to Secure OT

Traditional IT vulnerability management approaches using CVSS scores to prioritize patching are insufficient for OT environments. OT systems must prioritize availability and safety; CVSS does not account for these operational factors.

- **Risk-Based Priorities:** Focus efforts on vulnerabilities affecting critical assets or safety systems, considering technical severity and operational impact.
- **Alternative Mitigation Strategies:** Apply compensating controls, such as network segmentation, enhanced access control, or monitoring, where patching is impossible.
- **Lateral Movement Prevention:** Segment networks and monitor communication paths to prevent adversaries from reaching critical systems.
- **Continuous Reassessment:** Stay responsive to emerging threats by updating priorities as new intelligence becomes available.



How Dragos Helps

The Dragos Platform provides real-time intelligence on vulnerabilities actively exploited in industrial sectors, helping teams focus on the most relevant risks. The Platform identifies high-risk communication paths and provides insights from applying segmentation to reduce lateral movement. The Dragos Platform's real-time asset and network monitoring ensures vulnerabilities are reassessed with every new threat or change in configuration.

The Dragos Platform enables organizations to **centrally manage vulnerabilities** that align with operational priorities and security needs. With real-time OT-specific threat intelligence, alternative mitigations, and continuous monitoring, the Platform supports efficient vulnerability mitigation, even under complex conditions. This risk-based approach prevents disruptions, protects critical systems, and keeps operations running smoothly.

Scenario

An **oil refinery** discovers a vulnerability in its pressure monitoring system, which must remain online to ensure safe operations. With no immediate patch available, the team applies strict access controls and isolates the monitoring system within a dedicated network segment. Real-time asset and network monitoring detects any unusual behavior targeting the system. The patch is deferred until the next planned maintenance cycle, minimizing operational impact while ensuring the system remains secure.





How Risk-Based Prioritization Brings Everything Together

Traditional IT vulnerability management approaches fail to account for the unique challenges of OT. Patch-all strategies aren't practical in environments where downtime costs millions or jeopardizes safety. A **risk-based approach** to vulnerability management focuses on vulnerabilities that pose the highest risk to operations, ensuring mitigation efforts align with business and security priorities. This shift in strategy allows organizations to protect what matters most while maintaining operational continuity.

Key Challenges in OT Environments

- **IT vs OT Misalignment:** CVSS score alone doesn't reflect the operational risks specific to OT systems.
- **Emerging Threats:** OT environments face sophisticated threats that require continuous risk reassessment.
- **Resource Constraints:** Limited personnel and time mean every mitigation effort must have the maximum impact.

What it Takes to Secure OT

- **Operationally Focused Prioritization:** Assess vulnerabilities based on technical severity and operational impact.
- **OT-Specific Threat Intelligence:** Continuously update vulnerabilities with real-time intelligence on emerging threats.
- **Flexible Mitigation Options:** Apply segmentation or enhanced monitoring when immediate patching isn't possible.

How Dragos Helps

The Dragos Platform helps organizations focus on the most significant operational risk vulnerabilities. It provides up-to-date threat intelligence on vulnerabilities being actively exploited, ensuring organizations can make smarter decisions. Dragos recommends alternative strategies for managing cyber risk in OT environments, like network segmentation and monitoring, to minimize disruptions.

Risk-based vulnerability management prioritizes mitigation and remediation of vulnerabilities that, if exploited, are the most likely to impact the industrial process. These vulnerabilities:

- Are known to be exploited by adversaries
- Provide access to industrial control systems (ICS) and OT networks
- Cause loss of view, loss of control, or loss of safety to the process

The Dragos Platform ensures organizations adopt a risk-based approach tailored to OT environments, focusing on what matters most: safety, uptime, and operational continuity. With integrated threat intelligence, real-time monitoring, and flexible mitigation options, Dragos helps organizations mitigate risks effectively across OT environments while keeping critical systems running smoothly.

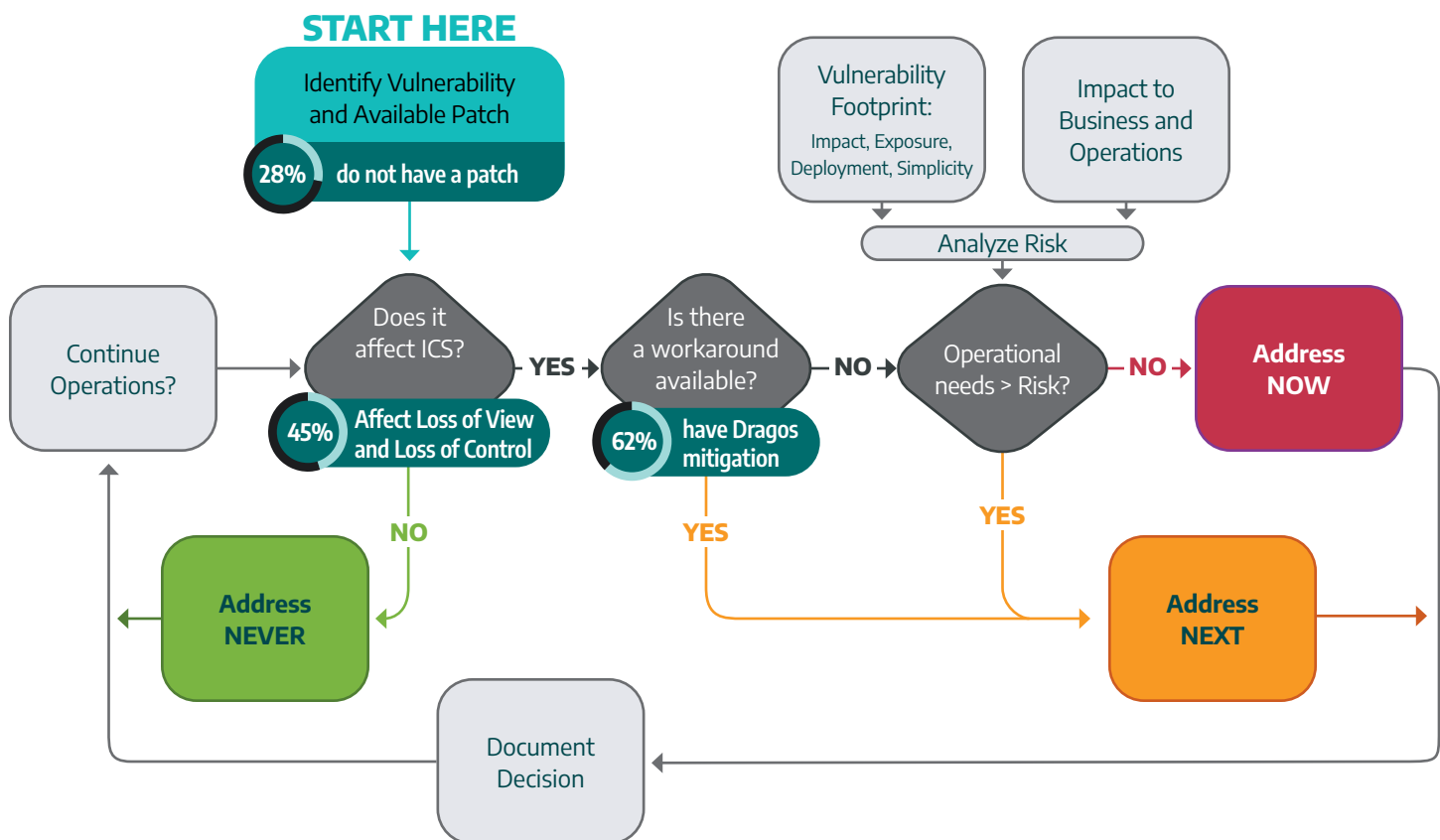
Scenario

A **power distribution company** initially classifies a vulnerability in a substation relay as low priority. However, Dragos threat intelligence alerts the team that adversaries exploit this vulnerability in similar environments. Recognizing the operational impact of a potential compromise, the team escalates the issue, applies segmentation to the relay, and schedules a patch as a priority task, preventing potential service disruption.



Using the DHS Patch Urgency Decision Tree

The [SANS ICS 5 Critical Controls](#) references the DHS Patch Urgency Decision Tree, which is an excellent resource for deciding whether a patch is worth the operational risk of an outage.



Solutions like the Dragos Platform support this approach by providing the visibility, intelligence, and monitoring required to assess risks and continuously make informed security decisions. This allows organizations to focus on what matters most—maintaining safe, reliable, and secure operations.

“Now, Next, Never” Methodology

Borrowed from [Art Manion](#), **Now, Next, and Never** are the priorities we set for vulnerabilities in the Dragos Platform. Those thresholds start with if you said “yes” to each of the inputs in the DHS Patch Urgency Tree on the previous page. These factors are considered in vulnerability assessments, and that determination is included per advisory in the database as “Now” vulnerabilities.

Dragos investigates each vulnerability and provides an assessment that generally includes mitigation advice in case a patch cannot be applied immediately or if the vendor doesn’t provide a patch or alternative mitigation. The evaluation considers the vulnerable component and how that impacts the rest of the process.

The “Next” vulnerabilities can be mitigated through proper network segmentation, returning us to the defensible architecture critical control. Often, network segmentation can be implemented without impacting the industrial process, where the alternative of patching these devices may cause an outage. After the network is segmented, adversaries must follow paths and chokepoints to get deep within the industrial network, where asset owners have the best insight to monitor for exploitation.

The “Never” vulnerabilities are items that will not improve the overall inherent risk of the device to your process even if you remediate fully. These vulnerabilities are generally overhyped, challenging to exploit, and vulnerable to the same impact via the available features.

The screenshot shows the Dragos Vulnerabilities dashboard. At the top, it displays '95 Vulnerability Detections' and '100 Unique CVE'. Below this, there are three summary cards: '18 Prioritized as "Now"', '33 Critical CVSS', and '24 Low/Medium Confidence'. A search bar and a 'Group By' dropdown are present. The main table lists vulnerabilities with columns for Title, Asset, CVE, CVSS, Risk Level, Confidence, Priority, First Detected, Last Detected, and Actions. The table is filtered by 'Risk Level' (4-High, 3-Medium, 5-Critical) and 'Priority' (Next, Now). The table shows 10 rows of data, including vulnerabilities for Siemens SIMATIC S7-300 CPUs and Schneider Electric Modicon M340 and B...

<input type="checkbox"/>	Title	Asset	CVE	CVSS	Risk Level	Confidence	Priority	First Detected	Last Detected	Actions
<input type="checkbox"/>	SIMATIC S7-300 CPUs and SINUMERIK...	PLC-5 192.168.40.31	CVE-2019-18336	7.5	4-High	Medium	Next	11/01/24, 11:27 AM EDT	11/04/24, 06:45 PM EST	⋮
<input type="checkbox"/>	Siemens SIMATIC S7-300 Denial-of-Ser...	PLC-5 192.168.40.31	CVE-2016-3949	7.5	4-High	Medium	Next	11/01/24, 11:27 AM EDT	11/04/24, 06:45 PM EST	⋮
<input type="checkbox"/>	Siemens SIMATIC PLCs Reported Issues...	PLC-5 192.168.40.31	—	—	3-Medium	Medium	Next	11/01/24, 11:27 AM EDT	11/04/24, 06:45 PM EST	⋮
<input type="checkbox"/>	Siemens TIM 1531 IRC Modules	PLC-5 192.168.40.31	CVE-2018-13816	10	5-Critical	Medium	Now	11/01/24, 11:27 AM EDT	11/04/24, 06:45 PM EST	⋮
<input type="checkbox"/>	Siemens SIMATIC S7-300 CPU	PLC-5 192.168.40.31	CVE-2018-16561	7.5	5-Critical	Medium	Now	11/01/24, 11:27 AM EDT	11/04/24, 06:45 PM EST	⋮
<input type="checkbox"/>	Schneider Electric Modicon M340 and B...	PLC-3 192.168.40.30	CVE-2024-5056	6.5	4-High	Medium	Next	11/01/24, 11:27 AM EDT	11/04/24, 06:15 PM EST	⋮
<input type="checkbox"/>	Schneider Electric Modicon Controllers	PLC-3 192.168.40.30	CVE-2018-7843 (+ 21 more)	9.8	4-High	Medium	Next	11/01/24, 11:27 AM EDT	11/04/24, 06:15 PM EST	⋮
<input type="checkbox"/>	Schneider Electric Modicon M340 contr...	PLC-3 192.168.40.30	CVE-2022-22724 (+ 1 more)	8.8	4-High	Medium	Next	11/01/24, 11:27 AM EDT	11/04/24, 06:15 PM EST	⋮
<input type="checkbox"/>	Schneider Electric Modicon M340 Buffe...	PLC-3 192.168.40.30	CVE-2015-7937	7.5	4-High	Medium	Next	11/01/24, 11:27 AM EDT	11/04/24, 06:15 PM EST	⋮

Essential Steps for Risk-Based Vulnerability Management

A **risk-based approach to vulnerability management** connects the critical elements of OT security – asset identification, network mapping, centralized management process, and correlated CVEs – into a cohesive strategy.

- Asset discovery provides the foundation by identifying what is in the environment and where vulnerabilities exist.
- Network mapping reveals which vulnerabilities pose the greatest threat through potential lateral movement or cross-network communication.
- Threat intelligence ensures that vulnerabilities are prioritized based on active threats and industry-specific risks.

By integrating OT-specific intelligence, continuous monitoring, and focused vulnerability assessments, a risk-based approach ensures that organizations can prioritize vulnerabilities effectively without jeopardizing operations.

1. Identify Critical Assets: Identify key OT assets essential to operational continuity and safety, such as SCADA systems or PLCs. If compromised, these “crown jewel” assets have the highest potential impact and must be prioritized for security efforts to prevent disruptions to core processes.

EXAMPLE: A SCADA system managing electrical distribution in a power grid is identified as a crown jewel asset as its failure would disrupt energy delivery to entire regions. Security efforts must prioritize protecting assets like SCADA over lower-risk administrative systems because an attack here could impact thousands of customers.

2. Map the OT Network and Understand Communication

Paths: Map OT networks to understand how devices communicate and where vulnerabilities might lie. This step identifies potential attack paths, facilitating better segmentation and security controls. The Purdue model can map out OT networks and identify critical zones, such as Level 1 devices like PLCs and Level 3 like SCADA and DMZs. Visualizing communication between OT and IT systems, as well as internal OT communications, is critical. Identifying risky communications, such as devices with outdated protocols, is crucial to the assessment.

EXAMPLE: A manufacturing facility discovers that engineering workstations communicate with PLCs controlling the production line. An outdated communication path between these devices poses a potential entry point for adversaries. Understanding the network paths helps reveal unexpected connections, which can be segmented to prevent lateral movement in case of an attack.

3. Assess Vulnerability Impact on Operations: Beyond simply analyzing the technical aspects of a vulnerability, assess how its exploitation could affect physical processes, safety, or system availability. OT-specific threat intelligence is essential for understanding the real-world implications of a vulnerability in the context of the industrial environment and threat landscape. Focus on the most critical assets and prioritize vulnerabilities that could disrupt operations or threaten safety.

EXAMPLE: A known vulnerability in an HMI controlling safety systems is discovered. Although it has a medium CVSS score, the asset's criticality for ensuring safety escalates its priority. Operational and safety impacts must be factored into prioritization. Addressing vulnerabilities based on asset criticality ensures that security actions align with operational risks.

4. Implement Alternative Mitigations: Organizations should consider alternative mitigation strategies when immediate patching is impossible due to operational constraints. These include network segmentation, enhanced monitoring, access control adjustments, or temporary system isolation to reduce exposure.

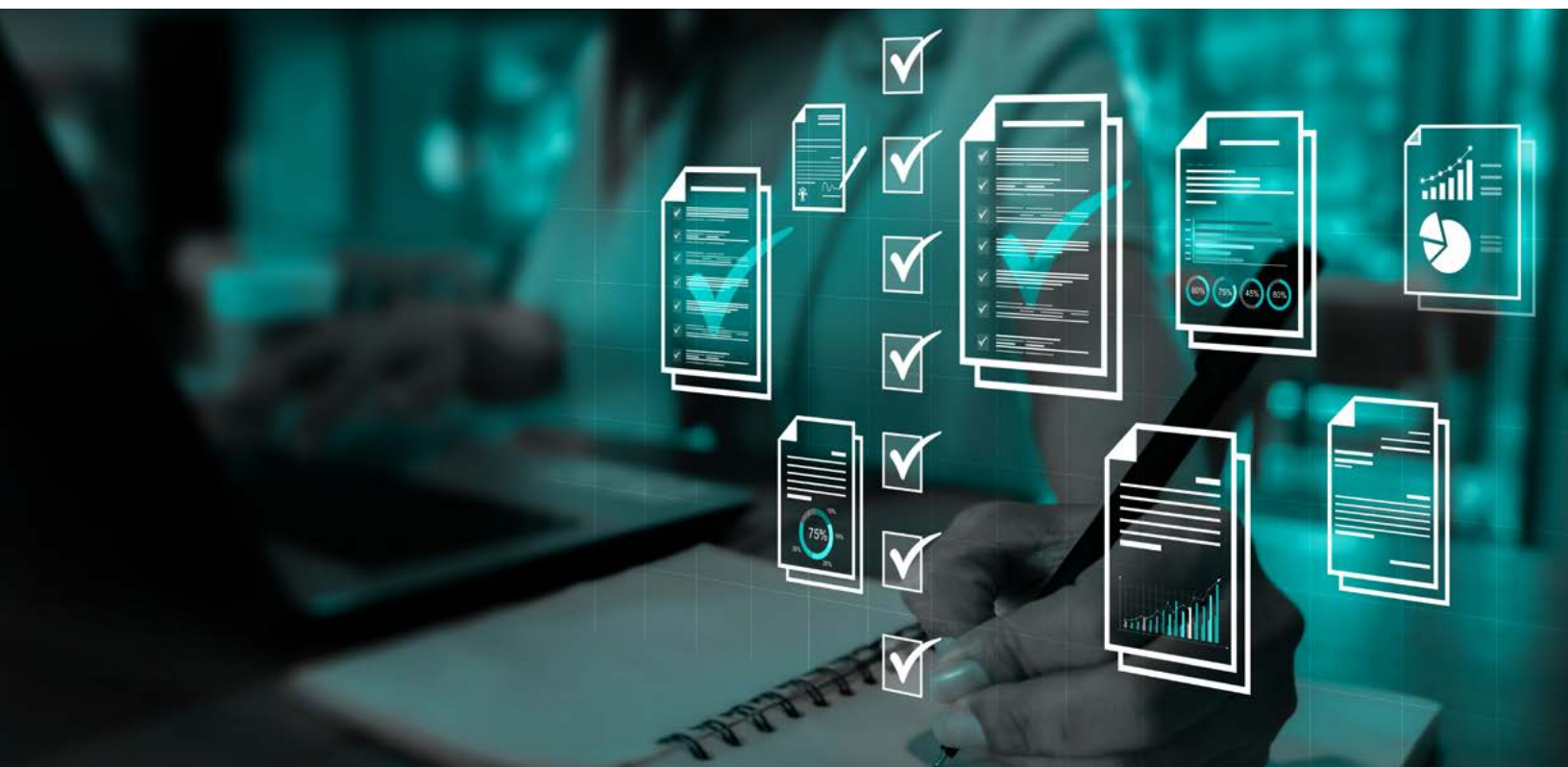
EXAMPLE: A legacy PLC cannot be patched due to vendor limitations, so the organization implements network segmentation and restricts access to only essential users. Alternative mitigations like segmentation ensure the vulnerability is managed without causing downtime or disrupting operations.


5. Leverage Continuous Monitoring of Anomalous Activity and Threat Behavior: Continuous monitoring detects unusual activities or behaviors, alerting teams to threats before they impact operations. OT-specific monitoring tools provide insights into industrial protocols.

DRAGOS PLATFORM: Continuous monitoring helps organizations identify when vulnerabilities are actively exploited and when immediate action is necessary by tracking assets, communication patterns, and behaviors.

6. Track and Manage Vulnerabilities Across Their Lifecycle: Effective vulnerability management relies on cross-team collaboration, ensuring each stakeholder plays a role in mitigation and resolution. Security teams assess the vulnerabilities, while operations and engineering teams provide input on maintenance windows and ensure changes won't disrupt critical processes. This coordinated effort ensures vulnerabilities are tracked in real time, mitigated through practical measures, and resolved at the earliest opportunity.

EXAMPLE: A ticket is created to address a vulnerability in a SCADA server. The security teams assess the severity and recommend segmentation. Operations teams schedule downtime during a planned maintenance window while engineering deploys the patch and updates the ticket with resolution details.





Achieve Resilience and Operational Security with the Dragos Platform

Comprehensive vulnerability management across OT environments requires a tailored approach that aligns security efforts with operational priorities. From identifying every asset and mapping communication paths to centralized vulnerability tracking and mitigating risks under complex conditions, each step builds toward a unified strategy. Traditional IT methods fall short in OT environments, where uptime, safety, and operational continuity are paramount.

The Dragos Platform integrates OT-specific threat intelligence, real-time asset and network monitoring, and flexible mitigation strategies, enabling organizations to proactively address vulnerabilities without compromising operations. With Dragos, teams collaborate seamlessly, prioritize effectively, and stay ahead of evolving threats, ensuring security and resilience.



Dragos is an industrial (ICS/OT) cybersecurity company on a mission to safeguard civilization.

Dragos is privately held and headquartered in the Washington, D.C. area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

[Dragos.com](https://dragos.com)

