DRAGOS

GUIDE

# Risk-Based Vulnerability Management for xOT Environments

A framework for prioritizing risk across the extended operational environment, so teams act on what threatens the process and leave the rest alone.

## Overview

The operational environment is no longer just PLCs and SCADA. Extended Operational Technology (xOT) includes every technology that directly or indirectly influences a physical process: engineering workstations, remote access, cloud and AI systems, automation and robotics, facility infrastructure, and the data centers that keep operations running. Enterprise IT belongs in scope when it can affect operations, not by default. Thousands of vulnerabilities each year affect the technologies deployed across xOT environments, far more than any team can review, let alone remediate. The challenge is knowing which demand action and how to respond without risking operations. This guide provides a framework for managing vulnerabilities across xOT environments through asset inventory and network mapping, centralized tracking, prioritization, and risk-based mitigation. It is based on the "Now, Next, Never" model used in the Dragos Platform. The Dragos Platform combines asset and network context with threat intelligence from the Dragos Intelligence Fabric to determine which vulnerabilities require action now, next, or never, and to guide the appropriate response.

## The Challenge

### The Scope of Your Vulnerability List Is Now Larger Than Your OT Program

For years, systems were sorted by type. OT here, IT there, IoT somewhere in between. Those categories describe what a system is. They say nothing about what those systems do.
This changes vulnerability management before prioritization even begins. If the asset inventory reflects the old definition of OT, the vulnerability list is incomplete at the start. Environmental sensors feeding control systems, building automation platforms sharing network infrastructure with controllers, remote access infrastructure, analytics platforms: none of them appear in a program scoped to the traditional OT core, and all of it can influence operations.

Adversaries are not working from that outdated map. They take whatever path moves them closer to the physical process, and the time between disclosure and exploitation keeps shrinking. Systems left out of the inventory are exactly that path: initial access, trusted connections, and a route to critical assets.

## The Approach

### The Framework for Managing Risk in xOT Environments

01
**Asset Inventory**
One asset inventory operators can trust, with every value traceable to its source.

02
**Network Mapping**
Deep packet inspection of 600+ OT protocols that reveal reachability and lateral movement.

03
**OT-Corrected Scoring**
Revised CVSS scores for xOT environments and impact.

04
**"Now, Next, Never"**
Three priorities simplified and actionable.

05
**Alternative Mitigations**
Risk reduction when patching is not on the table.

06
**Centralized Tracking**
One record from identification through resolution.


© 2026 Dragos, Inc. All Rights Reserved.

# Asset Inventory and Network Mapping

## The Foundation

Effective vulnerability management starts with knowing what devices are in your environment and how they communicate. A complete asset inventory covers every device, from PLCs and HMIs to IoT sensors and engineering workstations, down to exact hardware, firmware, operating system, version, function, and lifecycle status. That detail ties a vulnerability to the equipment it affects and shows which devices are nearing end of support. Network mapping adds context by visualizing communication paths and data flows, revealing where vulnerabilities may expose critical systems to attack paths. Under an xOT scope, the inventory must reach past the traditional OT core to any system that can influence a physical process, whichever team owns it and whichever category it was filed under.

### Key Challenges in OT Environments

- **Long asset lifecycles.** Devices stay in service for decades, often built before security was a design consideration. Many lack encryption or authentication, cannot be retrofitted, and keep accumulating vulnerabilities after vendor support ends.
- **Limited patching options.** Patches may not exist, may need vendor involvement, or may require requalification. Even when a fix is available, the window to apply it can be months away.
- **Operational constraints.** Downtime carries a direct cost to production and safety, and discovery methods not designed for OT put uptime at risk before the first vulnerability is found.
- **Prioritization without context.** Published severity scores describe a vulnerability in the abstract. Without knowing what a device does, what it can reach, and whether adversaries are exploiting it, teams either chase every advisory or ignore them all.
- **Extended environments.** Blending OT, IT, and IoT combines the vulnerabilities of each domain, with ownership split across more teams than the inventory accounts for.

### What It Takes to Secure xOT

- **OT-aware collection, active and passive.** Passive monitoring covers the network continuously. Controlled active collection fills in what traffic doesn't carry, from rarely communicating devices to host and module detail, without putting the process at risk.
- **Coverage across hardware, firmware, operating systems, and software.** Vulnerabilities map to curated device and configuration profiles, so make, model, firmware version, and OS correlate to real exposure.
- **Network mapping exposes reachability.** Mapped flows show where vulnerabilities on less critical devices could enable lateral movement toward high-value assets.
- **Coverage defined by influence, not category.** IT and IoT devices that can affect the process belong in scope. The test is what a system does, not what it is.
- **Inventory not limited by sensor coverage.** Scanners, endpoint collection, third-party tools, and file import feed one inventory, so segments that network monitoring cannot reach stay in scope and coverage gaps become measurable.


© 2026 Dragos, Inc. All Rights Reserved.

## How Dragos Helps

The Dragos Platform profiles each asset and correlates its hardware, firmware, operating system, software, and communications with relevant vulnerabilities. Passive monitoring across 600+ industrial protocols is the foundation, with active collection adding depth in segments that carry little traffic and file import covering sites that monitoring cannot reach. Visualizing communication paths shows how a vulnerability could be exploited within the network. Segmentation validation goes a step further: the Platform reads firewall, router, and switch configurations to reveal every path they permit, including paths that have never carried traffic, and sets those against the traffic sensors actually observe. That is how a team confirms that compensating controls hold and that critical vulnerabilities are isolated from attack paths rather than assuming they are. As new vulnerabilities emerge, the Platform updates asset inventories, network maps, and the exposure picture along with them.

### SCENARIO

A wastewater treatment plant relies on legacy PLCs that lack authentication, encryption, and firmware update capabilities and cannot be updated in place. Through the asset inventory in the Dragos Platform, these devices are identified and linked to known vulnerabilities.

Network mapping shows that the 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 unusual activity until a longer-term fix can be identified.


© 2026 Dragos, Inc. All Rights Reserved.

# A Centralized Process for Managing Vulnerabilities

## The Process

Given the complexity of xOT environments, managing vulnerabilities takes a centralized process that tracks them from identification through resolution. This keeps security, operations, and engineering aligned and addresses vulnerabilities without operational disruption. A centralized 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 by operational constraints, so vulnerabilities must be managed over extended periods.
- **Communications across teams.** Security, operations, and engineering often work in silos, which leads to misaligned priorities or duplicated effort. Under an xOT scope, ownership is split across even more teams.
- **Compliance pressures.** Frameworks such as NERC CIP and ISA/IEC 62443 require detailed documentation of vulnerability management activity, which adds administrative burden.

### What It Takes to Secure xOT

- **Status that reflects OT reality.** Open, in progress, and closed cannot express what happens to an OT vulnerability. Work sits in assessment, waits on a vendor patch, gets scheduled for an outage months out, or is risk-accepted with controls in place and a review date attached. Tracking systems that only model resolution push the real work into spreadsheets.
- **Collaboration across roles.** Role-based access for each team supports coordination without disrupting existing workflows.
- **Lifecycle visibility with continuous updates.** Maintain status on every vulnerability, including threat intelligence updates, mitigation guidance, whether the affected asset is still vendor-supported, and whether a patch is available.
- **Reporting for audit.** Reporting should map to the frameworks the organization is actually measured against, including NERC CIP, IEC 62443, NIS2, and TSA, with evidence collected continuously rather than assembled in the week before an assessment.
- **Evidence attached to the fix.** A closed vulnerability should carry proof: what changed, who approved it, when it was verified. Maintenance schedules with assigned ownership turn a backlog into work that can be tracked to completion.


© 2026 Dragos, Inc. All Rights Reserved.

## How Dragos Helps

The Dragos Platform tracks every step of the vulnerability lifecycle in one system. Teams work from the same record, with the ability to share findings, coordinate maintenance windows, and align mitigation. Dispositions map the real lifecycle rather than a flat open-and-closed model, so risk acceptance carries its compensating controls and a review date. Analysts work at the disposition level while leadership sees the portfolio roll-up.

### Dispositions and State Management

Every vulnerability sits in one of six states: New, Active, Triaging, Under Review, Planned, and Closed. Underneath, dispositions capture what is actually happening: assessment underway, blocked on a vendor patch, scheduled for the next outage, or risk-accepted with compensating controls in place.

Practitioners set dispositions through the Platform interface or the API as work progresses. Because every disposition rolls up to a parent state, leadership sees the portfolio while analysts work at the level of detail their job requires. Teams can add custom dispositions where a local workflow needs one.

Risk acceptance stops being a checkbox. An accepted finding carries the controls that justify the decision and the date it will be reviewed again. That is the difference between a defensible position in front of an auditor and an assertion. It also makes service level measurement mean something, because the clock is attached to a state that reflects real movement rather than a binary open or closed.

**SCENARIO**

A renewable energy facility identifies a vulnerability in a wind turbine controller. The Dragos Platform associates the vulnerability with the affected asset in a centralized tracking system.

Security initiates temporary segmentation to reduce risk, and operations identifies a maintenance window for the firmware update. The vulnerability is set to a Planned disposition so everyone can see it is scheduled for that outage. Teams stay coordinated through notifications and status updates throughout the process, and a final report is generated to meet regulatory requirements.


© 2026 Dragos, Inc. All Rights Reserved.

# Prioritizing and Mitigating Vulnerabilities

## Prioritization

With vulnerabilities identified and a process in place to track them, the next challenge is deciding which to address first. Not every issue can be patched immediately, particularly where uptime is critical. Priorities based on operational impact, paired with mitigation strategies such as segmentation and monitoring, are what makes this workable.

### Key Challenges in OT Environments

- **Operational constraints.** Continuous uptime limits the ability to apply patches or take systems offline.
- **Unpatchable equipment.** Many devices cannot be patched or require vendor involvement that extends resolution timelines.
- **Lateral movement risk.** Vulnerabilities in low-priority systems can be exploited to reach high-value targets across interconnected networks.

### What It Takes to Secure xOT

Traditional IT vulnerability management approaches that use CVSS scores to prioritize patching are insufficient for OT environments. OT systems must prioritize availability and safety, and CVSS does not account for either.

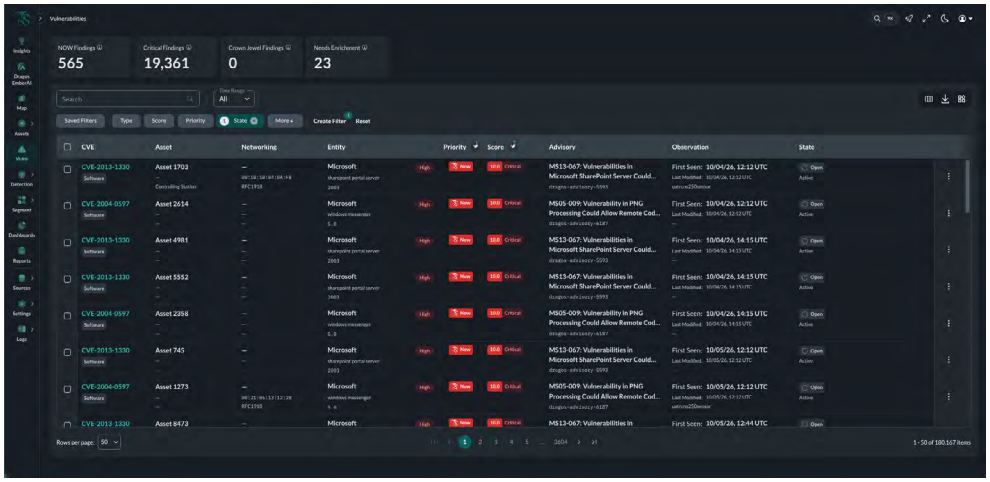
- **Risk-based priorities.** Focus effort on vulnerabilities affecting critical assets or safety systems, weighing both technical severity and operational impact.
- **Alternative mitigation strategies.** Apply compensating controls such as network segmentation, tighter access control, or enhanced monitoring where patching is not possible.
- **Lateral movement prevention.** Segment networks and monitor communication paths to prevent adversaries from reaching critical systems.
- **Continuous reassessment.** Neither the classification of a vulnerability nor the environment around it is permanent. As new intelligence arrives and exposure, compensating controls, and connectivity change, priority should move with them, weighed on blast radius as well as severity.

> **WHAT OT-CORRECTED SCORING MEANS**
>
> Published CVSS scores describe a vulnerability in the abstract; OT-corrected scoring describes it in your environment, weighing reachability, known exploitation by ICS-targeting groups, existing controls, and process impact. The result moves both ways: a critical-rated vulnerability in IT may have no exploitable path into your OT network, while a medium-severity one on a crown jewel asset exposed at the IT/OT boundary may be your top priority.


© 2026 Dragos, Inc. All Rights Reserved.

## How Dragos Helps

The Dragos Platform provides current intelligence on vulnerabilities being actively exploited against OT, which helps teams focus on the most relevant risk. The Platform identifies high-risk communication paths, and when a vulnerability can't be patched, it validates that segmentation keeps the affected asset out of reach. As threats emerge and monitoring picks up changes in the environment, priorities are reassessed.



### 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.

Asset and network monitoring detect any unusual behavior targeting the system. The patch is deferred to the next planned maintenance cycle, minimizing operational impact while the system stays protected.

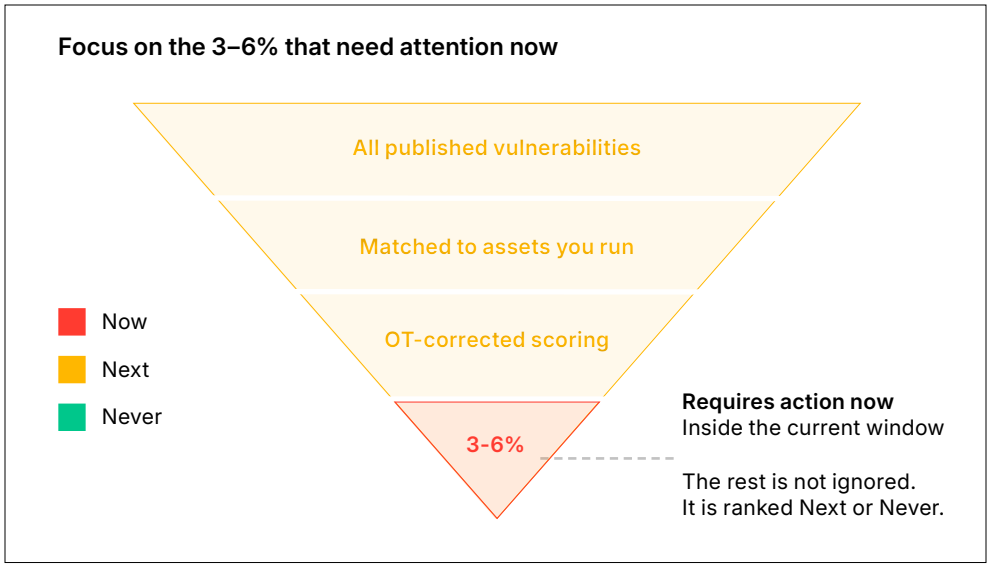

© 2026 Dragos, Inc. All Rights Reserved.

# How Risk-Based Prioritization Brings Everything Together

## The Model

Traditional IT vulnerability management approaches fail to account for the constraints of OT. Patch-all strategies are not practical where downtime costs millions or affects safety. A risk-based approach focuses on the vulnerabilities that pose the highest risk to operations, so mitigation effort aligns with both business and security priorities.

The Dragos 2026 OT Cybersecurity Year in Review found that only 3 to 6 percent of the vulnerabilities in a given environment require action inside the current operational window. That figure is not permission to ignore the rest. It is a statement about where finite maintenance windows, engineering hours, and vendor coordination should go first.




Source: Dragos 2026 OT Cybersecurity Year in Review

Each stage above narrows the list against a different question. Every published vulnerability is the starting universe. Matching to real assets removes everything that does not correspond to hardware, firmware, and operating systems actually deployed. OT-corrected scoring then removes what cannot be reached or exploited in this architecture, and raises what sits closer to the process than its published score suggests. What survives all three is the Now tier.

The remainder is ranked, not discarded. Dragos recommends that Next vulnerabilities be remediated in an upcoming maintenance window. That window could be months away, so Dragos provides OT-specific compensating controls to reduce risk in the meantime. With Never vulnerabilities, remediation would not materially reduce risk to the device or the process.

The impact is already available through the device's own features, the vulnerability is not realistically exploitable, or its published severity overstates the operational effect. A vulnerability management program that can account for all three tiers is defensible in front of an auditor in a way that an open backlog is not.

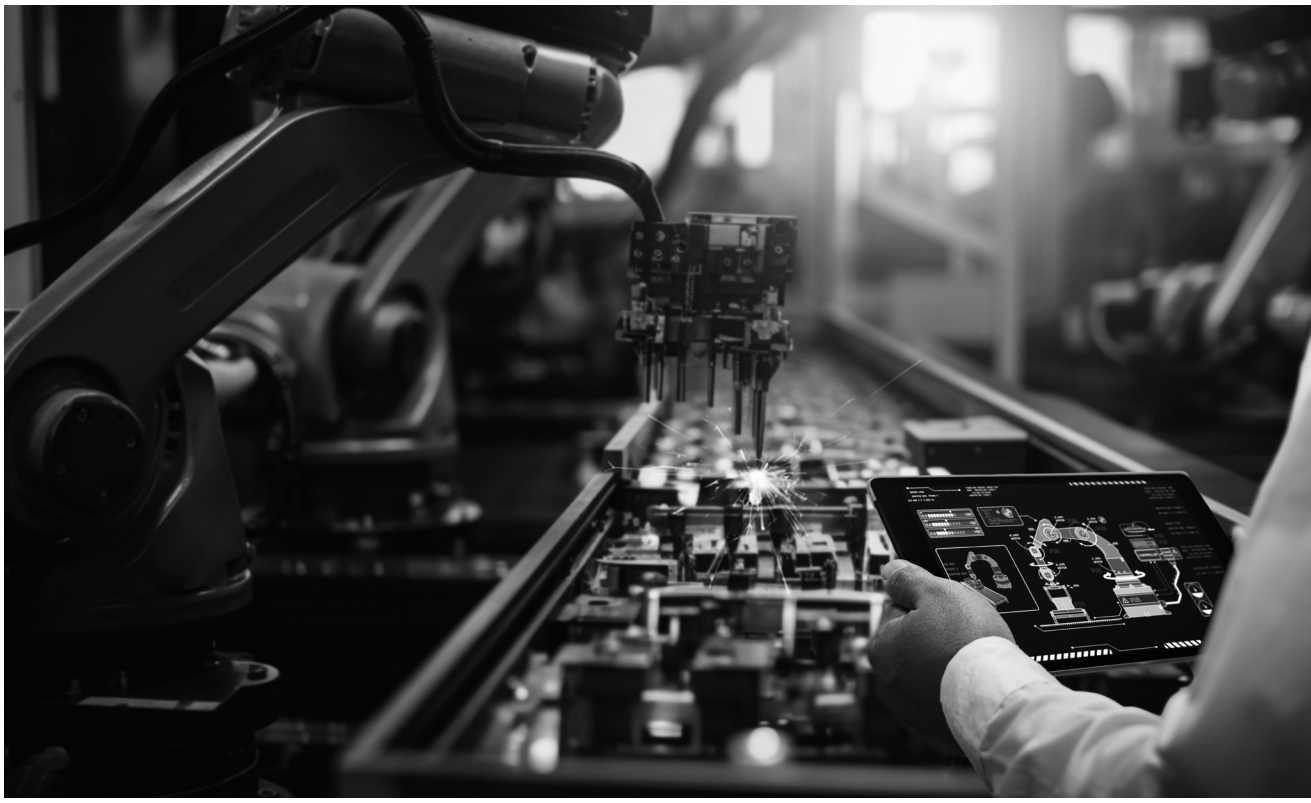

© 2026 Dragos, Inc. All Rights Reserved.

## Key Challenges in OT Environments

- **IT and OT misalignment.** CVSS score alone does not reflect the operational risk specific to OT systems.
- **Emerging threats.** Evidence of active exploitation, new exploit code, or adversaries targeting an affected technology or sector can increase the urgency of an existing vulnerability.
- **Resource constraints.** Limited personnel and time mean every mitigation effort must count.

## What It Takes to Secure xOT

- **Operationally focused prioritization.** Assess vulnerabilities on both technical severity and operational impact.
- **xOT threat intelligence.** Reassess vulnerabilities using evidence of active exploitation, affected systems and configurations, exploitation requirements, and available detection or mitigation guidance.
- **Flexible mitigation options.** Apply segmentation or enhanced monitoring when immediate patching is not possible.




© 2026 Dragos, Inc. All Rights Reserved.

## How Dragos Helps

Vulnerability research and adversary intelligence from the Dragos Intelligence Fabric reach the Platform through weekly Knowledge Packs. The Platform matches each vulnerability against the assets actually in the inventory, by hardware, firmware, operating system, and software, and applies the OT-corrected priority Dragos researchers assigned. When new exploitation evidence arrives or the environment changes, the priority moves with it.

The result is a working list of confirmed vulnerabilities on deployed assets that adversaries can reach and use to affect operations. The highest priorities are vulnerabilities that:

- Are known to be exploited by adversaries
- Could give adversaries the access or control needed to influence a physical process
- Cause loss of view, loss of control, or loss of safety to the process

### SCENARIO

A power distribution company initially classifies a vulnerability in a substation relay as low priority. Dragos threat intelligence then alerts the team that adversaries are exploiting this vulnerability in similar environments.

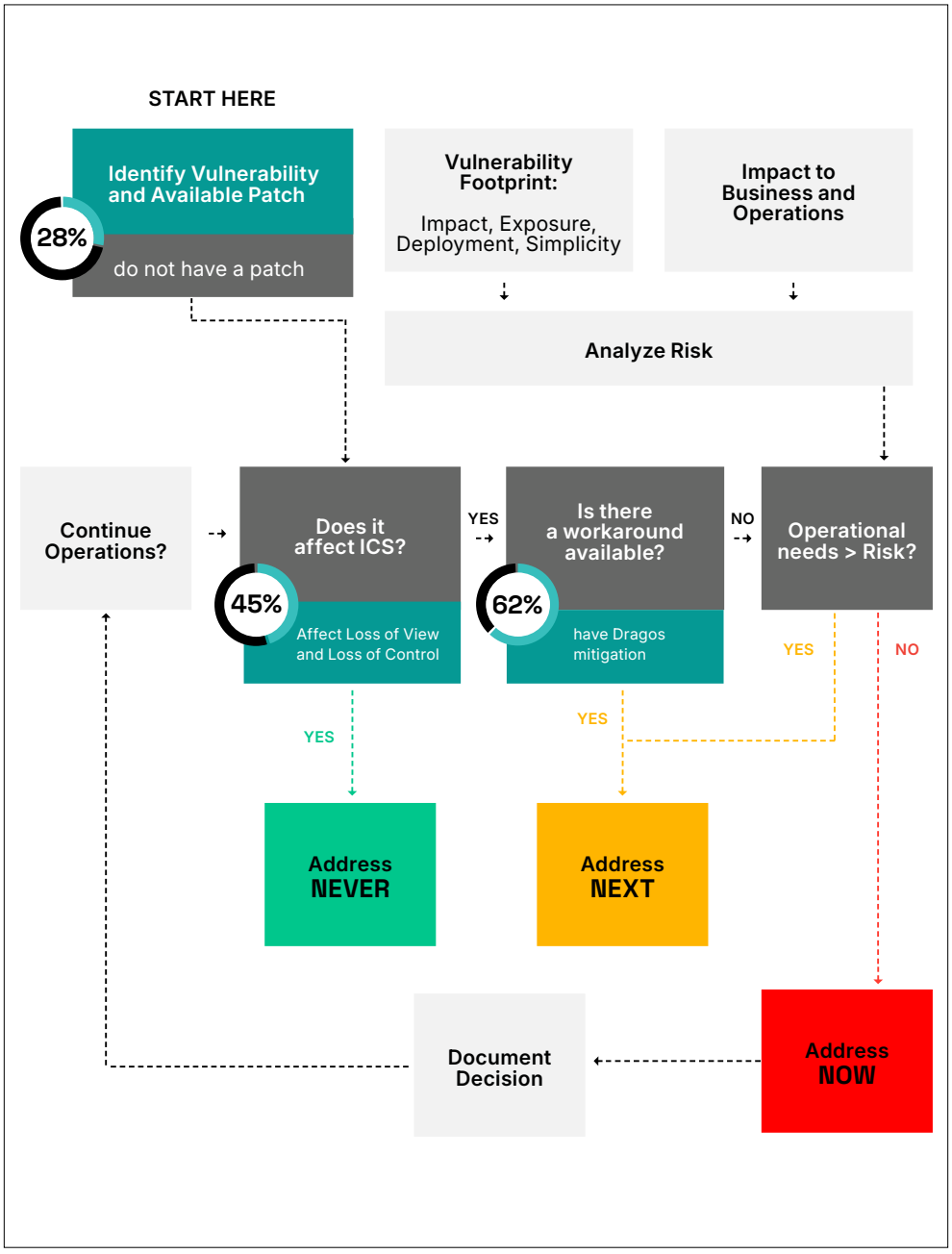
Recognizing the operational impact of a potential compromise, the team escalates the issue, applies segmentation to the relay, and schedules a patch as a priority task, preventing potential service disruption.


© 2026 Dragos, Inc. All Rights Reserved.

# The Decision

## Using the DHS Patch Urgency Decision Tree

The SANS ICS 5 Critical Controls references the DHS Patch Urgency Decision Tree, which is a useful reference for deciding whether a patch is worth the operational risk of an outage.




The Dragos Platform supports this approach by providing the visibility, intelligence, and monitoring required to assess risk and make informed security decisions on a continuing basis. That lets teams focus on maintaining safe, reliable, and secure operations.


© 2026 Dragos, Inc. All Rights Reserved.

# The Methodology

## Priority, Score, and Confidence in the Platform

Now, Next, and Never are the priorities Dragos sets for vulnerabilities in the Dragos Platform. Those thresholds start with the inputs in the DHS Patch Urgency Tree on the previous page. These factors are considered in vulnerability assessments, and the determination is included per advisory.

| NOW | NEXT | NEVER |
|---|---|---|
| Actively exploited, reachable in your environment, and tied to crown jewel assets or safety systems. | Significant but not immediately exploitable. Not yet actively exploited, partially mitigated by existing architecture, or constrained by operational access. | Will not materially improve the security posture of the device or environment even if fully remediated. |
| Act within the current operational window. Patch where possible. Apply compensating controls where patching is not yet feasible. | Plan remediation for the next available maintenance window. Track and monitor. Review if threat intelligence indicates the risk profile is changing. | Deprioritize. Do not spend a maintenance window on remediation that produces no risk reduction. Re-evaluate if threat intelligence shows the risk profile changing. |

In the Dragos Platform, the tier assignment sits alongside the published CVSS score rather than replacing it, so an analyst can see both the generic severity and the OT-corrected priority on the same row. Filtering to Now produces the working list. Confidence indicates how firmly the vulnerability has been matched to that specific asset.

High confidence means the Platform has confirmed that the vulnerability affects that specific asset. Medium confidence indicates a partial match that needs further qualification before the finding is worked. Where crown jewel assets have been tagged, a dedicated insight surfaces the count of Now-priority vulnerabilities carrying high-confidence matches on those assets, linking straight through to a filtered view of them.

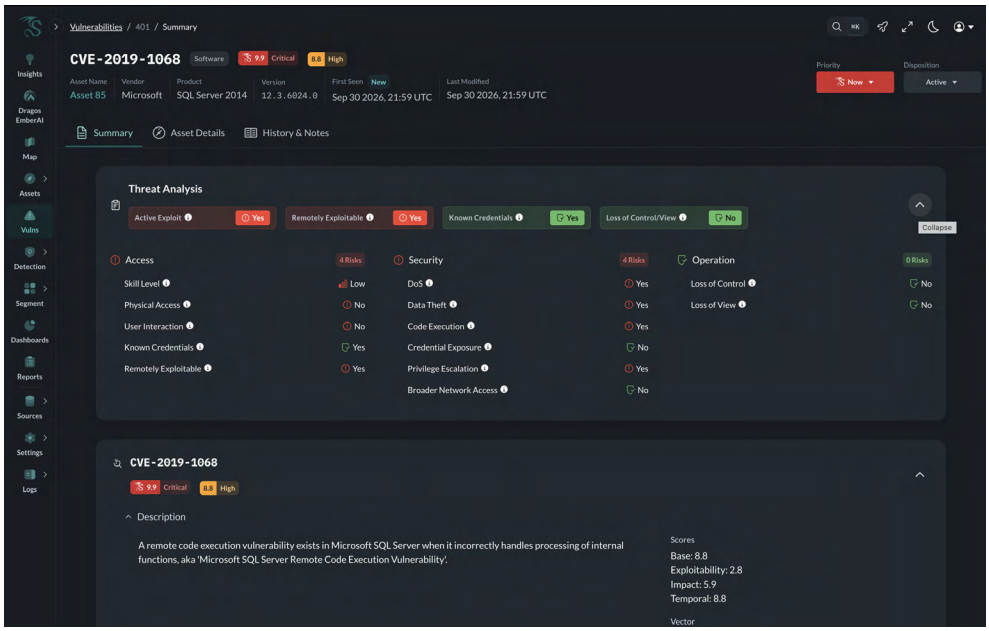
Dragos investigates vulnerabilities and provides an assessment that generally includes mitigation advice, in case a patch cannot be applied immediately or the vendor does not provide one. The evaluation considers the vulnerable component and how it affects the rest of the process.

Most Next vulnerabilities can be mitigated through network segmentation, which returns to the defensible architecture critical control. Segmentation can usually be implemented without impacting the process, where patching the same device might cause an outage. Once the network is segmented, adversaries must follow paths and chokepoints to get deep into the OT network, and those are exactly the places asset owners have the best visibility to monitor. Segmentation is only a control if it holds. Validating it against firewall, router, and switch configurations gives the team, and the auditor, evidence rather than assumption.


© 2026 Dragos, Inc. All Rights Reserved.

Segmentation is only a control if it holds. Validating it against firewall, router, and switch configurations gives the team, and the auditor, evidence rather than assumption.

Never vulnerabilities stay in the inventory and are re-evaluated as intelligence changes, but they do not earn a maintenance window. Remediating them would not reduce risk to the process, because the same impact is already available through the device's own features, the vulnerability is not realistically exploitable, or its published severity overstates the operational effect.




Vulnerabilities view in the Dragos Platform, showing Now, Next, and Never priority alongside CVSS score and match confidence.

## The Steps

## Essential Steps for Risk-Based Vulnerability Management

A risk-based approach connects the critical elements of xOT security, asset identification, network mapping, a centralized management process, and correlated vulnerabilities, into one 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 prioritizes vulnerabilities based on active threats and sector-specific risk.


© 2026 Dragos, Inc. All Rights Reserved.

## Identify Critical Assets

Identify the systems essential to operational continuity and safety, using the control loop test rather than device category. If compromised, these crown jewel assets carry the highest potential impact and should be prioritized to prevent disruption to core processes.

**EXAMPLE**

A control system managing electrical distribution in a power grid is identified as a crown jewel asset, because its failure would disrupt energy delivery across entire regions. Security effort should prioritize it over lower-risk administrative systems, because an attack there could affect thousands of customers.

## Map the Network and Understand Communication Paths

Map the operational network to understand how devices communicate and where vulnerabilities might lie. This identifies potential attack paths and supports better segmentation. The Purdue model can help identify critical zones. Identifying risky communications, such as devices using outdated protocols, is central to the assessment.

**EXAMPLE**

A manufacturing facility discovers that engineering workstations communicate with the PLCs controlling the production line. An outdated communication path between them is a potential entry point. Understanding the network paths reveals unexpected connections, which can then be segmented to prevent lateral movement.

## Assess Vulnerability Impact on Operations

Beyond the technical characteristics of a vulnerability, assess how exploitation could affect physical processes, safety, or availability. OT-specific threat intelligence is what makes that assessment real rather than theoretical.

**EXAMPLE**

A known vulnerability is discovered in an HMI controlling safety systems. Although it carries a medium CVSS score, the asset's criticality to safety escalates its priority. Operational and safety impact belong in the prioritization decision.


© 2026 Dragos, Inc. All Rights Reserved.

## Implement Alternative Mitigations

Where immediate patching is not possible, apply network segmentation, enhanced monitoring, access control adjustments, or temporary 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 essential users only. The vulnerability is managed without downtime.

## Use Continuous Monitoring of Anomalous Activity and Threat Behavior

Continuous monitoring detects unusual activity and alerts teams before it affects operations. OT-specific monitoring provides visibility into the protocols that matter.

**DRAGOS PLATFORM**

Continuous monitoring helps identify when vulnerabilities are actively exploited and when immediate action is warranted, by tracking assets, communication patterns, and behaviors.

## Track and Manage Vulnerabilities Across Their Lifecycle

Effective vulnerability management relies on cross-team collaboration. Security teams assess, while operations and engineering provide input on maintenance windows and confirm that changes will not disrupt critical processes.

**EXAMPLE**

A vulnerability is identified on a control server. Security assesses severity and recommends segmentation. Operations schedules downtime during a planned maintenance window while engineering deploys the patch and records the resolution.


© 2026 Dragos, Inc. All Rights Reserved.

## Why Dragos

01

### Built for the Full xOT Environment

Vulnerability matching runs against every system that can influence the process, not just the traditional OT core. Assets are profiled by make, model, firmware, and communication context, so exposure maps to equipment that actually exists in the environment.

02

### OT-Corrected Scoring, Not Generic Severity

Dragos vulnerability researchers review and correct published scores against reachability, active exploitation by ICS-targeting groups, existing compensating controls, and real process impact. Corrections move in both directions.

03

### Guidance That Works Without a Maintenance Window

When patching is not viable, guidance covers segmentation, access restriction, configuration change, and detection coverage, so risk drops before the window arrives rather than after it.

04

### Kept Current Through Knowledge Packs

New vulnerabilities, updated OT-corrected scores, refreshed mitigation guidance, and new detections arrive weekly. The research behind them comes from Dragos vulnerability researchers and intelligence analysts working exclusively in operational environments.

05

### Grounded in the Dragos Intelligence Fabric

The Dragos Intelligence Fabric brings together vulnerability research and insights from adversary activity, frontline experience, and exclusive telemetry. The Dragos Platform combines that intelligence with asset, network, and operational context to determine what requires action now, next, or never.

06

### Triage That Moves at the Speed of the Window

Dragos EmberAI puts that same intelligence in the hands of every analyst, through expert-built Skills for crown jewel analysis and vulnerability prioritization that run the triage a Dragos analyst would.


© 2026 Dragos, Inc. All Rights Reserved.

## How Dragos Helps

### 01

### Identify

Build inventory across the full operational environment and match vulnerabilities to real assets.

### 02

### Prioritize

Apply OT-corrected scoring and “Now, Next, Never” to find the 3 to 6 percent that matter.

### 03

### Mitigate

Patch where possible, apply compensating controls where it is not, and document the decision.

© 2026 Dragos, Inc. All Rights Reserved.

## About Dragos

Dragos is the world's leading OT cybersecurity firm headquartered in Hanover MD, USA area with offices around the world. It provides the most effective OT cybersecurity technology for industrial and critical infrastructure to deliver on our global mission: safeguarding civilization. The Dragos Platform provides visibility and monitoring of OT environments for asset identification, vulnerability management, and threat detection with continuous insights generated by the industry's most experienced OT threat intelligence and services team. Dragos protects customers across the range of operational sectors, including electric, oil & gas, data centers, manufacturing, water, transportation, mining, and government.

Learn more: dragos.com

© 2026 Dragos, Inc. All Rights Reserved.