

Vulnerability Management: Three Days To Decide

Making risk-based vulnerability management work in xOT environments. CISA has made it a federal mandate; private critical infrastructure will be measured against it next.



Executive Summary

Risk-Based Prioritization Is Now A Governance Obligation. Its Rules Were Written For IT.

In June 2026, CISA replaced the flat “it’s in the KEV, patch it in 14 days” model with Binding Operational Directive (BOD) 26-04, a graduated remediation framework built on four risk variables. Federal civilian agencies must be fully compliant by December 7, 2026.

The directive binds only federal civilian agencies. This paper is written for everyone else: the electric utilities, water systems, pipeline operators, and manufacturers who will be asked by regulators, insurers, and boards how their programs map to it, whether it applies to them or not.

This paper examines the directive through the lens of Extended Operational Technology (xOT): the complete set of interconnected systems that influence physical operations, from PLCs and safety systems to engineering workstations, remote access gateways, and cloud-connected devices. The scope test is simple: if the system impacts the control loop, it is part of the operational environment. That test, not device category, is what the directive’s risk variables need to measure.

December 7 is the due date on the federal calendar. The model behind it is not going away. Risk-based prioritization, mitigation as a first-class alternative to patching, and compromise assessment as part of remediation are the direction towards which every framework is moving. The deadline is the reason to read this now; the model is the reason it will still apply next year.

BOTTOM LINE UP FRONT

BOD 26-04 asks the right question: which vulnerabilities actually matter, and how fast do they need to be fixed? But its four inputs (public exposure, known exploitation, automatability, and technical impact) measure IT risk.

Applied unmodified across an xOT environment, they assign three-day urgency to assets that cannot be taken down in three days and bury the small set of vulnerabilities adversaries actually use against operations under everything that merely scored high. The three-day tier also assumes something most OT programs cannot do: determine within 72 hours whether the affected asset was already compromised.

Three Priorities for OT

01

Prioritization Needs OT Correction, Not OT Exception.

Only 3–6% of OT vulnerabilities require immediate action. A program that can identify which ones meets both the intent of 26-04 and the reality of a maintenance window that is months away.

02

“Remediate or Mitigate” is the Clause OT Teams Should Build Around.

The directive treats mitigation as compliant. Alternative mitigations, configuration changes, network controls, and detection signatures, are how OT programs close the gap when patching is not an option.

03

Forensic Triage is the Requirement that will Expose the Biggest Gap.

The average adversary dwell time in OT environments is 42 days. A program that cannot answer “were we already in the environment?” is not meeting the three-day tier, no matter how fast it patches.



Section 01

What Changed in June 2026

For nearly five years, federal vulnerability management ran on two directives.

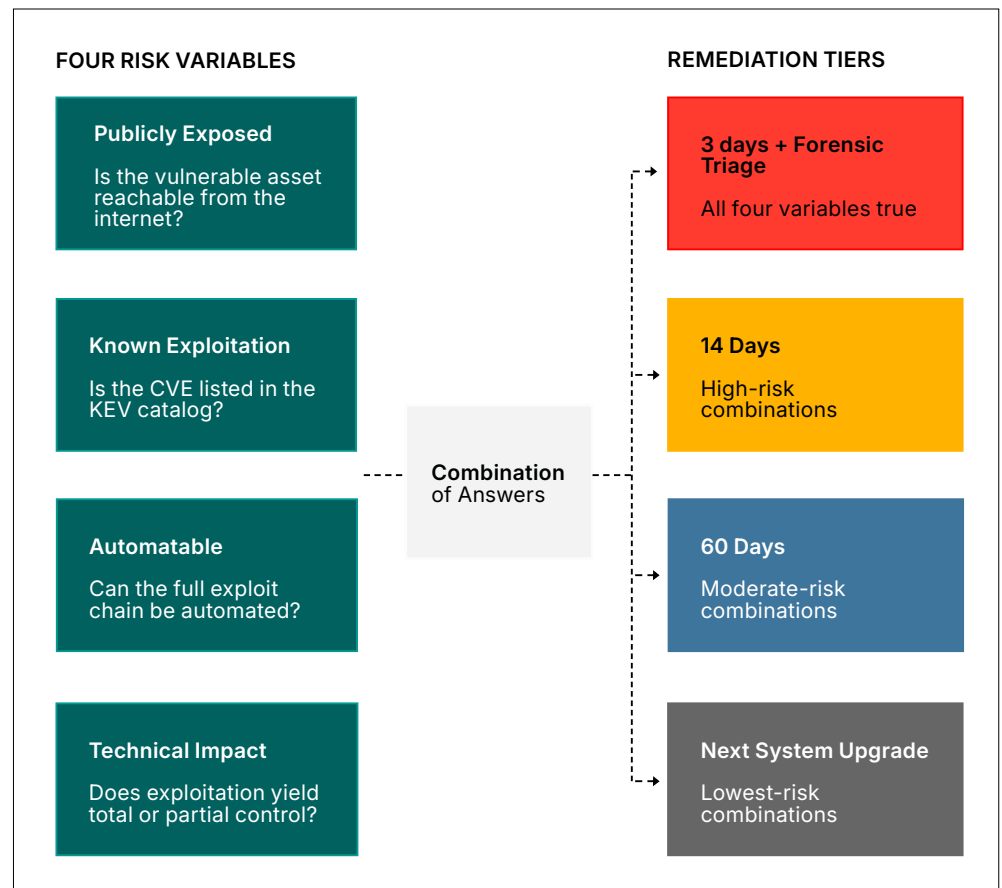
BOD 19 02 governed internet-accessible systems. BOD 22-01 established the Known Exploited Vulnerabilities catalog and set fixed remediation deadlines for anything listed in it. Both treated every listed vulnerability as roughly equal: if it appeared in the catalog, the clock started and the deadline was the same regardless of where the asset sat or what an attacker could do with it.

BOD 26-04, Prioritizing Security Updates Based on Risk, supersedes both. Issued June 10, 2026, it replaces flat deadlines with a decision model. For each vulnerability on each asset, the agency evaluates four binary questions and the combination of answers determines the remediation timeline.

FIGURE 1

The BOD 26-04 decision model. Four binary variables evaluated per vulnerability, per asset, determine which of four remediation tiers apply.

The top tier carries a mandatory forensic triage of the affected asset to determine whether it was compromised before the patch.



Simplified from CISA BOD 26-04 and its Implementation Guidance.

Three Features of the Directive Matter the Most for Organizations Securing xOT Environments



The Top Tier is Three Calendar Days

A vulnerability that is internet-exposed, in the KEV catalog, automatable, and capable of granting total control must be remediated or mitigated within 72 hours. That is a workflow requirement, not a policy update.



The Top Tier Requires Forensic Triage

Remediation alone does not satisfy it. The agency must also assess whether the asset was already compromised, following CISA's triage guidance: scope the incident, preserve volatile evidence before altering the system, establish out-of-band communications, and document the escalation decision.



Mitigation Counts

The directive consistently says "remediate or mitigate." Where a patch is unavailable or cannot be applied, a compensating control that removes the risk within the timeline is compliant.

Why a Federal Directive Matters to a Private Utility

BOD 26-04 is binding only on Federal Civilian Executive Branch agencies. CISA explicitly encourages state, local, and private-sector critical infrastructure to adopt the same model, and there is precedent for what happens next. BOD 22-01's KEV catalog was also a federal-only instrument. Within roughly eighteen months it had become the reference standard for commercial vulnerability programs, cyber insurance underwriting, and audit frameworks. Organizations that never fell under the directive were asked by regulators, insurers, and customers how their programs mapped to it.

The same trajectory should be assumed here. FedRAMP has already aligned its Vulnerability Detection and Response rules to 26-04's timelines. Sector regulators, insurers, and boards will follow. The practical question for an OT security leader is not whether 26-04 applies, but how it maps to their infrastructure.



Section 02

The Four Variables Do Not Translate Cleanly to OT

Each of the directive’s four risk variables is a reasonable proxy for risk on an enterprise asset. Applied to an asset that influences a physical process, each one breaks in a different way: some measure the wrong thing, and one measures something that barely applies. In an xOT environment, that includes systems the directive would never classify as control systems, from the remote access gateway to the engineering workstation.

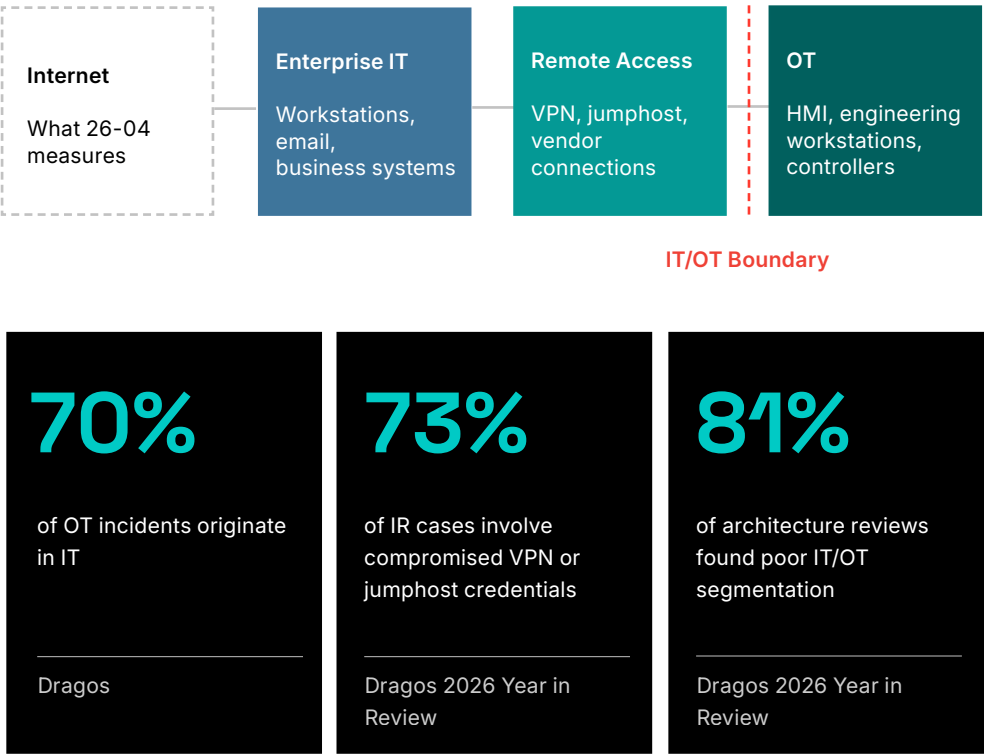
Publicly Exposed

The directive treats internet reachability as the exposure variable. In an xOT environment, that is the wrong perspective to take. Control systems are rarely internet-facing. They are reached through the IT network, through remote access infrastructure, and through the segmentation boundary that is supposed to separate the two. The remote access gateway and the engineering workstation are xOT devices in their own right: neither controls a process, but both can influence the control loop, and both are ways adversaries can actually penetrate systems.

Dragos incident response and architecture review data describes where OT exposure actually lives. Seventy percent of OT incidents originate in IT. Seventy-three percent of Dragos IR cases involve compromised VPN or jumphost credentials. And 81% of Dragos architecture reviews found poor IT/OT segmentation. A scan for internet-exposed assets would rate most of those environments low-exposure. The adversaries in them did not agree.

FIGURE 2
Where OT exposure actually lives. The directive’s exposure variable measures the dashed path on the left.

Dragos incident data points to the solid path: enterprise IT compromise, remote access credentials, and a segmentation boundary that does not hold.



Known Exploitation

The KEV catalog is a confirmation mechanism. A vulnerability is added after CISA has evidence it is being exploited. For enterprise software with millions of installs, that lag is short. For OT, it is structurally longer: exploitation is lower-volume, harder to observe, and often visible only to the asset owner or their incident responders.

Adversaries targeting OT do not wait for the catalog. In July 2026, U.S. authorities warned that Iranian-affiliated actors were targeting ICS devices from the three largest control-system vendors. The threat groups Dragos currently tracks, 26 and counting, are characterized by their behaviors and target sets, not by which CVEs have been catalogued. Prioritization tied to adversary behavior moves earlier than prioritization tied to a catalog entry.

Automatable

Automatability asks whether an adversary can chain exploitation end to end without a human. It is a strong predictor of mass-exploitation risk in IT. In OT it can be actively misleading. Exploitation of a Purdue Level 1 or Level 2 device is typically manual, process-specific, and requires engineering knowledge of the target.

An adversary who has reached a controller is not looking to automate; they are looking to understand the process. Scoring that de-prioritizes non-automatable vulnerabilities systematically under-weights the ones that matter most in an industrial environment.

Technical Impact

The directive's highest impact state is "total control" of the asset. Total control of a corporate workstation and total control of a safety instrumented system are not in the same tier of risk and should not receive the same score. This is where the xOT scope test applies. Impact is operational and physical: what process does the asset influence, what happens if it is manipulated or stopped, and what compensating controls sit between the vulnerability and the control loop.

Only 3–6% of OT vulnerabilities require immediate action. The question 26-04 raises for OT is not whether to prioritize. It is whether your program can identify which 3–6%.

Section 03

What OT-Corrected Prioritization Looks Like in Practice

The answer is not to exempt xOT environments from BOD 26-04. It is to feed the directive’s decision model the inputs it was missing. Dragos frames OT vulnerability prioritization as “Now, Next, Never.” The framework maps directly to the directive’s intent, and once the four variables are corrected for OT context, it maps to the directive’s tiers as well.

FIGURE 3

“Now, Next, Never” aligned to BOD 26-04 tiers. The left column shows the directive’s four variables restated for the xOT environment: exposure as actual network reachability, exploitation as tracked adversary behavior, impact as influence over the control loop, and compensating controls as an explicit input rather than an afterthought.

xOT-CORRECTED INPUT	PRIORITY	BOD 26-04 TIER
- Reachable via actual network path - Exploited by a tracked threat group - Direct influence on the control loop - No effective compensating control	NOW 3–6% of OT vulnerabilities	3 Days + Forensic Triage Patch, or mitigate if patching is not operationally viable
- Reachable, but through a monitored boundary - Exploit exists; no observed OT targeting - Indirect influence on operations - Compensating control partially effective	NEXT Schedule for the next window	14 or 60 Days Apply mitigation now; patch at the next maintenance window
- Not reachable from any adversary position - No known exploit; theoretical only - No operational impact if exploited - Or: CVSS score inflated for OT context	NEVER Track, do not act	Next System Upgrade Document the decision; revisit if threat or exposure changes



The Correction, Variable by Variable

26-04 VARIABLE	IT READING	XOT-CORRECTED READING
Publicly Exposed	Internet-reachable	Reachable from a position an adversary has demonstrated they can gain: enterprise IT, remote access, a vendor connection, or a flat segment
Known Exploitation	Listed in KEV	Listed in KEV, or associated with the tradecraft of a tracked threat group active against this sector or vendor
Automatable	Full chain scriptable	Weighted down for Level 1–2 devices where manual, process-specific exploitation is the realistic threat model
Technical Impact	Total or partial control of the asset	Influence over the control loop: safety, availability, and physical consequence of manipulation or loss of view
(Not In 26-04)	—	Compensating controls in place, and whether they are validated rather than assumed

A Worked Example

Consider a remote code execution vulnerability in an engineering workstation application. Its published CVSS score is 9.8. Under an uncorrected reading of 26-04, it is high-impact, likely automatable, and, if the workstation has any internet path, top-tier: three days, plus triage.

xOT-corrected scoring asks different questions. Is the workstation reachable from enterprise IT or a remote access path? In the example environment, yes, through a jump host with shared credentials. Is the vulnerability associated with tracked adversary activity against this sector? Yes. Does the workstation have write access to controllers? Yes. Are there compensating controls? Application allow-listing is deployed but has not been validated against this exploit path. Result: Now. The correction confirmed the priority and identified the mitigation that can be applied today (jump host credential rotation and MFA, validated allow-listing) while the patch waits for a window.

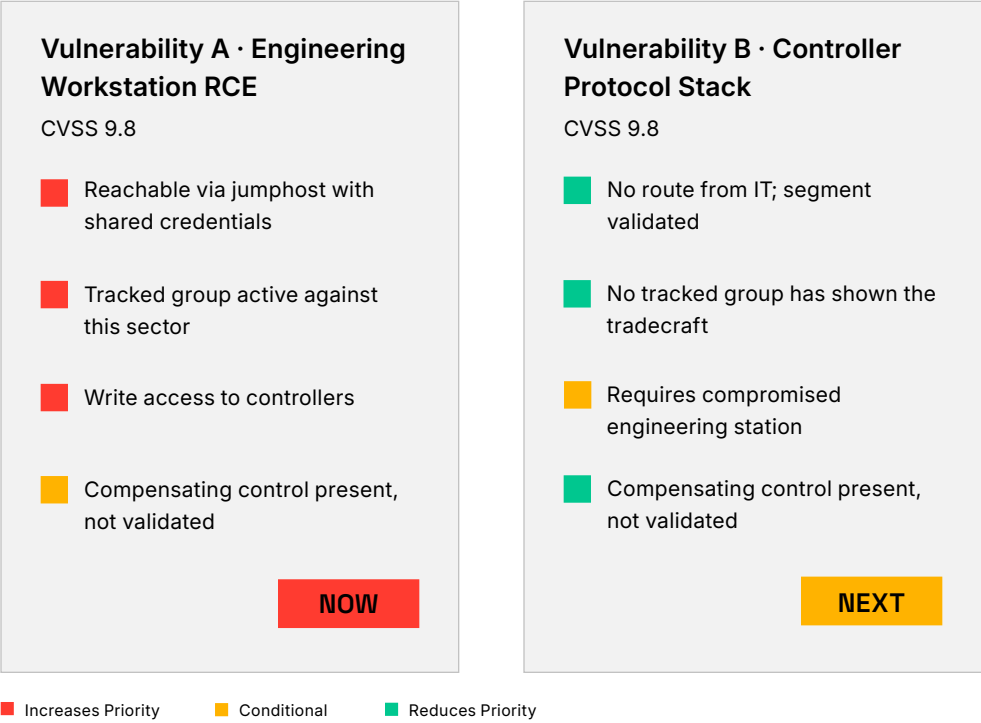
Now consider a second vulnerability with the same CVSS score, in a protocol stack on a controller. Uncorrected, it scores identically. Corrected: the controller sits in a validated segment with no route from IT, the vulnerability requires physical proximity or a compromised engineering station, and no tracked group has demonstrated the tradecraft. Result: Next. Schedule for the outage; monitor the segment boundary for changes that would reopen the question.

FIGURE 4

Two vulnerabilities, same CVSS score, and two different answers.

Without xOT context, both land in the three-day tier and one of them consumes an outage that was not necessary.

Same CVEs Score, Different Priority



Section 04

When The Answer is Not a Patch

The directive says “remediate or mitigate” throughout. Most OT programs read that as patch-or-wait. That reading is the single biggest source of unnecessary risk acceptance in xOT vulnerability management.

In OT, patching is frequently not an option within any timeline the directive contemplates. The vendor has not released a fix. The fix requires a firmware version the integrator has not certified. The asset can only be touched during an outage that is scheduled for spring. The system is end-of-life and will never be patched. None of those conditions reduces the risk. All of them are routinely used to move a vulnerability from the action list to the accepted-risk register.

26-04 gives xOT programs a compliant alternative and, more importantly, an expectation: when you cannot patch, mitigate within the same timeline. For OT, mitigation takes three forms.



Configuration Changes

Disable the vulnerable service, protocol, or interface where the process does not require it. Restrict the asset's communication to the specific peers it needs. Enforce authentication where the protocol supports it. These changes are typically reversible, low-risk, and achievable without an outage.

Network Controls

Block the vulnerable port or protocol at the segment boundary. Restrict the source addresses that can reach the asset. Where segmentation is weak, which Dragos architecture reviews find in the majority of cases, a targeted firewall rule around a single high-priority asset is a faster and more defensible mitigation than a full re-architecture.

Detection Signatures

Where neither of the above is possible, monitor for exploitation. A detection tied to the specific vulnerability and the adversary behaviors associated with it converts an unpatched vulnerability from an unknown into a watched risk. For the directive's purposes, it also produces the evidence trail a forensic triage will need.

The prerequisite for all three is knowing what adversaries are actually doing with the vulnerability. Mitigation guidance built on the tradecraft of tracked threat groups targets the exploitation path that is realistic for the sector and the vendor, rather than every path that is theoretically possible. That is how a mitigation earns the same standing as a patch under the directive, and how a program demonstrates risk reduction to an auditor or a board rather than a list of exceptions.

26+

OT threat groups tracked
by name

Dragos 2026 Year in
Review

119

ransomware groups
targeted industrial
organizations in 2025, up
from 80 in 2024

Dragos 2026 Year in
Review

42

days: average adversary
dwell time in OT
environments

Dragos 2026 Year in
Review

Section 05

Forensic Triage:
The Requirement Most xOT Programs Cannot Meet

The directive’s three-day tier does not only ask you to fix the vulnerability. It asks you to determine, in the same window, whether the adversary already used it.

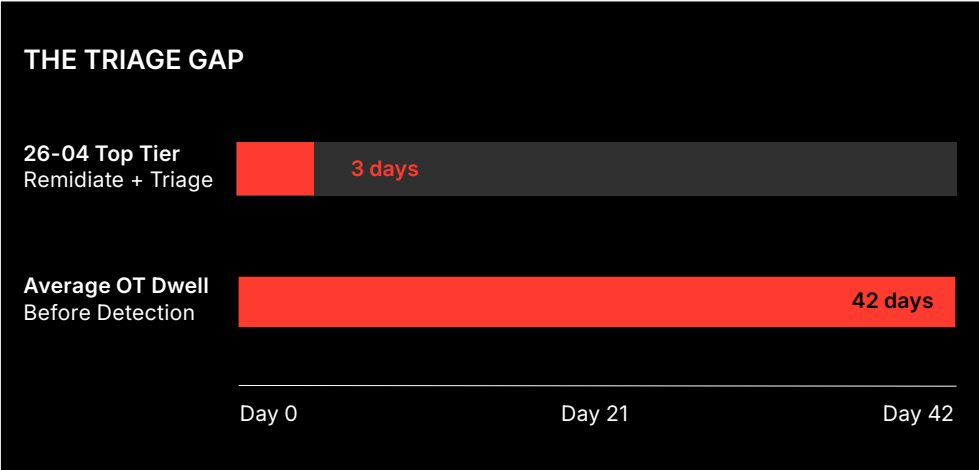
This is the part of BOD 26-04 that most vulnerability management programs are least prepared for, and the part that matters most in xOT. The logic is sound: if a vulnerability is internet-exposed, known-exploited, automatable, and grants total control, the honest assumption is that someone has already tried it. Patching it closes the door. Triage checks whether anyone is inside.

Set that against the Dragos 2026 Year in Review finding that adversaries dwell in OT environments for an average of 42 days before detection. Fourteen times the length of the directive’s remediation window.

FIGURE 5

The directive gives three days to remediate and confirm no prior compromise. Adversaries in OT environments have, on average, been present for 42 days before anyone notices.

The triage requirement is where 26-04 stops being a patching problem and becomes an incident response problem.



What Adequate Triage Looks Like In OT

CISA’s implementation guidance describes the shape of an adequate triage: scope the affected boundary, systems, and services; establish an out-of-band communication channel; capture volatile data before altering the system; collect non-volatile evidence within scope; analyze; and document the escalation decision. Every one of those steps has an OT complication.

Scoping requires an asset inventory the team trusts. Volatile data capture on a controller or an HMI is not a standard endpoint operation and may not be safe to perform during production. Evidence preservation conflicts with the operator’s instinct to restore the process immediately. And “analyze” assumes someone on the team can read industrial protocol traffic and recognize what normal looks like on this network. IT incident response playbooks reliably stall at the OT boundary on exactly these points.



Four Capabilities The Three-Day Tier Assumes

An xOT program that intends to meet the directive's top tier, or to be measured against it, needs four things in place before the clock starts.



A Baseline

Triage means comparing current state against a known-clean state. A compromise assessment performed before the three-day event is what makes the comparison possible. Without it, the triage question is unanswerable.



OT Incident Responders On Call

Three days is not enough time to source and onboard a team that understands industrial protocols and control-system forensics. A retainer that puts OT-specific responders on the clock is the only realistic way to meet the window.



A Tested Process

The directive requires documented escalation decisions. A tabletop exercise built around a three-day-tier vulnerability on a real asset class reveals, in advance, where the process stalls: who authorizes evidence capture on a production system, who decides between restore and preserve, who briefs the regulator.



Continuous Visibility

Detection and monitoring between events is what turns a 42-day dwell time into a shorter one, and what gives a triage team the historical traffic they need to answer, "when did this start?" A managed OT monitoring capability extends that visibility to teams that do not have round-the-clock OT analysts.



Section 06

Sector Implications

The directive lands differently across the CISA 16. Four sectors illustrate the range.



Electric

NERC CIP already requires vulnerability assessment and patch management with defined timelines for BES Cyber Systems. BOD 26-04 goes further in two respects: its risk model is per-vulnerability, per-asset rather than per-system category, and it adds forensic triage. Expect auditors to ask how the CIP program handles both.



Oil and Gas

TSA security directives for pipelines already push toward risk-based programs and reporting. BOD 26-04 supplies a specific model that regulators can point to. Operators with remote and unmanned sites should focus on the exposure variable: remote access is the realistic path, and the directive’s internet-facing definition understates it.



Water and Wastewater

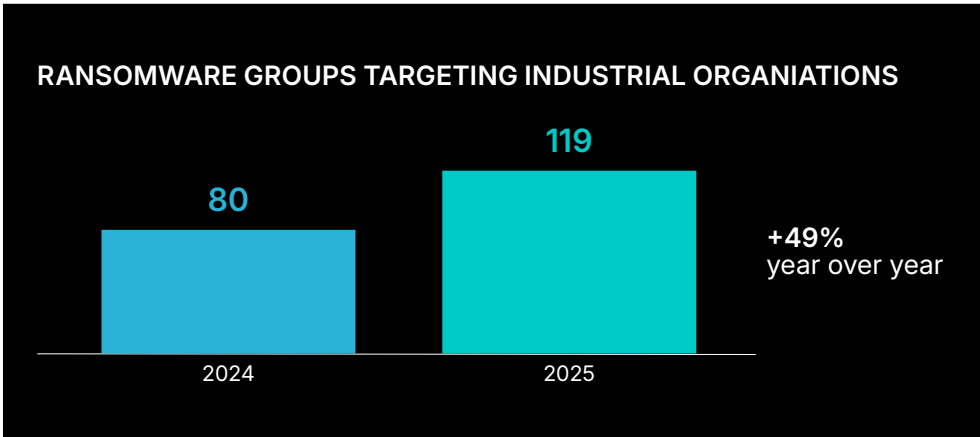
Resource-constrained utilities have the most to gain from the 3–6% principle. A program that identifies the small set of vulnerabilities that matter is achievable with a small team; a program that tries to patch everything is not. Mitigation over patching is the realistic path.



Manufacturing

No federal mandate applies today. The pressure will arrive through customers, insurers, and supply-chain requirements that import the standard. With 119 ransomware groups targeting industrial organizations in 2025, manufacturers are also the most likely to face the three-day scenario without a regulator having asked them to prepare for it.

FIGURE 6
The number of ransomware groups targeting industrial organizations grew nearly 50% in a single year.



Source: Dragos 2026 OT Cybersecurity Year in Review.



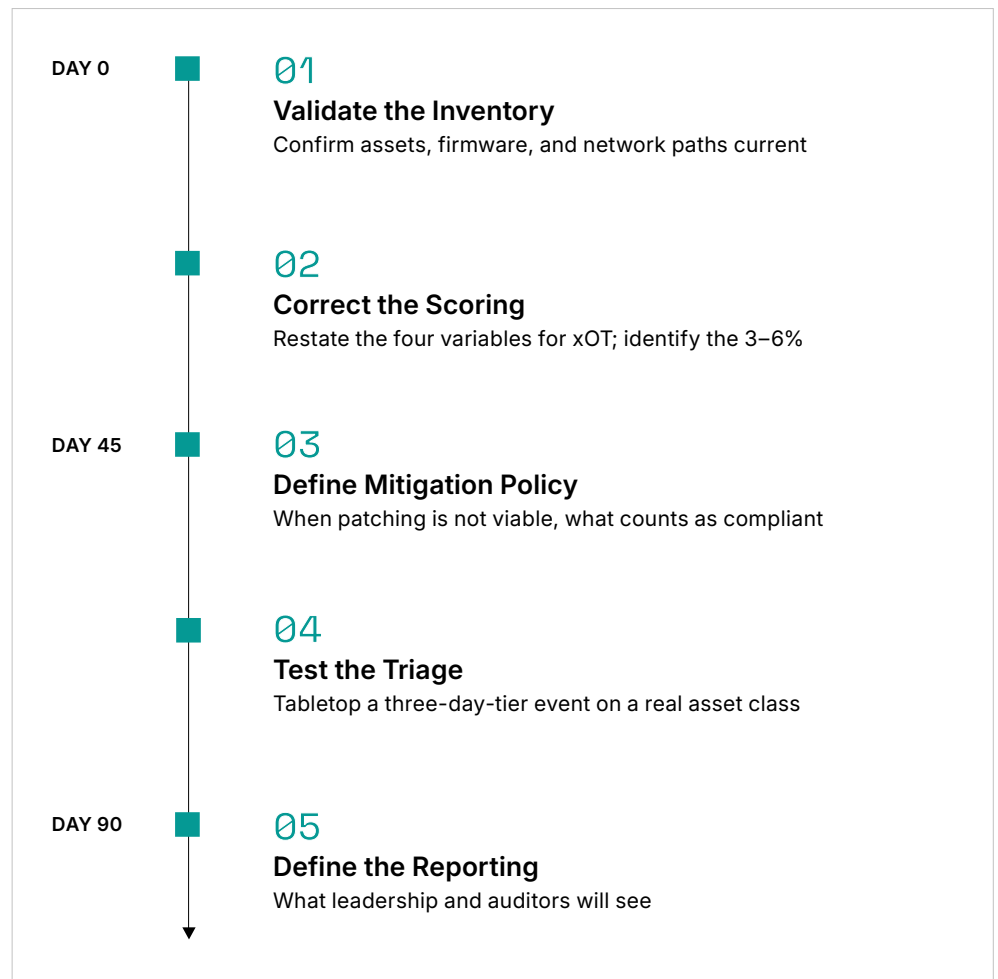
Section 07

A Readiness Path

The federal compliance date of December 7, 2026 is the first checkpoint, not the finish line. The five steps below take roughly 90 days for most organizations, and they are applicable whether the pressure arrives from CISA, a sector regulator, an insurer, or a board. The order matters more than the calendar.

FIGURE 7

A five-step readiness path, roughly 90 days for most organizations. Steps one and two are prerequisites for everything that follows; a program cannot prioritize what it has not inventoried.



Source: Dragos 2026 OT Cybersecurity Year in Review.

First Checkpoint: December 7, 2026

Federal compliance date for BOD 26-04. After that, the same five steps are what any regulator, insurer, or board will ask about.



Validate The Asset Inventory

Prioritization is per-asset. If the inventory is a spreadsheet last touched during commissioning, the four variables cannot be evaluated. Confirm firmware versions, network placement, and communication paths against observed traffic, not documentation.



Establish OT-Corrected Scoring

Restate exposure, exploitation, automatability, and impact on the environment. Identify the current "Now" list. If it is more than 3–6% of the total, the scoring is not corrected enough; if it is zero, the exposure variable is probably being read as internet-facing.



Write The Mitigation Policy

Define in advance what compensating controls are acceptable substitutes for a patch at each tier, who approves them, and how they are validated. This is the document that turns an accepted risk register back into an action list.



Test Forensic Triage Against a Real Asset

Run a tabletop on a three-day-tier vulnerability affecting an engineering workstation or HMI. Identify who authorizes evidence capture on a production system, what tooling is safe to use, and how long it actually takes. Then decide whether the team can do it alone.



Define The Reporting

BOD 26-04 makes prioritization a governance issue. Decide now what the board, the regulator, and the auditor will see: how many vulnerabilities in each tier, how many remediated versus mitigated, and how many triage events were completed within the window.

\$31.1B

annual global OT cyber risk

Marsh McLennan, 2025

\$500K

per hour, cost of unplanned downtime (up to)

ABB, 2025

31%

of breached organizations experienced operational disruption

IBM Cost of a Data Breach, 2025

Closing

Compliance and Risk Reduction are the Same Goal. xOT Context is the Difference.

BOD 26-04 is the most significant change to how vulnerability management is measured in half a decade, and it points in the right direction. It replaces severity scores with risk decisions. It treats mitigation as legitimate. It insists that a program which patches without checking for prior compromise has only done half the job. Every one of those principles is one the OT security community has argued for since long before the directive existed.

What the directive does not do is account for the asset. Its four variables were built for a world where exposure means the internet, impact means the machine, and exploitation is confirmed by a catalog. In an xOT environment, exposure means the path through IT and remote access, impact means influence over the control loop, and the adversaries who matter are known by their behavior before they are known by a CVE.

A program that adopts BOD 26-04 unmodified will comply and still be surprised. A program that feeds the directive's model the context it was missing, actual reachability, tracked adversary tradecraft, influence over the control loop, and validated compensating controls, will identify the 3–6% that matter, mitigate what it cannot patch, and be able to answer the triage question when the clock is running.

That is the difference between meeting the directive and meeting its intent. It is also the difference between a program that reports compliance and one that can demonstrate risk reduction, which is what the board, the regulator, and the operator on shift actually need.

How Dragos Helps

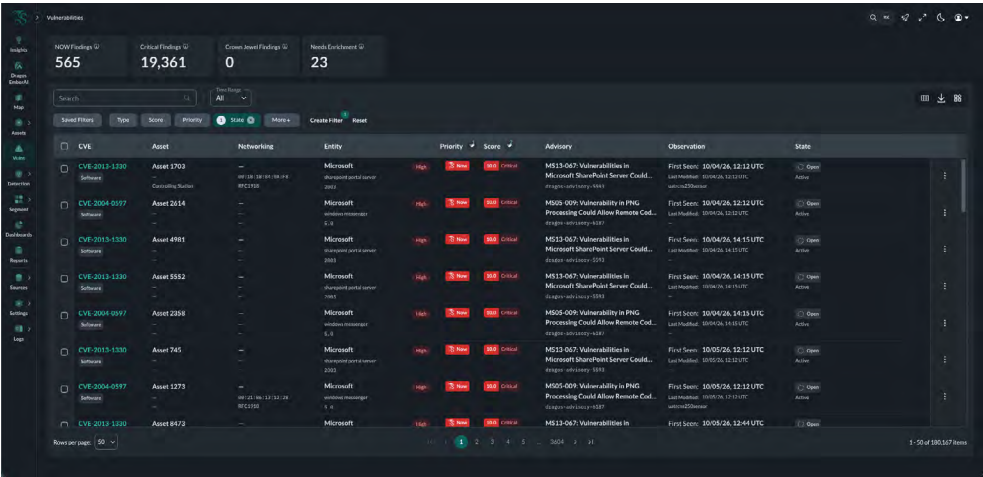
Vulnerability Management in the Dragos Platform

Most OT vulnerability programs are overwhelmed by volume and paralyzed by irrelevance. The Dragos Platform cuts through the noise with OT-specific context and “Now, Next, Never” prioritization.

Every correction this paper argues for is already how the Dragos Platform works. It was not built in response to a directive. It was built because CVSS scoring was designed for IT and overstates risk in OT context, and because teams without OT-specific enrichment either chase every advisory or ignore them all.

The Dragos Platform is purpose-built for OT, delivers visibility across the xOT environment, and applies the Dragos Intelligence Fabric so that vulnerability decisions reflect what adversaries are actually doing.





CVE	Asset	Networking	Entity	Priority	Score	Advisory	Observation	State
CVE-2013-1330	Asset 1703	—	Microsoft	High	9.8	MS13-047: Vulnerabilities in Microsoft SharePoint Server Could...	First Seen: 10/04/26, 12:12 UTC	Open
CVE-2004-0897	Asset 2614	—	Microsoft	High	9.8	MS04-009: Vulnerability in PNG Processing Could Allow Remote Cod...	First Seen: 10/04/26, 12:12 UTC	Open
CVE-2013-1330	Asset 4981	—	Microsoft	High	9.8	MS13-047: Vulnerabilities in Microsoft SharePoint Server Could...	First Seen: 10/04/26, 14:15 UTC	Open
CVE-2013-1330	Asset 5552	—	Microsoft	High	9.8	MS13-047: Vulnerabilities in Microsoft SharePoint Server Could...	First Seen: 10/04/26, 14:15 UTC	Open
CVE-2004-0897	Asset 2204	—	Microsoft	High	9.8	MS04-009: Vulnerability in PNG Processing Could Allow Remote Cod...	First Seen: 10/04/26, 14:15 UTC	Open
CVE-2013-1330	Asset 745	—	Microsoft	High	9.8	MS13-047: Vulnerabilities in Microsoft SharePoint Server Could...	First Seen: 10/05/26, 12:12 UTC	Open
CVE-2004-0897	Asset 1273	—	Microsoft	High	9.8	MS04-009: Vulnerability in PNG Processing Could Allow Remote Cod...	First Seen: 10/05/26, 12:12 UTC	Open
CVE-2013-1330	Asset 8573	—	Microsoft	High	9.8	MS13-047: Vulnerabilities in Microsoft SharePoint Server Could...	First Seen: 10/05/26, 12:44 UTC	Open



OT-Corrected Scoring

Dragos analysts review and correct CVSS scores for OT context, evaluating exploitability, exposure, and operational impact. This is the corrected input the directive's four variables need.



"Now, Next, Never" Prioritization

Only 3–6% of OT vulnerabilities require immediate action. The framework identifies exactly which ones, so the backlog becomes a prioritized, manageable action list rather than a register of exceptions.



Alternative Mitigations

When patching is not operationally viable, Dragos provides OT-specific compensating controls: configuration changes, network controls, and detection signatures. This is the "remediate or mitigate" clause, made practical.



Exploit and Threat Context

Tied to active threat intelligence, flagging what adversaries are actually exploiting. Prioritization moves when a tracked group's behavior changes, not when a catalog updates.

The Foundation Underneath

Prioritization is only as good as the inventory it runs on. The Dragos Platform builds and continuously updates asset inventory through passive monitoring across 600+ industrial protocols, Active Collection for firmware and patch-level detail in segmented or legacy environments, and Data Import from engineering and control systems. When a CVE drops, defenders know every affected device in minutes, not days. Segmentation validation maps real network topology against intended zones, which is how the exposure variable gets an honest answer.

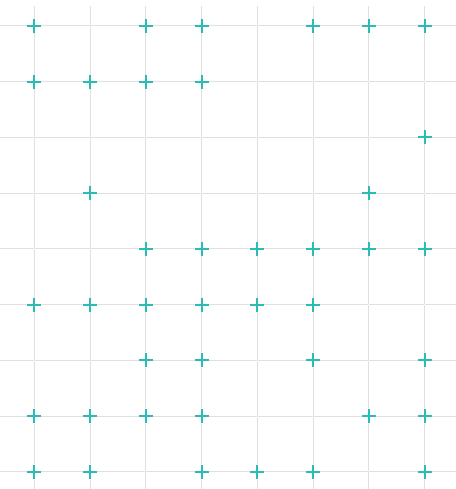


When the Clock is Running

The directive's three-day tier is an incident response requirement as much as a patching one, and the Dragos Platform is where the evidence lives. Case management pulls activity logs, forensic data, and timeline views into a single investigation.

Response Playbooks authored by Dragos OT experts guide the triage. For teams that need expertise on the clock, Dragos services close the gap:

- **OT Cybersecurity Assessment.** Four assessment options ranging from Compromise Assessment to the full OT Cybersecurity Assessment, establishing the baseline that makes forensic triage answerable.
- **Rapid Response Retainer.** 24/7 access to OT cybersecurity experts. For organizations running the Dragos Platform, SLA-backed response begins with first contact within one hour and analysis underway within four. Unused hours can be applied to architecture reviews, penetration testing, and tabletop exercises.
- **OT Watch and OT Watch Complete.** Expert-led threat hunting behind the Platform, or full 24/7 managed monitoring, alert triage, vulnerability management, and hardening recommendations for organizations that want a mature OT security program without building one in-house.
- **Dragos xOT Threat Intelligence.** Vulnerability research tested on physical devices, enriched with corrected CVSS scores, OT impact assessments, and alternative mitigations. IT-focused risk scoring is wrong 30% of the time for OT. xOT Threat Intelligence fixes that.



FIND YOUR 3–6%

See how the Dragos Platform applies OT-corrected scoring and “Now, Next, Never” prioritization to your environment, and what your current backlog looks like once the noise is removed.

TALK TO AN OT SECURITY EXPERT

dragos.com/request-a-demo

Sources

Cybersecurity and Infrastructure Security Agency. Binding Operational Directive 26-04: Prioritizing Security Updates Based on Risk.	2026
Cybersecurity and Infrastructure Security Agency. BOD 26-04 Implementation Guidance: Forensic Triage Requirements.	2026
Dragos, Inc. 2026 OT Cybersecurity Year in Review.	2026
Dragos, Inc. Dragos External Pitch Deck 2026 and approved corporate statistics.	2026
U.S. government advisory on Iranian-affiliated targeting of ICS devices.	2026
FedRAMP. Response to CISA BOD 26-04.	2026
Marsh McLennan and Dragos. OT Cyber Risk Modeling.	2025
IBM. Cost of a Data Breach Report.	2025
ABB. Value of Reliability survey.	2025

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

