DRAGOS

Whitepaper

Understanding The Challenges of OT Vulnerability Management and How To Tackle Them

info@dragos.com
@DragosInc

TABLE OF CONTENTS

I. INTRODUCTION

As cybersecurity leaders improve the maturity of their vulnerability management programs, operational technology (OT) environments consistently stand out as the most challenging to bring into the fold. Many organizations, with the possible exception of those who follow North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards, aren't fully equipped with a detailed inventory of OT assets, let alone actively managing the vulnerabilities and risks existing within all of them.

In fact, according to a recent study from SANS Institute, while more than 91% of organizations include on-premises information technology (IT) infrastructure assets in their existing or planned vulnerability program, just 23% do the same for their OT assets.[1]

Organizations struggle to manage vulnerabilities within OT environments because the process is so different than for IT, requiring unique tools and philosophies to carry out compared to traditional IT vulnerability management.

And yet, according to the Cybersecurity and Infrastructure Security Agency (CISA)[2] and others, as threats increasingly target OT assets, the need grows by the day for effective mitigation of vulnerabilities that attackers can exploit. Organizations must come into balance with proven, documented OT vulnerability management practices to not only protect themselves from these threats but also come into compliance with a growing base of regulations meant to address them.

II. WHY OT VULNERABILITY MANAGEMENT IS DIFFERENT

The lag by enterprises in bringing the maturity of OT vulnerability management in line with IT vulnerability management is less a testament to any innate failing or weakness than it is to the unique challenges of finding and remediating flaws within OT environments.

Sure, many OT systems deal with the same types of technology and flaws that IT systems do. You'll find significant crossover, with many OT assets such as industrial control systems (ICS) relying on similar operating systems, network connections, and architectures as their IT counterparts.

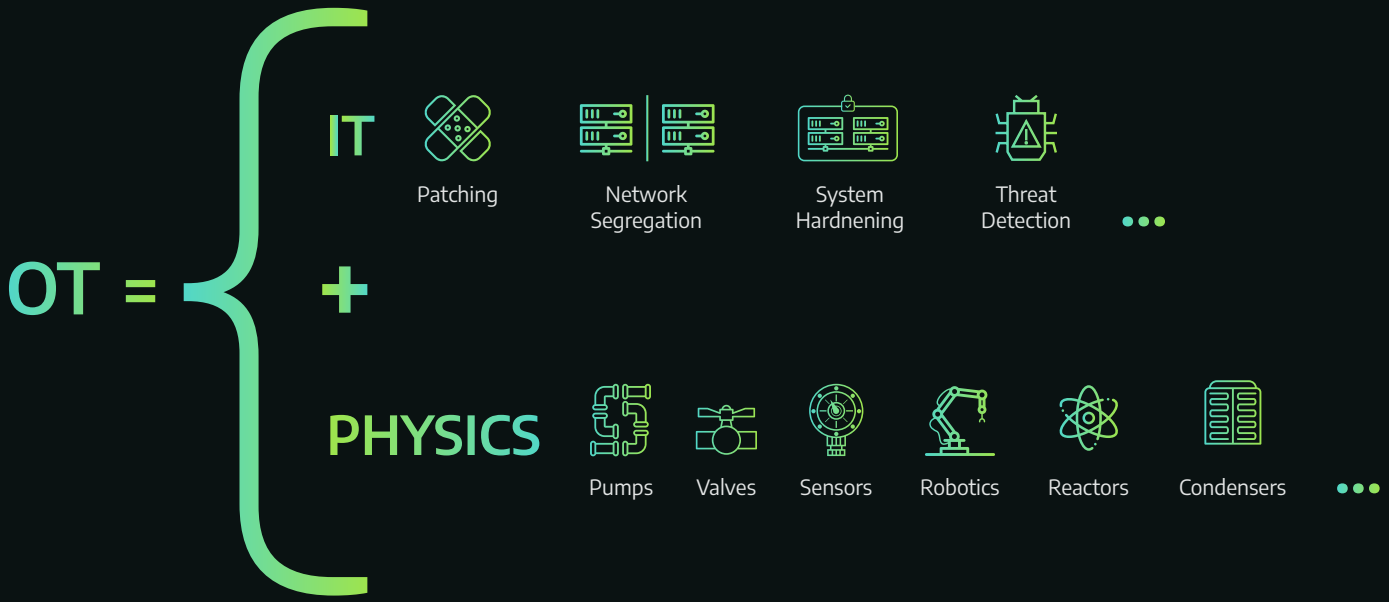
However, ICS/OT working environments are very different than IT, as are the potential cyber risks and the impact from them. Layered on top of that are additional protocols unique to OT, complicated vendor support agreements that impact how and when systems can be patched, and stringent regulatory and operational requirements that are often existential to business sustainability.

1 SANS Vulnerability Management Survey 2020 https://www.sans.org/reading-room/whitepapers/analyst/vulnerability-management-survey-2020-39930
2 Ransomware Threat to OT, CISA https://www.cisa.gov/publication/ransomware-threat-to-ot

> “The most angst that I have had in my career working in OT environments was around vulnerability management, because when a new vulnerability hit, senior leadership knew about it. It always bubbled up quick. And then it was always like, ‘what are you going to do about it?’ So, there would be this massive panic to go out, identify if we had the affected systems, and then report back with daily and weekly reports to show our status. And then we’d have to say, ‘by the way, we really can’t do anything about it’.”

Mike Hoffman

Principal Industrial Consultant
Threat Operations Center – Dragos



The following list enumerates important factors that explain why vulnerability management is so different for OT compared to IT:

Biggest risks exist in different places:
The highest risks posed by OT vulnerabilities tend to be the ones that threaten the integrity of systems rather than the confidentiality of the data they deal in. While IT is often consumed by privacy and data breach concerns, the thing that keeps OT operators up at night are problems like loss of view or loss of control in ICS systems that could translate into disruption or malfunction of physical machinery and possibly threaten the business or even people's safety. So, the exact same vulnerability in an IT system may not matter as much in an OT system if it doesn't threaten how it operates.

Downtime tolerance is slim to none:
Industrial operations have incredibly low tolerance for downtime in their OT systems compared to the leeway that the rest of the business can give IT systems. One of the biggest worries operators have is that the vulnerability management cure will be worse than the disease of letting a flaw exist within a system. This complicates the risk calculus for OT vulnerabilities. It also increases the urgency that an organization might feel when it comes to addressing any aspect of OT vulnerability management.

Active scanning is frequently problematic:
Not only do operators have to worry about the impact to uptime that vulnerability mitigations could have on OT systems, but they also must consider the risk that just looking for a vulnerability could have on a particularly critical OT asset. In many instances, IT-style active scanning for vulnerabilities is unsuitable for critical ICS assets. The interrogation and probing attempts active scanning makes could cause inadvertent disruption to industrial processes that could have huge operational or compliance ramifications.

Vendors hold a lot of control:
Often simply applying a Windows update is not so simple when the operating system is running a vendor's proprietary OT software and hardware. Vendors often design support contracts to have patching duties intermediated out to their cybersecurity or maintenance service teams, to be performed by this third-party on a pre-determined frequency. In many instances organizations may be contractually obligated to get approval from their OT vendors to make changes or patch systems on their own, risking voiding a contract without pre-approval.

Exceedingly long patch cycles:
For many OT and ICS systems, there's no such thing as weekly or monthly maintenance windows where administrators can easily sneak in a software patch. In fact, some systems may need to run continuously with regularly scheduled maintenance downtime spaced five or more years apart. This means that even when patches or updates are available, OT vulnerabilities frequently need to be mitigated with compensating controls instead.

Legacy systems are entrenched:
Most OT systems are necessarily tied to very expensive equipment, the lifecycles of which can span decades. Ripping and replacing systems to get them up to date is never an option the way it can be for IT systems. And often even when a system is new, it must be put into service with a less secure configuration to support backward compatibility with other interconnected OT legacy systems or vendor infrastructure. All of these unpatchable legacy systems require an organization to turn to creative and meticulous mitigations to harden them from attack.

Unique, fit-for-purpose hardware and software:
While there is a considerable amount of crossover with IT, OT environments also include a wide array of assets that depend upon arcane protocols and specialized software that IT administrators may have never even heard of, let alone have experience with. Additionally, the configuration of these systems is often unique to every organization. This means that mitigating flaws in these setups demands very close collaboration with the asset owners who know them best.

Everything is highly manual:
The remediation and mitigation of many OT vulnerabilities is by necessity a highly manual affair, compared to IT systems that can frequently be patched through automatic updates. But even OT vulnerability management practices that can be automated tend to remain manual at most organizations. Many organizations update their asset inventories manually, compare that inventory to known vulnerabilities manually, and track their known issues manually in spreadsheets. All of this is error-prone, time consuming, and difficult to scale, especially as the rate of disclosure of OT vulnerabilities grows.

III. VULNERABILITY ASSESSMENT VS. VULNERABILITY MANAGEMENT

Many organizations have made inroads in recent years in regularly assessing for and identifying vulnerabilities in their OT environments. But the OT challenges highlighted above create a situation where many industrial organizations struggle to push beyond vulnerability assessment into full-cycle vulnerability management.

This is problematic because vulnerability assessment without vulnerability management leaves issues unfixed and untracked. It also opens regulated industries like electrical utilities and pipeline operators up to compliance headaches if flaws found during assessment aren't addressed within time frames mandated by the regulators.

To understand the difference between assessment and management of vulnerabilities, it might help to visualize the vulnerability management cycle, which can be broken down into four stages of activity.

VULNERABILITY MANAGEMENT GLOSSARY

ASSET MANAGEMENT
The process of deploying, tracking, maintaining, upgrading, and disposing of assets across their lifecycle. Vulnerability management is a subset of broader asset management activities.

VULNERABILITY ASSESSMENT
A point-in-time activity where an organization collects and presents the vulnerability state of a system or environment.

VULNERABILITY MANAGEMENT
A cyclical and continuous process of identifying, classifying, prioritizing, remediating, mitigating, and accepting risk of vulnerabilities, tracking the disposition of vulnerabilities throughout.

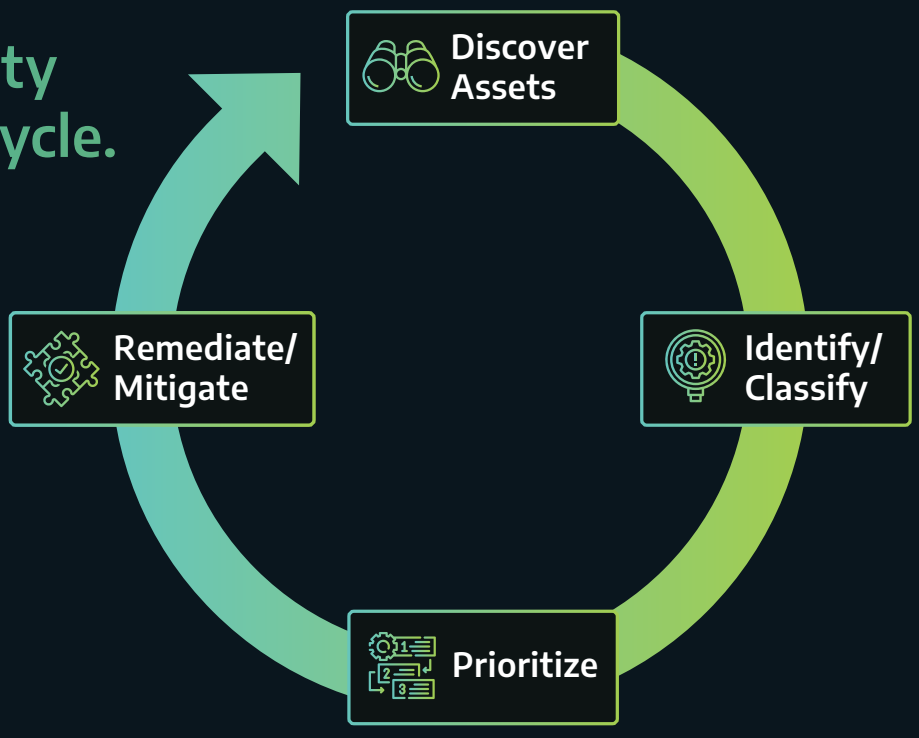
REMEDIATION
The process of fixing a vulnerability through patching, reconfiguring, or uninstallation/ decommissioning of equipment or software.

MITIGATION
The process of utilizing compensating controls like firewalls, network segmentation, or data diodes to minimize the risk of a vulnerability when it can't be eliminated through remediation.

RISK ACCEPTANCE
The process of consciously accepting the risk of a vulnerability when operational risk outweighs the vulnerability risk of a particular flaw.

Figure 1:

Four Stages Of The Vulnerability Management Cycle.



DISCOVER

The first stage of vulnerability management is discovery. In this stage, organizations meticulously find all their assets and build out a documented inventory they'll use to know what needs to be examined for vulnerabilities. This serves as the foundation for vulnerability management because an organization can't manage the risk posed by assets they can't see.

IDENTIFY/CLASSIFY

Stage two is identify/classify, otherwise known as vulnerability assessment. During assessment, organizations find vulnerabilities within an asset or group of assets-be they operating systems, applications, firmware, or protocols-and classify them to get ready for the later stages of work. Though they are distinct activities, stage one and two are often mentally lumped together under the umbrella of vulnerability assessment. Unfortunately, this is also about as far as many organizations go—getting so caught up in the difficulties of finding flaws that they never actually advance to methodically addressing them.

PRIORITIZE

Stage three of vulnerability management is to prioritize. This is a crucial one for both OT and IT vulnerabilities, because an organization will always find more flaws in their assets than their team will ever be able to fix. In the prioritize stage the team decides what gets fixed and when, utilizing classification data like Common Vulnerability Scoring System (CVSS) scoring about a flaw's severity, as well as threat intelligence about how it is typically exploited in the wild. This also involves business risk based on what the asset is, how it is used, and what the risk level means for the business. Prioritization of OT vulnerabilities takes special care because there are so many other dimensions of risk to be considered that don't exist for IT systems.

REMEDIATE/MITIGATE/ACCEPT

Stage four is remediate/mitigate, which could also be considered the vulnerability resolution stage. This is where an organization closes out found vulnerabilities. While many in the IT world have come to equate vulnerability resolution with remediation steps like patch or configuration management, in OT environments it's crucial to realize that this is just one path to closure. Organizations can also mitigate risk by using compensating controls. And they can also consciously choose to accept the risk of vulnerabilities when operational risks outweigh the risk of the flaw being exploited. Remediation and mitigation decisions should be based on a complete picture of risk, not just vulnerability risk. Operational risk can often outweigh vulnerability or security risk, especially with OT.

Because environments are dynamic and constantly changing, vulnerability management teams run through these stages cyclically, continuously repeating stages as they make progress closing out old vulnerabilities, and as existing systems are changed, new ones are brought online, and old ones are decommissioned.

There are a lot of differences between vulnerability assessment and vulnerability management, but the ultimate differentiators are the resolution of vulnerabilities and the tracking of the resolution progress in the vulnerability management process made across an OT inventory.

> "The difference between vulnerability management and vulnerability assessment: resolution and tracking disposition."

True vulnerability management requires not only cycling through the four stages, but also documenting the team's work as it does so.

Documentation on the disposition of vulnerabilities—whether they're open, eliminated through patching, mitigated through compensating controls, or purposely left alone through risk acceptance, closes the loop on the vulnerability management cycle, especially in OT environments.

Because remediation and mitigation decisions are be based on a complete picture of risk, in OT operational risk quite often outweighs vulnerability or security risk. This means that vulnerabilities are risk accepted more frequently in OT than in IT.

> "In OT the vulnerability management cure is often worse than the disease of letting a flaw exist within a system. Vulnerabilities are risk accepted more frequently in ot than in it."

Even when flaws remain unfixed through risk acceptance, they're not hidden if they've run through a vulnerability management program that tracks disposition. Through disposition tracking, organizations gain visibility into where flaws exist within their assets and how they've been addressed. In this way they can and obtain a roadmap for future work as risk factors and the threat environment changes.

IV. RECENT OT VULNERABILITY TRENDS

In addition to all of the factors that make vulnerability management different for OT, cyber defenders and OT operators should consider one other huge but hidden challenge. Namely that public vulnerability sources used for assessment, classification, and prioritization often contain incomplete or inaccurate data.

Through careful analysis and field validation, Dragos has found that existing severity scores are often inaccurate, incomplete and lack both context and guidance. Industrial teams struggle with how to interpret and apply in their environments and spending too much time chasing the wrong issues. Consider the following findings from Dragos' **2020 ICS Cybersecurity Year in Review report**.[3]

3 Dragos' 2020 ICS Cybersecurity Year in Review report: https://www.dragos.com/blog/industry-news/2020-ics-cybersecurity-year-in-review/

IV. RECENT OT VULNERABILITY TRENDS

Organizations that want to build out an OT vulnerability management program or improve the maturity of their existing program will need to address the shortcomings of these public sources. Simply relying on them without added context distorts the process of prioritizing vulnerabilities appropriately and makes it harder to efficiently resolve vulnerabilities at scale.

43% **of vulnerability advisories contained errors making it difficult to prioritize mitigations**

61% **of advisories with a patch had no vendor mitigation**

64% **of advisories with no patch had no vendor mitigation advice**

73% **of vulnerabilities are deemed more severe by Dragos than Public Advisory CVSS score**

V. 10 WAYS TO GET STARTED

Building out an OT vulnerability management process is a slow, methodical process that will take resources and wherewithal to get right. There is certainly no cookie-cutter path for an industrial organization to follow, but these 10 pointers do offer some valuable way points for a successful journey.

1. Don't Rush In

One of the most common mistakes that organizations make when first tackling OT vulnerability management is caving into panic. Often a security incident or a regulatory requirement creates sudden, intense pressure to address a specific ICS vulnerability or set of vulnerabilities.

Executives make mandates from on high and in the scramble to fix a flaw, the security team breaks systems due to improperly testing or not truly understanding how OT systems are being used.

Doing OT vulnerability management right requires security and operations staff to slow down, think through risk implications so they can help leadership create the right mandates for resolving vulnerabilities, and create a repeatable system for making good decisions that truly lower overall risk to the business.

2. Everything Starts With an Asset Inventory & Visibility

At the foundation of every great OT vulnerability management program there exists a thorough inventory of OT assets. To get started properly, organizations need to undergo an asset discovery process that can not only dig up all those assets, but also classify them by a range of attributes, map their connections, and track their configuration state. Ideally, the organization shouldn't just plan on doing a point-in-time survey of assets but strive to build out automated mechanisms to gain continuous visibility into the state of the inventory. This kind of ongoing monitoring will ensure the sustainability of a successful vulnerability management program.

Many it asset visibility tools and tactics do not translate well to the OT environment—for example, you can't put an agent on a programmable logic controller (PLC). This means that organizations may need to take a different approach that's specific to OT environments to achieve a level of visibility into assets, vulnerabilities, and risk that corresponds to what their security team may be used to seeing across the it asset portfolio. Make sure a plan is established that determines data collection requirements through a structured approach like Dragos's collection management framework [4]. A good plan will lay the foundation for a successful outcome that creates a sustainable, scalable, and efficient asset visibility program that continuously updates the inventory.

3. Don't Fear Automation

While we've got automation on our minds, let's put to rest the idea that OT vulnerability management must be a completely manual process. True, you're not going to blanket OT systems with automatic patches and updates the way you do in it. However, while the remediation and mitigation of many critical ICS systems must necessarily remain manual, many aspects can be automated.

A lot of the automation occurs on the front end of the process, during the first three stages of the vulnerability management cycle—ultimately OT is very safe in automation of reporting tasks and understanding the environment. As mentioned, asset discovery is low-hanging fruit here. Similarly, vulnerability assessment and the process of tracking configuration baselines and instances of configuration drift provide opportunity for a lot of automation. Prioritization of assets can also be automated with the data provided by discovery and assessment.

Execution of resolution may be risky in many areas, but tasks like backing up systems and testing backups are imminently automatable. Additionally, don't discount the time saved by automatically patching non-critical OT systems.

4 Dagos, Inc.: Building a Collection Management Framework for Industrial Control Systems
https://www.dragos.com/blog/industry-news/building-a-collection-management-framework-for-industrial-control-systems/

4. Periodic Walk Downs Are a Must

Sometimes it can be difficult getting started with automated discovery because an organization doesn't know what it doesn't know about its infrastructure. This is why it can be valuable to kick off the initiative with manual discovery. Start first by mapping high-level architectures and performing comprehensive facility walk-downs to start physically identifying hidden assets that will need to be accounted for.

This early manual work will make it easier to prioritize and decide where to establish telemetry first for continuous, automated discovery.

Walk downs are also crucial throughout the vulnerability management process to validate what automated asset discovery is producing and to fill in the gaps across the environment that may not necessarily be covered by monitoring and telemetry. Consider organizing regular Gemba[5] walks to go and see environments and compare results to what's been previously documented. Ideally the organization should have an easy path within its documentation or mapping mechanism to add the results of periodic manual discovery.

5. Documentation is Crucial

Documentation is key in OT vulnerability management for a number of reasons. First of all, because so much of the process does remain manual, documentation of processes brings discipline to bear to ensure that they're not done on an ad hoc basis. Ultimately, an organization should try to spin that documentation into compliant workflows that ensure that everything is standardized, repeatable, and provable.

It's crucial to be sure that part of the documentation includes information on roles and responsibilities across the workflows. Given the long time-frames for updating systems, make sure that responsibilities aren't designated to individuals but instead to specific roles or titles. This ensures that even if your teammate isn't around in six years when the maintenance window of a piece of equipment opens up, it still will get patched when the time comes.

Finally, as previously mentioned, documentation of what has actually been done about found vulnerabilities is what differentiates vulnerability management from assessment. Documentation of the disposition of vulnerabilities is especially important for OT vulnerabilities that must be risk accepted due to operational consideration.

Ultimately all this documentation work can be a huge factor in satisfying regulatory auditors and helps lower the blood pressure of executives concerned about risks stemming from OT vulnerabilities.

6. Understand OT Vulnerability Prioritization is Different

OT vulnerability prioritization is very different than in IT, where the focus is primarily on severity scoring of the flaw and, ideally, business criticality of an asset. The added dimensions of operational risk and physical world ramifications changes how things are calculated. The industrial space has also exceeded a key threshold: in 2020 more than one high severity vulnerability in industrial products was disclosed for each working day of the calendar year[6].

5 Six Sigma Daily, What is a Gemba Walk and Why is it Important? https://www.sixsigmadaily.com/what-is-a-gemba-walk/
6 Dragos' 2020 ICS Cybersecurity Year in Review report: https://www.dragos.com/blog/industry-news/2020-ics-cybersecurity-year-in-review/

Identifying critical 'crown jewel'[7] systems is crucial for making these prioritization decisions, but keep in mind that it isn't as simple as saying 'That's a vulnerability in a crown jewel asset, we've got to patch that immediately.' Often these assets also carry the highest operational risk if they're disrupted by remediation activity. They're also critical pieces of equipment that are most likely to be buffered by the most security controls in an OT environment. So, the decision is much more nuanced than that.

Automation standards and compliance regimens like IEC (International Electrotechnical Commission) 62443 tend to focus on assets deeper in the Purdue Model[8], but organizations should also consider other factors as they establish risk scoring for prioritization. For example, asset owners should be providing heavy weight to the most connected systems in their OT networks—connected to third parties, different vendors, and the outside world, especially if a path to the internet exists on these assets. Those are systems that are normally at the most risk to many of the OT vulnerabilities that surface. Additionally, priority should be given to assets with single points of failures or existing as centralized systems. This includes things like Active Directory, management consoles, even Windows Server Update Services (WSUS) patching. The SolarWinds fallout offers a great example how one box can have its fingers into the whole OT environment.

Other considerations may be whether there are mitigating factors to the operational risks that would keep an organization from remediating. For example, systems that have redundancy built in could potentially go higher up the priority list if they're relatively easy to take offline.

7. Master The Art of Compensating Controls

It bears repeating that in many OT systems, patching simply is not an option due to the operational risks involved with changing those assets. In fact, data gathered for the 2020 Dragos Year in Review found that among the OT vulnerabilities disclosed in 2020, more than one in five didn't even have a patch available when announced by vendors.

Additionally, critical OT assets are frequently insecure by design such that even with the patch applied they're still vulnerable to loss of view or loss of control through abuse of normal functions. In these cases, asset owners must ask themselves why they should incur patching risk if a system will remain vulnerable to design issues.

This means that effective OT vulnerability management programs must master the art of compensating controls to lower the risks of not only vulnerabilities but latent design flaws that must persist in certain assets. The goal should be to reduce attack surface wherever possible by hardening asset configuration, shutting down unneeded functionality, limiting the footprint and connectivity of assets, and updating the systems that can be patched that touch vulnerable systems.

For example, take the well-known vulnerabilities in Microsoft Server Message Block (SMB) v1. If it isn't possible to update the system to SMB v2, depending on how systems are functioning the right move may be to shut the protocol off. As with risk acceptance, mitigations like these should be meticulously documented in thorough vulnerability

7 Improving OT Defense and Response with Consequence-Driven ICS Cybersecurity Scoping
https://www.dragos.com/resource/dependency-modeling-for-identifying-cybersecurity-crown-jewels-in-an-ics-environment/
8 Dragos, Inc.: Threat Hunting Part 2: Hunting on ICS Networks
https://www.dragos.com/blog/industry-news/threat-hunting-part-2-hunting-on-ics-networks/

disposition tracking so that changes are not accidentally reversed.

For the crown jewels, the idea is that they should be using as little of the functionality and communicating with as few parts of the network as is necessary for processes. Network and application firewalls can be invaluable for this, as can application white listing. Similarly, organizations should reevaluate network segmentation.

8. Actively Manage Vendors Relationships

Across the OT landscape, most major vendors offer cyber solutions and services that typically include patching, endpoint protection, and configuration management. But organizations shouldn't consider these as a replacement for an internal vulnerability management program. These services don't provide 'set it and forget it' assurances for true vulnerability management, nor do they do the documentation necessary to provide organization-wide visibility into risk. Organizations need to actively manage their vendor relationships to not only validate that the services are upgrading or mitigating systems as agreed, but also to document the status of vulnerabilities across all vendors and the entire asset inventory.

In the cases where the organization is patching its own systems, it will also need to be mindful of working with vendors to ensure that the changes don't void support contracts or warranties. Often vendors require pre-approval before changes are made to critical ICS systems.

9. Change Management

For many critical ICS assets, change management governance is extremely rigid due to compliance for safety management. An asset like a PLC, for instance, would always go through a formal change management process mandated by process safety management according to the requirements of different industries. If the asset is involved with an industrial process, the requirements will likely be much more rigorous.

However, there are also gray areas in OT where certain assets don't have a process impact but for which changes and configuration states could still impact operational risk. Take a historian, for example, which will not have a process impact if it crashes but is still vital in the overall OT ecosystem. A maturing OT vulnerability management program should take care to create a change management process that catches assets that could otherwise fly under the radar, governing and tracking changes as you make remediations and mitigations.

10. Hire Dedicated Staff

An effective OT vulnerability management program is an ongoing concern that requires dedicated resources to maintain. While many duties in discovery and assessment can be automated, there's a considerable amount of work necessary to coordinate with asset owners, update systems, employ compensating controls, validate, and track progress. Expecting an individual or even several individuals to do break/fix, project work, engineering duties, and also do all of their own vulnerability management work is not a reasonable expectation.

VI. PARTNERING WITH DRAGOS: THE PATHWAY TO MATURE OT VULNERABILITY MANAGEMENT

Dragos's vulnerability management solutions provide the most accurate and complete information available to industrial organizations. The **Dragos Platform**[9] provides continuous monitoring of OT networks to streamline discovery of asset inventory, map out resources and automatically assess for flaws in the environment by comparing the inventory to known OT vulnerabilities.

Purpose-built for OT, the Dragos Platform uses our own vulnerability knowledge base for this assessment. Dragos provides added context during these checks by validating the accuracy of public information about vulnerabilities and providing confidence ratings to detections to help organizations prioritize risk. Dragos also enriches that information with unique mitigation guidance that goes above what the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) and the National Vulnerability Database (NVD) offers.

Most importantly, Dragos layers in threat intelligence about how attackers are using vulnerabilities and OT-specific domain knowledge about operational risks to develop a system to score vulnerabilities based on a "Now-Next-Never" system for prioritization of all detected vulnerabilities in an environment. This Now-Next-Never system folds insight from Dragos based on our experts' evaluation of the software, the vulnerability itself, the OT attack surface areas, and the steps necessary for attackers to leverage the flaw to impact OT processes. This analysis offers the most thorough threat insight to provide a risk-based prioritization fully relevant to OT environments.

This gives users the clarity to focus their effort on the highest priority issues so they can mitigate the biggest risks and minimize wasted time. Dragos provides complete vulnerability lifecycle tracking, offering an automated way to track patch status, compensating controls, and risk acceptance.

If you are interested in a discussion about how Dragos can help meet your needs around OT vulnerability management, a number of options are available. Organizations looking for a scaled vulnerability assessment can speak with our Professional Services team. Those who require a robust technical solution for ongoing Vulnerability Management, including CVSS score correction and enrichment, with expert guidance around remediation priority and full historical disposition, should consider the Dragos Platform. For more information, please contact **sales@dragos.com**.

9 The Dragos Platform: https://www.dragos.com/platform/

ABOUT DRAGOS

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

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

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE INDUSTRIAL COMMUNITY, PLEASE VISIT WWW.DRAGOS.COM.