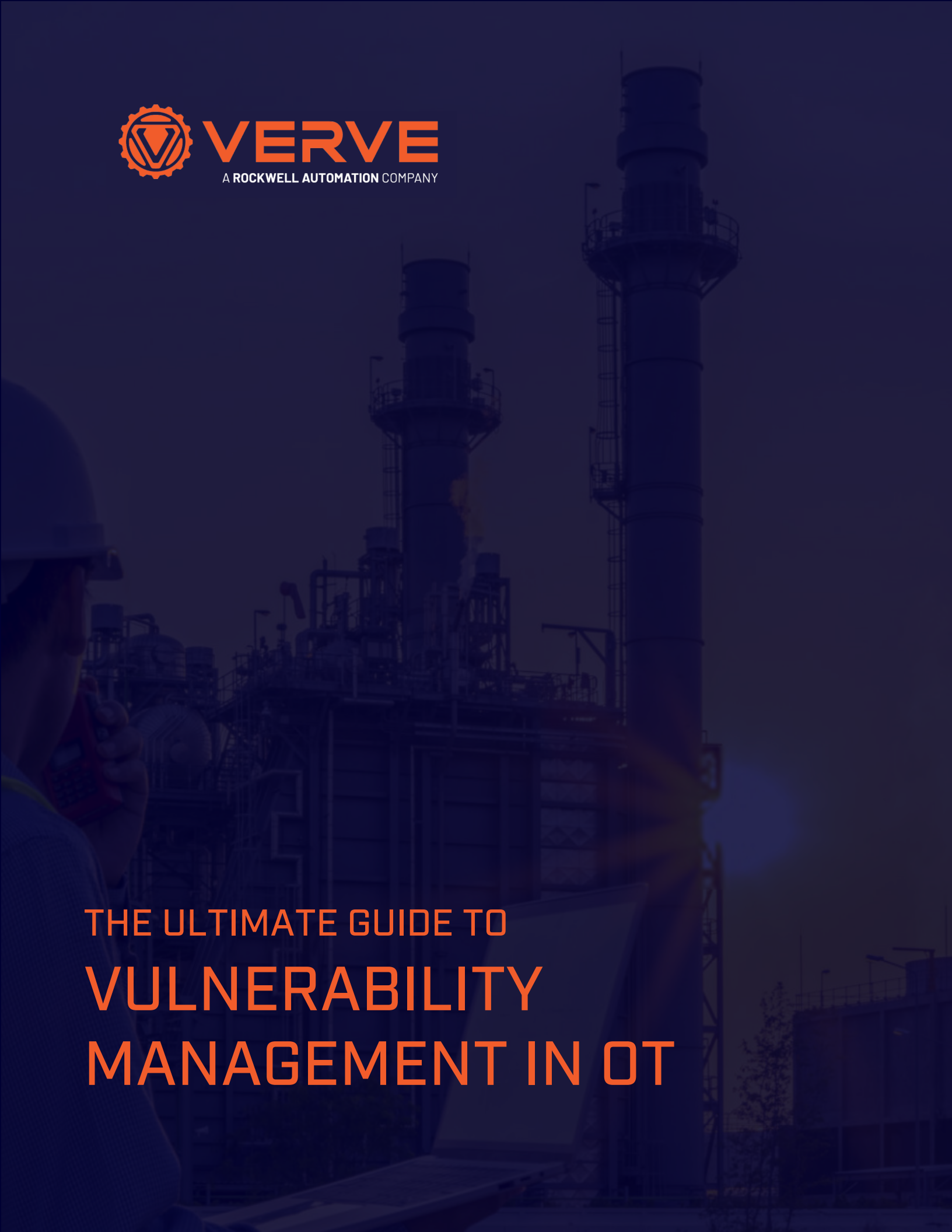


VERVE
A ROCKWELL AUTOMATION COMPANY

THE ULTIMATE GUIDE TO VULNERABILITY MANAGEMENT IN OT

TABLE OF CONTENTS

Background

OT vulnerability management is a seemingly straightforward cyber security process meant to reduce the amount of cyber-related threats and attacks. But it tends to be easier said than done. In this Ultimate Guide to OT Vulnerability Management, we discuss the biggest challenges around vulnerability management and provide actionable recommendations to overcome them for optimal cyber security efficiency.

Introduction

Cyber threats and attacks are on the rise for industrial, manufacturing, and critical infrastructure organizations. Many of these threats are the result of vulnerabilities present in the organization's OT systems. Targeted threat actors or untargeted ransomware attacks exploit these vulnerabilities to gain access into industrial networks for financial gain or to interrupt operations.

The rise of cyber-related threats stems from the acceleration of IIoT technology and digital transformation such as Industry 4.0 in manufacturing, an increase in remote work and remote access amid the COVID-19 pandemic, and the prevalence of ransomware.

Cyber criminals are growing smarter, and these factors have undoubtedly increased the attack surface for threat actors to take advantage of, costing the U.S. economy as much as $109 billion in 2016.

Enter vulnerability management – A seemingly straightforward OT cyber security process that is meant to significantly reduce the amount of cyber-related threats and attacks. But if it's so easy, why aren't we doing it?

What is OT Vulnerability Management?

Let's take a step back and start by answering the question, what is vulnerability management?

Vulnerability management is defined as the business process of identifying, prioritizing, remediating, and reporting on software insecurities and misconfigurations of endpoints in Operating Technology (OT) or Industrial Control System (ICS) environments.

Compared to traditional IT environments, OT vulnerability management is more complex. Vulnerability management, as defined in IT, specifically focuses on identifying known software insecurities published by vendors or third parties. But in OT, it's not as simple as scanning for known insecurities then rebooting a computer to install the latest OS updates.

First, industrial control systems in OT environments often-times use legacy or outdated equipment and software that no longer receive security updates. Scanning the systems can cause risks to operations and applying patches requires taking these systems offline for maintenance, which is not only expensive but disruptive to critical operations.

Second, in many cases, the most immediate path to remediation – i.e., patching – is not possible with outdated, sensitive, or continuously running systems that one finds in OT. And finally, "vulnerabilities" in OT need to include "insecure by design" not just software risks – things such as insecure ports and services, insecure user & account management, etc. It's no wonder industrial organizations find themselves neglecting vulnerability management and broader risk management of OT systems.

A full OT vulnerability management program includes:

- Assessing assets for known vulnerabilities AND broader insecure by design risks
- Prioritizing those based on possible exploitation and impact
- Remediating vulnerabilities and risks through software patches, managing configurations, or deploying various compensating controls

Vulnerability management is often a complex, manual effort requiring hand-offs and the involvement of many systems. Most devices found in OT/ICS networks are sensitive, so traditional IT vulnerability scanner solutions are not tenable.

Challenges and Solutions to OT Vulnerability Management

Vulnerability Management Challenge #1: Incomplete Asset Inventory

Many operating companies have very little asset inventory data. In most cases, asset data is limited to aging spreadsheets or incomplete data from a mix of sources, providing intermittent or spotty coverage. When a new vulnerability is discovered, you turn to asset inventory to determine how many OT assets are in scope for this risk and how many can be safely patched. But without the detailed profile of each asset, this job becomes impossible.

We all know the common motto, "you can't protect what you can't see," and while this is true, your asset inventory should be more than a list of assets. A powerful asset inventory management solution is crucial for a successful vulnerability management program when combined with detailed profile data per asset (such as the criticality of the asset to operations, what layer the asset is located, is it remotely accessible, etc.). The more context you have about each asset, the stronger your vulnerability analysis and prioritization.

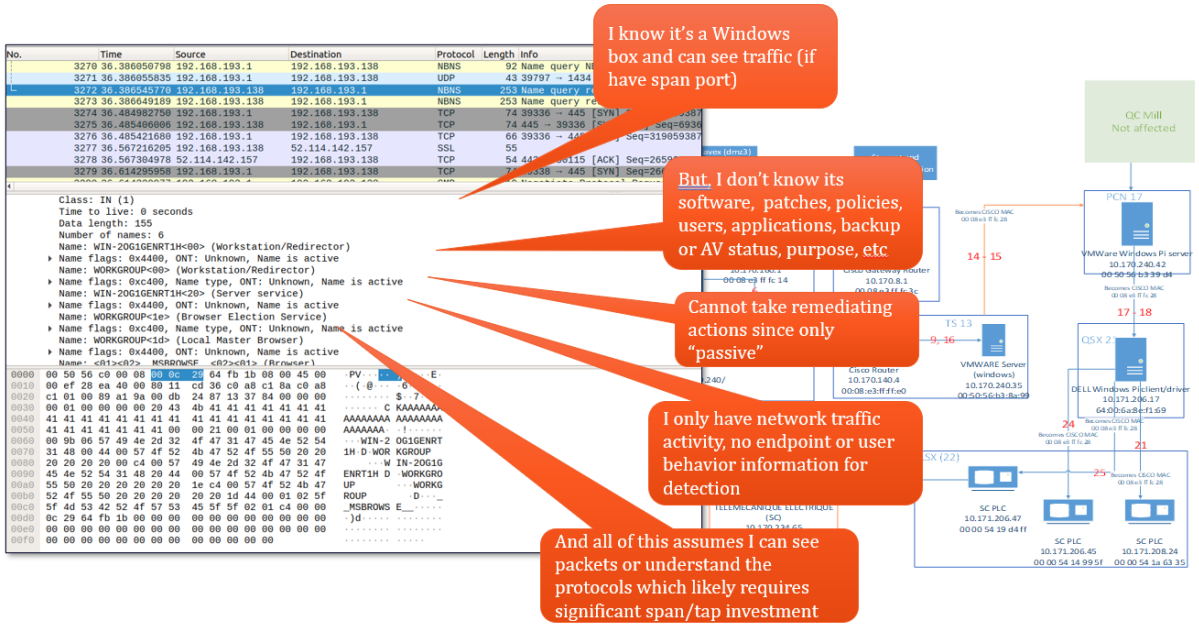
But this level of detailed asset information is extremely rare because the biggest challenge for any OT security environment is aggregating this information. Most operating companies have very little asset inventory data. In most cases, asset data is limited to aging spreadsheets or incomplete data from a mix of sources, providing intermittent or spotty coverage.

Many industrial companies turn to passive or network-based listening tools as a first step in compiling an asset inventory. Passive tools are valuable to an extent but do not provide the necessary data to build a robust vulnerability management program.

3 ways passive anomaly detection tools fall short in asset inventory:

1. Incomplete coverage: A passive listening tool only picks up assets it can “hear”, meaning if you don’t have your asset communicating through a specific “listener”, its presence will not be detected, thus not included in your asset inventory. Serially connected relays, for example, are highly unlikely to be included in your list of assets. It also means putting “listeners” into all subnets, requiring exponential resources.
2. Inaccurate data and characteristics: Passive anomaly listening provides content on what is transmitted. If the endpoints are not tuned to send data, it won’t be captured. This includes firmware, serial numbers, software versions, user accounts, ports, and services that are listening. They do pick up a lot of traffic, but not everything. In the end, that is not really the use case they were initially designed for.
3. Inability to tune: It is valuable to identify whether systems are working or gather feedback that something is at risk. But it’s not enough to simply identify the vulnerability if you cannot manage it. An alert is just that – a warning. Taking action to remediate is impossible with passive anomaly detection tools.

“Passive” Network-based approaches fall short…



Over the past 15 years, Verve has developed an alternative approach that allows deep visibility into these systems and does not rely on what is "on the wire" to determine vulnerabilities and risks. This approach leverages a combined OT agent and agentless approach that goes directly to the endpoint. As a result, the inventory is both deep and broad.

What data types are useful in a vulnerability management program?

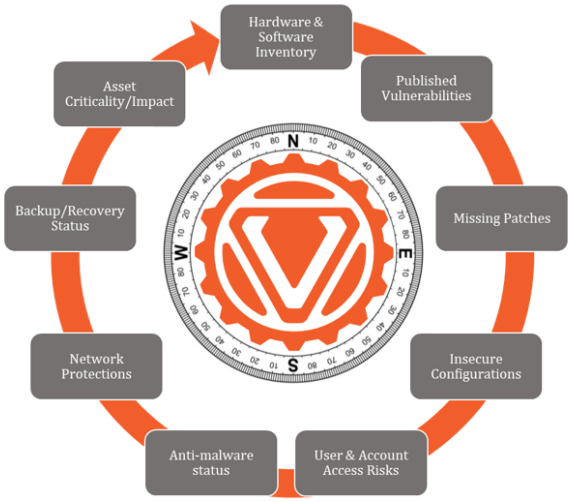
The data that this approach collects allows for a comprehensive risk assessment. Let's run through a scenario taking a raw vulnerability risk score and applying practical analysis to it in the context of an OT environment:

A vulnerability is identified, and we know its attack vector, severity, complexity to execute, and which systems are affected. How do we decide to proceed?

- Is the system at risk critical to operations? (This requires system analysis and ranking often called metadata or tribal knowledge.)
- Is the system hardened? (This requires detailed knowledge of the asset characteristics.) Is remote access enabled only for administrative accounts?
- Is the system likely to be compromised based on contextual data relative to the attack vector?
- Is this asset in layer one or two, and is it an adjacent network or network attack vector? How about a layer 3.5 asset?
- What if we have a current backup plan, and whitelisting is in enforcement mode?

These types of data sources and the insight they provide are a significant benefit to the analysis and eventual action plan an OT environment requires. To eventually prioritize the remediation of vulnerabilities, organizations need an asset inventory that provides a 360-degree view of the assets including comprehensive risk scoring beyond CVE or CVSS. By gathering this data in a single database, practical remediation strategies are enabled down the road.

Verve's 360 Degree view provides deep insight into each asset



Benefits of 360^0 risk view in ICS:

- Prioritize limited resources on most critical assets and risks
- Stop the spread by focusing on compensating controls when protection isn't feasible – e.g., 100% patching
- Address "insecure by design" assets regardless of CVE Vulnerabilities
- Understand recovery status – backups, network connections, etc.
- Address user/accounts in non-AD environments
- Ensure initial protections (e.g., network segmentation) haven't experienced "rot"

Vulnerability Management Challenge #2: Identifying Vulnerabilities

There are many options for vulnerability scanners on the market. They usually require the latest threat intelligence and markers loaded into the application, which targets end devices for scanning. There are controls and settings to adjust to increase or decrease the force and functions of the scan, which is a good thing for OT where thousands of ports are scanned with requests at once.

Vulnerability scanning was designed to identify weaknesses of a system to quickly secure gaps in infrastructure from being exploited, but this provides greater challenges in OT than in IT. In OT environments, we dial down vulnerability scans to a lower volume for a gentle approach and conduct the scans on redundant and more robust systems.

Many industrial organizations prefer to scan only during outages or turnaround opportunities to further reduce the risk introduced by a vulnerability scan. These are established OT safe practices for bringing IT tools into the OT world but produces ineffective results.

In OT environments, scanning presents three challenges.

First, OT device scanning can disrupt operations or worse, disable them completely. Because of the integration of these various systems, if one system goes down, this may cause others to have issues, eventually tripping the plant.

Second, it happens infrequently, so as soon as a scan is finished, it is already outdated. Conducting a scan during an outage or during scheduled downtime means there are large gaps between scans, leaving you with an incomplete picture of the vulnerability landscape at any given time.

Third, if you do conduct vulnerability scanning, it does not gather 100% of vulnerability information. While vulnerability scanners have settings to decrease the force and functions of a scan intended to minimize potential damage to sensitive OT systems, this gentle approach reduces accuracy because it cannot gather deep asset inventory knowledge.

In lieu of vulnerability scanners, a combination of an agent-based and agentless OT systems management approach is the best alternative. With real-time coverage of your assets and their vulnerabilities, you're one step closer to responding and protecting your most critical OT assets.

Leveraging an OT agent that is proven across all OEM vendor systems and tuned to the particular requirements of those OT devices on OS-based devices, while simultaneously using an agentless service to profile network, communications gear, and embedded control equipment, generates a robust and complete asset inventory including firmware versions, patch status, configuration settings, etc.

That robust inventory can be automatically cross-referenced with various vulnerability databases such as the National Vulnerability Database (NVD). Mapping this to your inventory reveals the cross-section between your known assets and where the cyber risks lie. The differences are significant:

- Deep risk information: Know all details about each endpoint, and profile information about the asset not only the CVE scores but also the other "insecure by design" risks as well as any compensating controls currently deployed.
- Unlimited systems: 100%, real-time coverage of all assets means your vulnerability management view is complete across the entire OT environment.
- Ages slowly: Asset inventory updates in near real-time, so querying your asset base (normal NVD update or manual polling for emerging/evolving risk) is instantaneous, and your data is new, relevant, and fresh.

Vulnerability Management Challenge #3: Prioritizing Vulnerabilities

According to ESG Research, 34% of cyber security professionals reported their biggest vulnerability management challenge is prioritizing which vulnerabilities to remediate. With hundreds or thousands of vulnerabilities, it can feel a bit like playing whack-a-mole with no end in sight. When an organization conducts its first vulnerability and risk assessment on its OT systems, it is typically overwhelmed by the volume of risks to remediate.

It is not atypical to have thousands of critical vulnerabilities that need to be patched – not to mention insecure configurations, dormant users and accounts, improper passwords, etc. In many cases, OT operators may throw up their hands-on how to make any progress at all.

As the organization attempts to remediate these risks, the challenge of taking those remediating actions becomes the next hurdle (discussed below). As a result, prioritization of actions AND possible compensating controls is a key task.

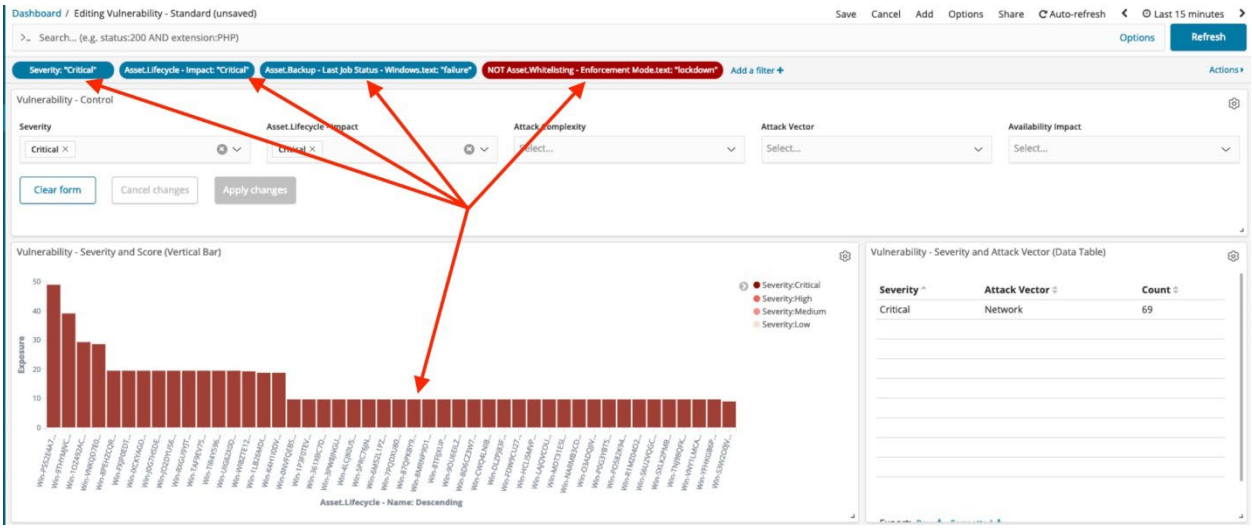
Piggybacking on the earlier discussion about the value of a robust 360-degree asset inventory as the foundation for your vulnerability management program, the context of the most critical or at-risk assets determines priority because every critical vulnerability doesn't present the same security risk to operational systems.

A 360-degree view of the asset enables the organization to score an asset on much more than the sum of CVSS scores from vulnerability databases. It allows for prioritization based on the comprehensive view of that asset in its risk context.

For example, two assets with an equal number of critical vulnerabilities may have very different risk prioritization based on information such as the asset's criticality to the process, the presence or lack of network firewall or application firewall protections, the presence or lack of application whitelisting or updated antivirus signatures, the presence of insecure accounts that may be used to exploit a vulnerability, etc.

In one client example, a vulnerability management dashboard that showed over 35,000 total patches (low to critical) was filtered to show critical assets (operations deemed these assets to be critical to safe operations) with a critical risk that failed their recent backup and does not have whitelisting in lockdown mode.

The dashboard eliminated 34,934 risks to focus attention on the highest priorities:



Vulnerability Management Challenge #4: Timely Remediation of Vulnerabilities

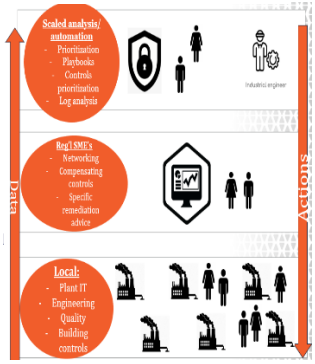
Remediating vulnerabilities includes patching, hardening configuration settings, and possibly the deployment of compensating controls or remediations such as application whitelisting firewalling, etc. In IT, this is a somewhat straightforward task given the presence of automated tools and teams dedicated to IT Security Management functions. In OT, however, it's not that simple.

While software patching in IT occurs daily or weekly, in OT environments it tends to be tedious, difficult, and time-consuming when there is a shortage of time and necessary skills. Tracking which patches are in scope, if they are approved by the vendor, which devices it belongs on (hello, detailed asset inventory, anyone?), and the current status of each system is a lot to keep up with. Furthermore, operational requirements for constant run-times means patching may require taking an outage which can be expensive.

There are several challenges:

- Available, knowledgeable resources to identify which patches should be deployed and when
- Available resources to conduct the patching at the site level given the usual manual processes
- OEM push-back on the deployment of patches
- Systems integration often requires multiple upgrades if a single patch is deployed to one part of the control system
- Resources to track and monitor the application of remediation tasks – patching, configuration hardening, AV updates, etc.

1. Think Global: Scale analysis in the centralized platform – Gather data from all sites into a centralized database for vulnerability and risk analysis and remediation/response planning.
2. Leverage regional SMEs with access to the same platform for specific security advice.
3. Act Local: Operations control over actions to provide automation to plant/regional personnel to enable action in a way that is sensitive to requirements for operational environments.



The most effective way to address this challenge is to take a "Think Global: Act Local" approach to OT Security Management. This approach centralizes the oversight and analysis of risks and vulnerabilities into an efficient, trained team of OT security personnel. This requires a consolidated database of all assets – across OEM vendors, sites, etc. – into an enterprise view.

It also requires the 360-degree view mentioned earlier. This group drives efficiency in the analysis and playbook phase. Otherwise, an organization needs to have vulnerability experts at each plant – and often for each different control system – adding significant costs on OEM services.

The second component of this strategy is the "Act Local" part. This means the remediation actions are in the control of the operators closest to the process involved. One of the biggest risks in OT vulnerability management is the unintended consequences of patching or hardening a system from thousands of miles away without the visibility of the OT operators in that task. This can cause trips to plants or worse – safety concerns. As a result, the final action step needs to be handled by those with insight into the process and the timing of when to apply those actions. At the same time, this cannot mean those actions need to be taken manually. Resources are too limited. Therefore, technology should enable the automated local action when the operator

has approved it and "pulled the trigger" on the action, so to speak. The platform needs to enable distributed actions designed centrally, but where the automation puts the control in the hands of the operator – or "Act Local".

This approach can apply to patches, user & account management, configuration hardening, software management, etc. – the whole range of vulnerabilities, risks, and compensating controls.

Vulnerability assessment is NOT management. Management involves taking action to fix risks in the environment. This is another reason that the agent-agentless approach is more effective. It allows for the practical, OT-safe, efficient remediation of risks, not just their detection.

An agent-based approach enumerates endpoint security settings like disabling the guest account from initiating remote access protocols or listing, then disabling, known bad ports or services if they are not needed. An agent tunes any parameter on the endpoint, providing the ability to filter at-risk assets, target specific compensating controls, and automate the execution of applying those compensating controls.

In essence, an agent-based technology, coupled with a central reporting capability, allows for the most effective, yet OT-safe approach to the remediation portion of a vulnerability management program.

Vulnerability Management Challenge #5: Tracking the Vulnerability Management Process

Many ICS security leaders find it difficult to manage the full vulnerability management process from start to finish. In many cases, organizations conduct one-time or infrequent vulnerability assessments because of the manual effort required. Once the assessment is complete, a separate tool or internal labor is needed to act, or remediate, the identified vulnerabilities. It is easy to lose track of the process when many balls are in the air.

A closed-loop vulnerability management process with integrated remediation is key but bringing administrative functions such as marking patches as reviewed and approved into the same toolset brings management to an entirely new level. Asset inventories, vulnerabilities, and remediation information update in real-time so querying an asset base is instantaneously refreshed with relevant data.

Aligning the right people for organizational success

There is no doubt that vulnerability management in OT is a difficult enterprise. However, there are available tools and processes to significantly improve the effectiveness and efficiency of remediating and reducing risk in the environment. To accomplish this effectively, industrial organizations need to adopt technology to accomplish the needed 360-degree view of risk, centralization of prioritization, and OT-safe remediation.

They should also need to consider the "people" and "process" side of the PPT. In many cases, industrial organizations are already conducting vulnerability management on IT assets and have people and processes set up to do so. OT needs to leverage that knowledge base and expertise. By the same token, OT systems are very different, and the eventual organization model needs to find a way for the two parts of the organization to work together.

IT OT convergence is a fundamental requirement in this age of risk and a lack of skilled resources to combat it. This topic produces a significant amount of debate, with some feeling that IT/OT is not understood and likely to fail, so instead, we should focus on risk and remediation.

OT particulars mean we need to adapt off-the-shelf IT practices and toolsets for unique and demanding environments.

Perhaps the biggest problem is that IT technology is found in OT environments and neither a pure OT person nor a pure IT person can handle all security requirements on their own. The depth and breadth of risk coupled with the weird and wonderful ways OT is often put together (legacy situations, greenfield are coming along well) mean a combination of skills and knowledge are required to collaborate on useful, safe ways of providing security tools and functions in an operational environment.

There are no shortages of specific topics or practices required of a robust security program to examine, but perhaps the most complex or involved practice that requires precise and delicate negotiation between IT and OT skills and tools sets is in vulnerability management.

We have seen the "Think Global: Act Local" approach work very well in practice. This allows the teams to leverage scale and knowledge at both ends of the process. And it seamlessly fits with the technology that enables this – an agent-agentless platform that can aggregate data across sites and vendors but allow for rapid, OT-controlled remediation actions.

Vulnerability management on its own is short-sighted and difficult to execute in OT. The true path to OT risk reduction is adopting a new way of thinking and scaling technology to enable it. 360-degree risk management provides the insight, context, and toolset to identify, contextualize and prioritize actions. This approach enables fleet-wide visibility into risk and provides security experts' last-mile asset oversight to boots-on-the-ground OT staff to extend the analysis of the action. This is how leading industrial companies make meaningful and profound improvements in OT risk reduction.