

OTbase

THE OT VULNERABILITY MANAGEMENT HANDBOOK

A cookie-cutter approach to effective OT vulnerability management, by the team that cracked Stuxnet.



Table of Contents

Executive summary	3
Introduction	4
Known Vulnerabilities Primer	5
Laying the Foundation: Tooling	7
Furnishing your Mitigation Strategy	11
Prioritizing by likelihood of exploitation	13
Prioritizing by system criticality	15
Plan and Execute	16
Monitor and Report Progress	17
Conclusion	19

Executive Summary

Every organization feels the pressure towards better cyber security.

Management demands vulnerability management efforts, but often doesn't have good ideas how to turn aspirations into measurable results. This handbook acts as a how-to guide for the implementation of an effective OT vulnerability management process that is repeatable and delivers measurable and meaningful reductions of the attack surface.

Written by the team that cracked the infamous **Stuxnet** malware, it focuses on three major aspects:

- Proper tooling
- A remediation strategy that is easy to implement
- Superb reporting

It addresses both OT security practitioners and top management.

Introduction

If you've downloaded this eBook, it's likely you've started an OT vulnerability management process only to determine you're not getting anywhere. Despite your best efforts, vulnerabilities keep piling up, and management is not amused.

OT vulnerability management is a process that involves identifying, assessing, and mitigating vulnerabilities in OT systems. And it's a continuous process. New vulnerabilities are discovered every day, with growing frequency. While you're doing something, you're not making much, if any, progress.

The reality is most OT security teams end up frustrated. That turns into frustration shared by management, who want to see demonstrable progress.

The bottom line is that without a very clear-cut strategy, set of metrics, and workflow automation, you will never get out of the weeds.

What you need is effective OT vulnerability management: **a repeatable process that achieves measurable and meaningful reductions of the attack surface.**

In this handbook, we outline the process, shaped by more than twenty years of experience in OT security consulting in everything from automotive factories to nuclear power plants. But a smart process alone is useless if you don't have the proper tools to execute. That is where the OTbase OT asset management software comes in. It's the predominant tool for achieving effective OT vulnerability management.

This handbook provides a clear understanding of the landscape and strategies to help you. You might have some questions along the way. Once you've read the handbook – visit [langner.com](https://www.langner.com) to learn more about OT Vulnerability Management and how OTbase can enable your strategy from implementation to mitigation to future planning.

Known Vulnerabilities Primer

Basic question first:

Where would one find a list of all vulnerabilities known to affect both IT and OT systems?

Answer:

The National Vulnerability Database (NVD). It is operated by the United States Department of Commerce's National Institute of Standards and Technology – NIST for short. It categorizes and archives all Common Vulnerabilities and Exposures (CVEs). You can access the NVD here:

<https://nvd.nist.gov/>

The most important thing to know is:

CVEs relate to products in a specific version, rather than to configuration flaws such as default passwords.

We're mostly referring to software or firmware products, but they also exist for some hardware products. A particularly infamous example for the latter is CVE-2016-8672, a vulnerability in the Siemens S7-400 controller family for which there is no fix, i.e. it can't be mitigated by firmware updates:

<https://nvd.nist.gov/vuln/detail/CVE-2016-8672>

But again, this is the exception to the rule. Most OT vulnerabilities affect specific firmware versions and can be mitigated by updates.

Let's take a step back. If CVEs are really all about certain product versions, it tells you that you don't need some hacker-style "vulnerability scanning" to identify CVEs in your installed base.

You need a correct, up-to-date account of installed software and firmware products, along with exact version details, to understand your attack surface.

For that reason, a detailed, comprehensive OT asset inventory of products and versions is mission-critical to OT vulnerability management. Without it, the quest for vulnerability reduction is a lost cause.

The screenshot displays the OTbase Inventory interface. On the left, there is a sidebar with navigation options: CVE, PROBLEMS, and AUDITS. The main area is split into two panes. The top pane, titled 'Attack Surface Map', shows a 3D bar chart representing the attack surface. Below it, a tooltip reads: 'Drag with mouse to move/rotate; mouse wheel to zoom; right-drag to pan; double click for profile'. The bottom pane shows a table of vulnerabilities with the following columns: Fixed, #Fixed, #Vulnerable, #Affected, CVE ID, Severity, VScore, Base Score, and Published. The table is filtered to show 'Vulnerable only' and contains 286 CVEs. The following table represents the data shown in the screenshot:

Fixed	#Fixed	#Vulnerable	#Affected	CVE ID	Severity	VScore	Base Score	Published
0	183	184	CVE-2019-0708	CRITICAL	1793.4	9.8	2019-05-16	
38	117	155	CVE-2017-8543	CRITICAL	1146.6	9.8	2017-08-15	
0	71	71	CVE-2023-23397	CRITICAL	695.8	9.8	2023-03-14	
0	69	69	CVE-2020-0646	CRITICAL	676.2	9.8	2020-01-14	
0	64	64	CVE-2022-4135	CRITICAL	614.4	9.6	2022-11-25	
0	63	63	CVE-2021-37973	CRITICAL	604.8	9.6	2021-10-08	
0	63	63	CVE-2022-3075	CRITICAL	604.8	9.6	2022-09-26	
0	63	63	CVE-2023-2136	CRITICAL	604.8	9.6	2023-04-19	
0	63	63	CVE-2021-30633	CRITICAL	604.8	9.6	2021-10-08	
0	62	62	CVE-2020-16017	CRITICAL	595.2	9.6	2021-01-08	
0	60	60	CVE-2016-4117	CRITICAL	588.0	9.8	2016-05-11	
0	60	60	CVE-2018-15982	CRITICAL	588.0	9.8	2019-01-18	
0	60	60	CVE-2018-4878	CRITICAL	588.0	9.8	2018-02-06	
0	60	60	CVE-2016-4171	CRITICAL	588.0	9.8	2016-06-16	
0	60	60	CVE-2016-1019	CRITICAL	588.0	9.8	2016-04-07	
0	60	60	CVE-2018-5002	CRITICAL	588.0	9.8	2018-07-09	
1	52	53	CVE-2020-1350	CRITICAL	520.0	10	2020-07-14	
0	40	40	CVE-2020-1472	MEDIUM	220.0	5.5	2020-08-17	
0	36	36	CVE-2020-1040	CRITICAL	324.0	9	2020-07-14	

List of known vulnerabilities that affect the installed base, along with CVSS scores and other information. This list is automatically updated every 24 hours.

Laying the Foundation: Tooling

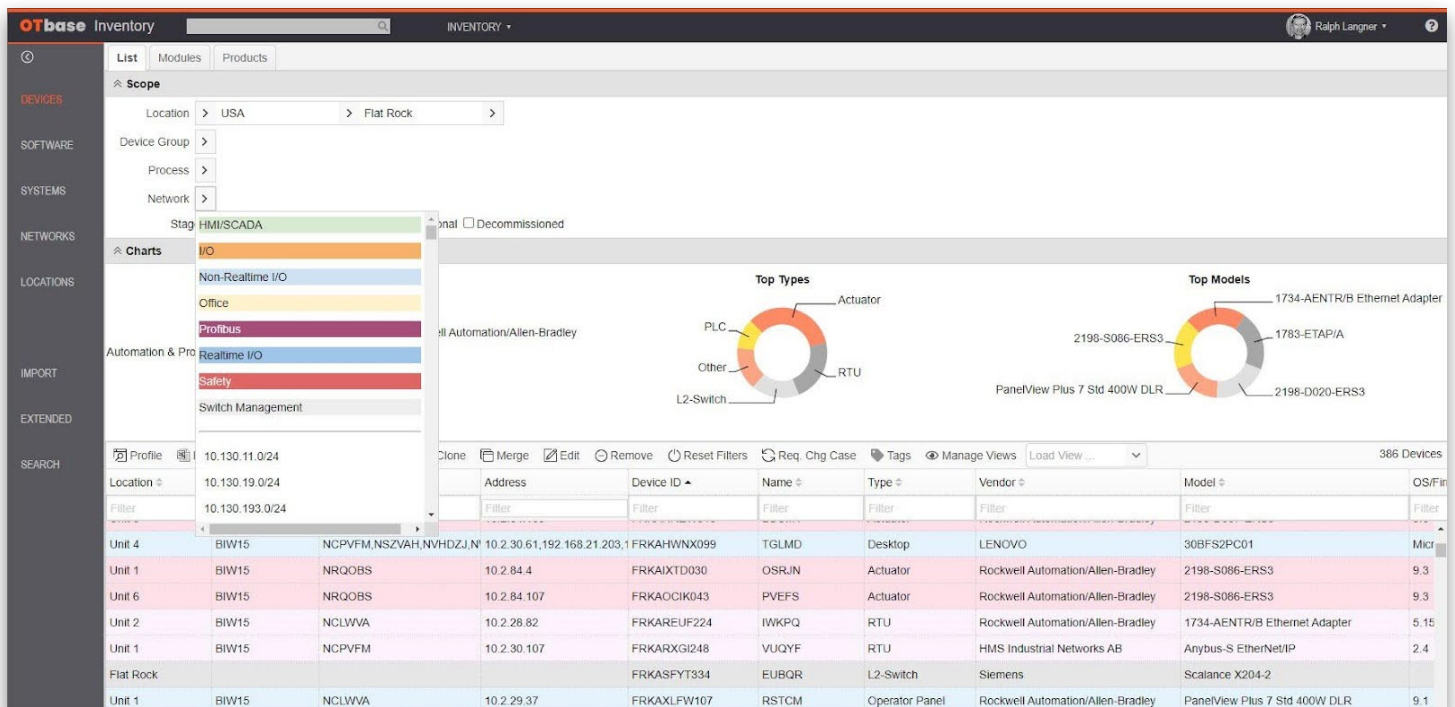
Since all CVEs are associated with specific product versions, you can't know which ones affect you if you don't have an asset inventory – and you can't know which vulnerabilities are already fixed. This simple truth is also reflected in the following statement:

“ Asset management is one of the most critical components of a vulnerability management program (VMP). Of all the fundamental building blocks of a successful VMP, it's crucial to get asset management right and complete before focusing on other aspects of vulnerability management. ”

Hughes, C., Robinson, N. (2024). Effective Vulnerability Management: Managing Risk in the Vulnerable Digital Ecosystem. Wiley

The reality is:

The lack of a comprehensive OT asset inventory is the number one root cause why most OT asset owners fail at OT vulnerability management.



The device inventory in OTbase. Asset information is detailed, up to date, and enriched with contextual metadata.

Most organizations approach OT vulnerability management like this:

- Somebody (maybe your boss) sends you an email that references a new CVE that was just pumped up in industry publications or social media. You are asked to check if you are affected by the CVE.
- You do your best to determine if your organization uses the affected products. That might be done by writing emails to local engineering and maintenance staff.
- Local staff try to figure out if they have the products mentioned, often by browsing Excel tables that somebody had created last year and were never updated.
- Weeks later you hear back from your friends in engineering and maintenance that some may use the affected products.
- You report to your boss that you might be affected by the CVE but have little means to verify. The boss is not happy.
- All you have accomplished is to demonstrate that your organization has no OT vulnerability management process.

So, there's no way around an automated OT asset inventory if you want to do OT vulnerability management for real. But that automation only helps you if the asset data that you get is both highly detailed and up to date.

For a long time, it was thought that creating such a comprehensive and detailed OT asset inventory was practically impossible. The well-known ICS Detection products, for example, don't get there, and for a simple technical reason. ICS Detection (or IDS, intrusion detection, anomaly detection, threat detection products as they are sometimes called) use "passive scanning", a type of scanning that sniffs network traffic from a SPAN port and parses it for data that can be used to identify end points and traffic patterns.

The problem is real-time network traffic only yields so much when it comes to identifying make, model, hardware version, installed firmware version on each I/O module etc. Let's face it: it's not like the process data that travels through typical OT networks would constantly expose this information. In many cases, it is never exposed.

That's why ICS Detection products that expose vulnerabilities slap a probability or likelihood on the vulnerability. Guess what? Such likelihoods don't exist in the CVE.

What you see as the likelihood of a vulnerability in a passive scanning product is nothing but the confidence with which make, model, version, and installed software was discovered.

That's not helpful, because you need to see reality to achieve effective OT vulnerability management. Guesswork isn't good enough.

To avoid that problem, OTbase uses active discovery and it does so exceptionally well. Active discovery probes all OT devices, including network switches and routers, Windows PCs, sensors and actuators, barcode readers and so on, using legitimate protocols and access credentials. It leverages the fact that virtually every relevant protocol in the OT space can query metadata from product identity over firmware versions to layer 2 network connectivity.

Since the discovery process in OTbase is automatically executed every 24 hours, you will also see configuration changes being recorded. Where those configuration changes indicate that a vulnerability is mitigated (such as installing security patches on a Windows PC), your vulnerability list is updated automatically. You have the essential tool for effective OT vulnerability management in your hands.

OTbase Device Profile FRKXDHMB210

Rockwell Automation **FRKXDHMB210 (JYKTN)**
 PLC
 Rockwell Automation/Allen-Bradley 1756-L71/B LOGIX5571

> General
 > Extended
 > Tags
 > Hardware

▼ Rack

Slot	Vendor	Model	Name	Version	Firmware	Serial Number	Order Number	Manufacture Date	Lifecycle Phase	Warranty	Description
1.0	Rockwell Automation/Allen-Bradley	1756-L71/B LOGIX5571			20.54	0x00D0BC3B			Active		Controller,ControlLogix,2 MB User Memory
1.1	Rockwell Automation/Allen-Bradley	1756-EN2TR/C			10.10	0x01058015			Active		EtherNet/IP communication module, dual p
1.2	Rockwell Automation/Allen-Bradley	1756-ENBT/A			6.6	0x00D34138			Discontinued		Communication Module,ControlLogix,Ether
1.3	Rockwell Automation/Allen-Bradley	1756-IB32/B DCIN			3.6	0x00D0EB73			Active		Input Module,ControlLogix,DC Digital,32 Pt
1.4	Rockwell Automation/Allen-Bradley	1756-OB16/A DCOU ^T ISOL			3.3	0xC0191905			Active		Output Module,ControlLogix,DC Digital,16
1.5	Rockwell Automation/Allen-Bradley	1756-OB16/A DCOU ^T ISOL			3.3	0xC01913F8			Active		Output Module,ControlLogix,DC Digital,16
1.6	Rockwell Automation/Allen-Bradley	1756-OW16/A RELAY n.o.			3.3	0xC0190623			Active		Output Module,ControlLogix,Relay Digital,1
1.7	Rockwell Automation/Allen-Bradley	1756-IF8/A			1.5	0x00D6833F			Active		Input Module,ControlLogix,Analog,8 Point,
1.8	Rockwell Automation/Allen-Bradley	1756-IF16/A			1.5	0x00D57B7A			Active		Input Module,ControlLogix,Analog,16 Point
1.9	Rockwell Automation/Allen-Bradley	1756-IRT8/A			2.12	0x4073FC7C			Active		RTD / Ohms / Thermocouple / mV Input Mc
1.10	Rockwell Automation/Allen-Bradley	1756-IRT8/A			2.12	0x4073FE0A			Active		RTD / Ohms / Thermocouple / mV Input Mc
1.11	Rockwell Automation/Allen-Bradley	1756-IRT8/A			2.12	0x01019525			Active		RTD / Ohms / Thermocouple / mV Input Mc
1.12	Rockwell Automation/Allen-Bradley	1756-CNB/E 11.005			11.5	0x00CD06C4			End of Life		Communication Module,ControlLogix,Cont

Sample device details for a Rockwell PLC rack. All details exposed, including highlighted outdated firmware versions, are discovered automatically.

Let's sum this up.

- Known vulnerabilities are always tied to specific products and versions.
- If you don't have a comprehensive, detailed, and up-to-date OT asset inventory, you have no practical way to know which CVEs affect you.
- If you do have such an asset inventory, however, the inventory can tell you right away which CVEs affect your installed base because the whole CVE database is loaded into the asset inventory automatically and updated daily.
- This process doesn't require any "vulnerability scan". It doesn't require anyone to press a button. It's a simple database operation that happens behind the scenes.
- It also gives you direct insight into your mitigation process.

Furnishing your Mitigation Strategy

Now we have the foundation for our vulnerability management, we need to decide what to do with the data. When you see all the unpatched vulnerabilities that affect your installed base, you will most likely be shocked.

A typical manufacturing operation with tens of thousands of OT devices usually faces several hundred thousand, if not over a million vulnerabilities.

That's not an exaggeration. It's not fear mongering. It's reality. Just think about it: NIST has cataloged more than 250,000 CVEs and any one of those can affect multiple devices. Since your typical OT asset fleet is oftentimes substantially old, and nobody bothered to patch or update the systems (because they are running just fine), your backlog of unresolved vulnerabilities is substantial. Rather than the typical IT landscape where you would expect mostly recent CVEs, OT vulnerabilities can go back a long time.

In the following table we have sorted vulnerabilities by CVE identifier, which contains the publication date. What you can see is that in that sample data set, unpatched vulnerabilities go back to 1999, the year MITRE & NIST started the NVD.

Will you ever be able to patch hundreds of thousands of vulnerabilities?
No, you won't. Ever.

A 2022 survey from Rezilion and the Ponemon Institute found 66% of respondents cited having a backlog of more than 100,000 vulnerabilities, and they were only able to patch less than half.

If IT can only patch less than 50,000 vulnerabilities from the backlog each year, how can OT be expected to patch greater than 500,000 vulnerabilities with fewer resources, especially when patches cannot be automatically applied? The answer is: Never. The only solution is to furnish an effective strategy.

An effective strategy allows you to arrive at meaningful reductions in your attack surface even though you'll only be able to mitigate a small fraction of all vulnerabilities that affect your installed base.

Luckily, OTbase comes to the rescue.

CVE	Device ID	Name	Type	Vendor	Model	Base Score	Risk Score	Fixed	Relevance	Patched	Vulnerable	Comment
CVE-1999-0142	KWR-10.DT2	Bob's workstation	Desktop	innotek GmbH	VirtualBox	7.5		x	Yes	x	Yes	
CVE-1999-0142	MDRZNIWJ007	YRFLT	Desktop	Dell Inc.	OptiPlex 780	7.5		x	Yes	x	Yes	
CVE-1999-0142	abc.Desktop1	PC87BN1	Desktop	Rockwell Software, Inc.	RSLinx Server	7.5		x	Yes	x	Yes	
CVE-1999-0153	KWR-10.DT2	Bob's workstation	Desktop	innotek GmbH	VirtualBox	5		x	Yes	x	Yes	
CVE-1999-0249	KWR-10.DT2	Bob's workstation	Desktop	innotek GmbH	VirtualBox	7.2		x	Yes	x	Yes	
CVE-1999-0293	KWR-10.L2-Switch1	Cisco2940	L2-Switch	Cisco	WS-C2940-8TT-S	7.5		x	Yes	x	Yes	
CVE-1999-0293	KWR-10.L2-Switch7	CiscoSF300	L2-Switch	Cisco Systems, Inc.	SRW208-K9	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYBMAZQ404	CFYIJ	L2-Switch	Cisco	WS-C4506-E	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYOWIRB405	MPEUZ	L2-Switch	Cisco	WS-C4506-E	7.5		x	Yes	x	Yes	
CVE-1999-0293	andreasimmW10.L2-Switch	Cisco2960	L2-Switch	Cisco Systems, Inc	WS-C2960CG-8TC-L	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYJFXRZ001	MDYTV	L2-Switch	Cisco Systems	WS-C6504-E	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYFMVJB112	ZGUDP	L2-Switch	Cisco Systems	WS-C6504-E	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYBHKML135	VWFAE	L2-Switch	Cisco	WS-C4506-E	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYDXOCA351	MGSFP	L2-Switch	Cisco	WS-C4506-E	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYRCFVY357	WJZJK	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYSAUGH359	DVREP	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYVNJML360	ZIUAC	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYEHBUA366	JORVI	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYKUHBJ369	RFJYS	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYBGCUR371	KXIQF	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		x	Yes	x	Yes	
CVE-1999-0293	GBYBUZFF373	TPMKD	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		x	Yes	x	Yes	

OT vulnerability management can be like archeology, when you discover unpatched vulnerabilities in your installed base that go back to when CVEs were first documented.

Prioritizing by likelihood of exploitation

For exercise purposes, let's say you have 700,000 vulnerabilities you've just found through OTbase. You know you'll only be able to mitigate 5,000 of these (insert your favorite number here), so the question is which ones do you focus on.

If you have dealt with vulnerability management before, you will most likely focus on CVE severity. This is a data field in the CVE information that expresses the "badness" of the CVE, as assessed by MITRE. Unfortunately, it doesn't yield much practical value for OT. What you want to focus on is the likelihood of exploitation. Consider the **following factors:**

- Existing exploit code in the wild
- Exploitation doesn't require local access but can be accomplished via routing
- Exploitation doesn't require a high attack complexity.

All this data is readily available in OTbase for every single CVE, and it can be used to reduce your result list with just a couple of mouse clicks.

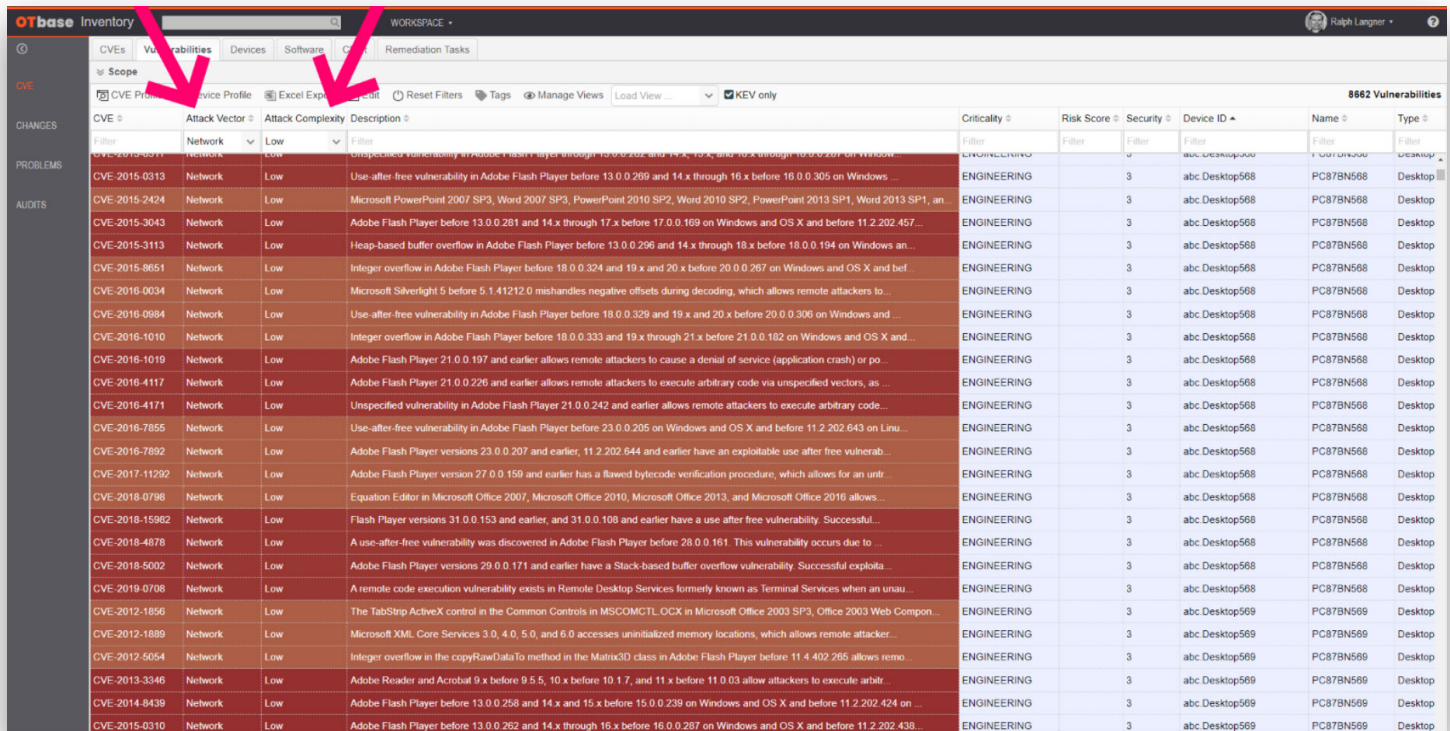
Let's start with CVEs with known exploits. Consider this:

“ Despite there being over 25,000 known vulnerabilities published in 2022, less than 1% of all these known vulnerabilities were exploited by malicious actors. This means that organizations are spending energy, effort, and resources on addressing vulnerabilities that never actually get exploited by malicious actors, and are trying to make sense of and prioritize the ones that have been or are likely to be exploited. ”

Hughes, C., Robinson, N. (2024). Effective Vulnerability Management: Managing Risk in the Vulnerable Digital Ecosystem. Wiley

If you know you will never be able to mitigate all OT vulnerabilities, why waste effort on those that might never see an exploit?

Here's how we can take advantage of this in practical terms. CISA maintains a list of such CVEs and that list is constantly updated. OTbase automatically downloads it every day. As a result, all you must do to filter for CVEs with known exploits is to check the "KEV" box. Done!



OTbase lets you filter vulnerabilities to only display those with known exploits – all it takes is checking a box.

Look at the screenshot above. Once we checked the "KEV" checkbox, the number of vulnerabilities went from more than 700,000 to less than 25,000. That's less than ideal, but something that can be addressed.

Another way to focus on the likelihood of exploitation is the question of whether routed network access is sufficient. To put it another way, a vulnerability that requires local system access, maybe even physical system access, is much less likely to be exploited in an OT environment. Logic dictates that you want to focus on those vulnerabilities for which routed network access is good enough. Luckily, this characteristic is exposed in the CVE information as the "access vector" and can be put to good use.

A similar CVE feature requires attack complexity. For example, a hard-coded password vulnerability is much easier to exploit than one that requires a ton of brute force. Required attack complexity is also coded in the CVE definition and is exposed by OTbase.

Along with required access, it gives you two excellent options to identify vulnerabilities that demand much more attention than those that either require local access or a highly sophisticated exploit code. Combine that with the KEV flag and you arrive at a vulnerability set that you should worry about. At the same time, you have removed tens of thousands of vulnerabilities that require super hackers to cause harm.

Using the means provided by OTbase to narrow down the likelihood of exploitation will allow you to arrive at a substantially reduced, much more meaningful vulnerability result set. This can be achieved within seconds by simply clicking the respective buttons in the OTbase vulnerability management workspace.

Prioritizing by system criticality

There's yet another strategy to further reduce your vulnerability result set. It is focusing on the cost of consequence.

Guess what? When it comes to devices, not all exploits are created equal.

For example, a nasty Windows vulnerability may affect both an office computer in the electrical workshop that is used by staff to do calculations and documentation and a SCADA server. Would you regard both systems as equally important? Most likely not. In the interest of prioritization, you would focus on the SCADA server while ignoring the office computer for the time being.

OTbase provides all the means necessary to establish and document system criticality. It can be assigned to a device level, a system level, or a network level. It even comes with the tools to help you identify hidden cyber-physical dependencies, thereby allowing you to arrive at solid criticality ratings. From there, you can focus on mitigating those systems where it makes a difference.

Device ID	Name	Type	Vendor	Model	OS/Firmware	Criticality	Exposure	#CVE	VScore	RScore
KWR-10.Desktop3	eng-station-b52	Desktop	Gigabyte Technology Co., Ltd.	GA-MA69G-S3H	Microsoft Windows 7 Professional	ENGINEERING	Public	107	887.4	5204.4
CLTBSPW1182	JVTOK	Virtual Machine	Rockwell Software, Inc.	RSLinx Server	Microsoft Windows 7 Enterprise	ENGINEERING		175	1472.5	2945.0
CLTJSOYI187	GAPNC	Virtual Machine	Rockwell Software, Inc.	RSLinx Server	Microsoft Windows 7 Enterprise	ENGINEERING		175	1472.5	2945.0
CLTFPARU185	KZILM	Virtual Machine	Rockwell Software, Inc.	RSLinx Server	Microsoft Windows 7 Enterprise	ENGINEERING		175	1472.5	2945.0
CLTRGQM183	SBZXV	Virtual Machine	VMware, Inc.	VMware Virtual Platform	Microsoft Windows 7 Enterprise	ENGINEERING		175	1472.5	2945.0
CLTSKEPA188	TGXFD	Virtual Machine	Rockwell Software, Inc.	RSLinx Server	Microsoft Windows 7 Enterprise	ENGINEERING		175	1472.5	2945.0
CLTTOBNF170	VRXIZ	Virtual Machine	Rockwell Software, Inc.	RSLinx Server	Microsoft Windows 7 Enterprise	ENGINEERING		175	1472.5	2945.0
CLTZBDSV186	PQGEQ	Virtual Machine	VMware, Inc.	VMware Virtual Platform	Microsoft Windows 7 Enterprise	ENGINEERING		175	1472.5	2945.0
CLTEKPTN184	MAZBC	Virtual Machine	Rockwell Software, Inc.	RSLinx Server	Microsoft Windows 7 Enterprise	ENGINEERING		175	1472.5	2945.0
DUREGPW1213	HZBAV	Virtual Machine	VMware, Inc.	VMware Virtual Platform	Microsoft Windows 7 Enterprise	ENGINEERING		172	1445.8	2891.6
FRKTQXMY273	HGKIV	Virtual Machine	VMware, Inc.	VMware Virtual Platform	Microsoft Windows 7 Enterprise	ENGINEERING		172	1445.8	2891.6
DURXMOID195	FSLAG	Virtual Machine	VMware, Inc.	VMware Virtual Platform	Microsoft Windows 7 Enterprise	ENGINEERING		172	1445.8	2891.6
DURWISJG204	HEBRO	Virtual Machine	VMware, Inc.	VMware Virtual Platform	Microsoft Windows 7 Enterprise	ENGINEERING		172	1445.8	2891.6
FRKNPLWX271	GZSQO	Virtual Machine	VMware, Inc.	VMware Virtual Platform	Microsoft Windows 7 Enterprise	ENGINEERING		172	1445.8	2891.6
DURXWMPG200	CYRJA	Virtual Machine	VMware, Inc.	VMware Virtual Platform	Microsoft Windows 7 Enterprise	ENGINEERING		172	1445.8	2891.6
FRKGHTZ269	CYWDF	Virtual Machine	VMware, Inc.	VMware Virtual Platform	Microsoft Windows 7 Enterprise	ENGINEERING		172	1445.8	2891.6

Once that SMEs have tagged devices as critical, OTbase automatically elevates their risk score.

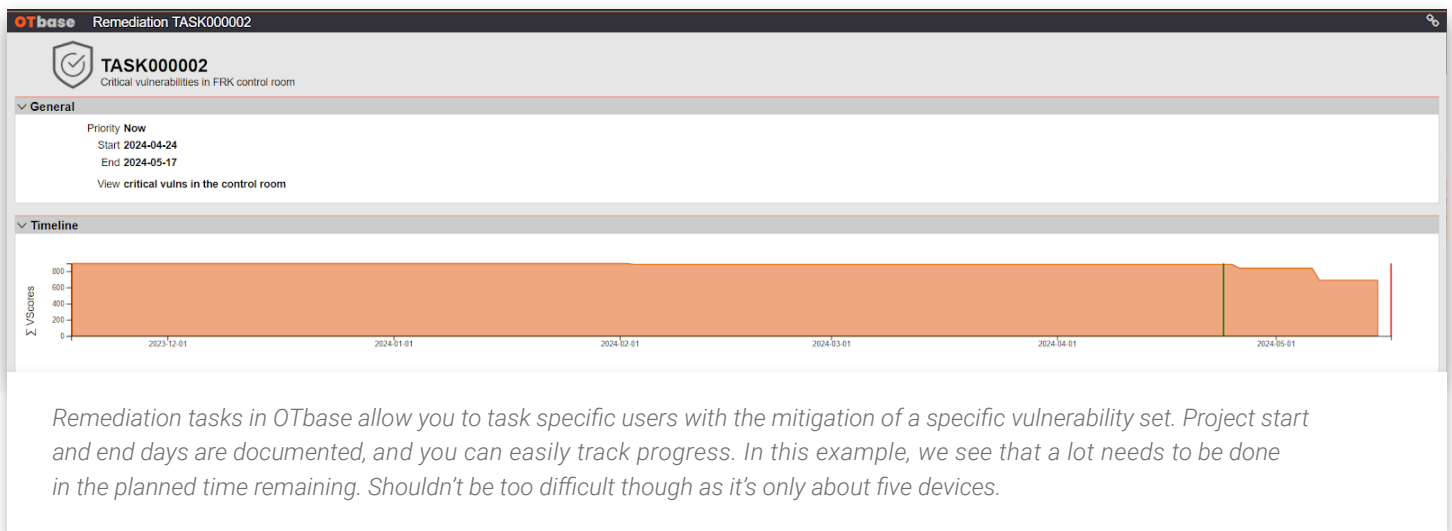
Plan and Execute

At this point, powerful metrics are in play that let you identify those vulnerabilities that you want/need to address – the vulnerabilities that allow for the most meaningful risk reduction in the shortest amount of time. Which is exactly what management expects.

The next step is to put that into some kind of planning framework, which you find in the OT vulnerability management workspace in OTbase. Here, you can assign individual risk scores to specific vulnerabilities, i.e. on a device level. Even better, you can open remediation tasks where you assign vulnerabilities to specific users for mitigation.

In this workflow, you can also specify a planned end date when you expect the task to be finished, along with context information in the form of comments or even file attachments. All referenced users will automatically see “their” vulnerabilities they’re supposed to mitigate, be it in the form of patching, compensating controls (usually network security), or hardening.

The necessity for planning cannot be overstated. Consider that when it comes to regulation, most regulatory frameworks don’t require you to achieve measurable risk reduction, but they do require you to demonstrate the existence of an organized and documented approach toward vulnerability management.



The screenshot displays the OTbase interface for a remediation task. The task is titled "TASK000002" and is described as "Critical vulnerabilities in FRK control room". The "General" section shows a priority of "Now", a start date of "2024-04-24", and an end date of "2024-05-17". A link is provided to "View critical vulns in the control room". The "Timeline" section features a bar chart showing the number of vulnerability scores over time. The y-axis is labeled "Σ V/scores" and ranges from 0 to 800. The x-axis shows dates from 2023-12-01 to 2024-05-01. A vertical green line marks the end of the remediation task on 2024-05-01. The chart shows a high, steady level of scores until the end date, after which the scores drop significantly, indicating progress in remediation.

Remediation tasks in OTbase allow you to task specific users with the mitigation of a specific vulnerability set. Project start and end days are documented, and you can easily track progress. In this example, we see that a lot needs to be done in the planned time remaining. Shouldn't be too difficult though as it's only about five devices.

Monitor and Report Progress

Turns out, management often isn't as humble as regulators. And even if you aren't subject to cyber security regulations, here's a job performance golden rule to follow:

You must document progress. Otherwise, you'll easily lose thrust, and management support (translation: budget).

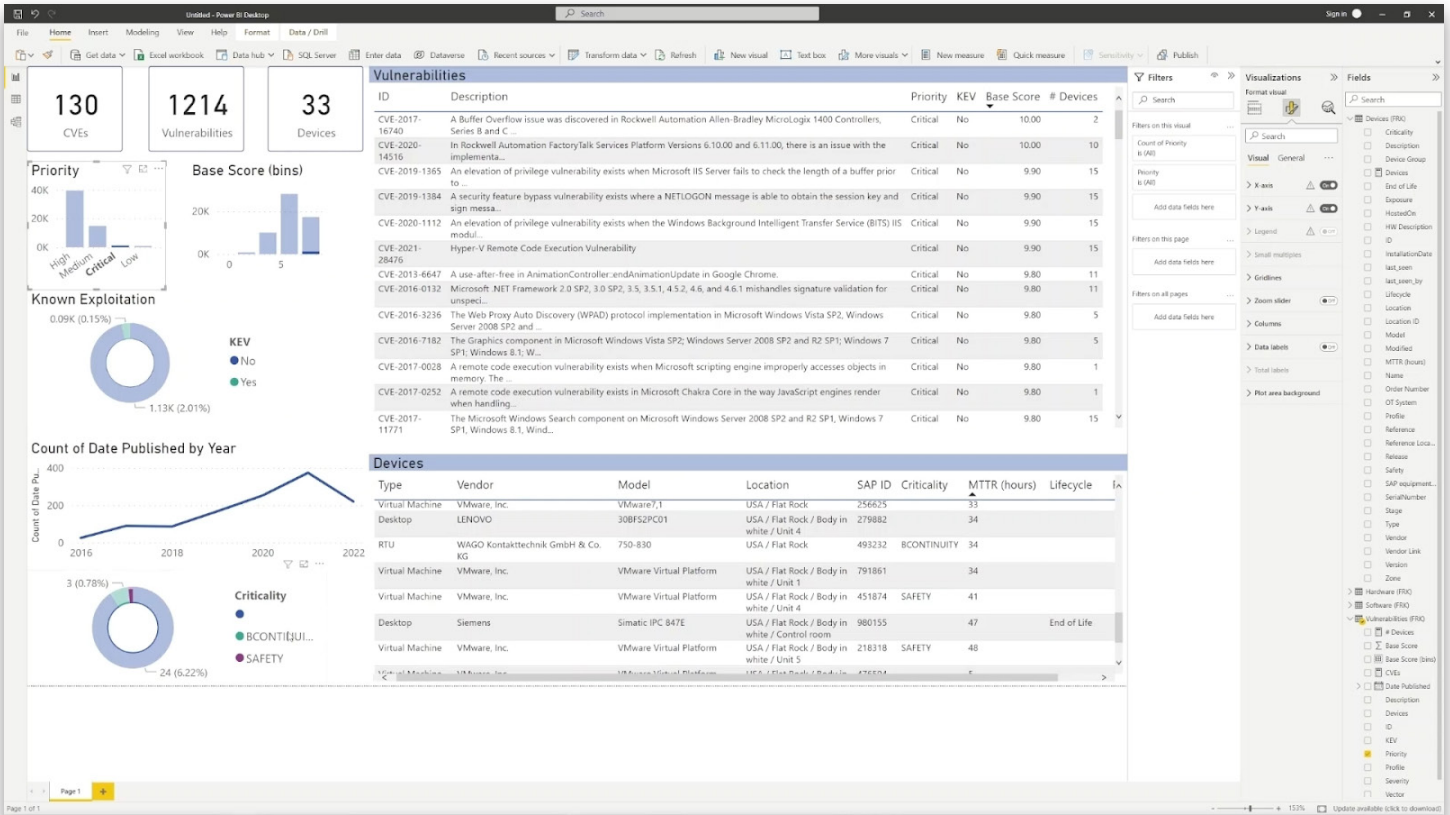
Consider the following:

- Do your mitigation efforts yield a reduction of the attack surface?
- How much?
- Will you be finishing your mitigation tasks on time, or is it totally hopeless with given resources?
- What's the present situation, and when do you plan to arrive at the target state?

Without specific and robust answers to these questions, you are dead in the water when the time comes to answer to management.

Fortunately, the OTbase OT asset management software provides all the necessary data points. You can see those in reports, dashboards, tables, etc. But that isn't always digestible information for everyone in your organization.

When it comes time to present progress updates to management, easy-to-understand, awesome dashboards **are needed**. To create that CISO dashboard, we suggest using Microsoft's Power BI, which is nicely integrated with OTbase. Using the tool and the corporate standards they expect from you shows management you are on top of the game.



Creating a CISO dashboard is best done in the platform that top management loves. With the OTbase Connector for Power BI, it's a snap.

Conclusion

Consider why you downloaded this handbook for a second.

You know you need OT vulnerability management, and you are:

- doing it but not successfully, or (and more likely the case)
- you have no idea how to start.

Everything you've read in this handbook lays out the landscape AND an actionable path forward. We've shown you the proper approach and strategy. Now all you need is the proper tool and execution. Show your team and your management that there's a clear path out of risk, fear, and doubt. Implement effective OT vulnerability management in your organization and reap the benefits.

About OTbase

OTbase is the first OT security and documentation tool not designed with hackers in mind, but with you – the user. It is a pure-play OT asset management system. OTbase makes users more productive – users in engineering, auditing, cyber security, plant planning, and related fields. To learn more about why OT asset management is a product category in its own right, please check out [this blog post](#).

