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	
Introduction	
Known Vulnerabilities Primer	5
Laying the Foundation: Tooling	
Furnishing your Mitigation Strategy	
Prioritizing by likelihood of exploitation	
Prioritizing by system criticality	
Plan and Execute	
Monitor and Report Progress	
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 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 <u>products</u> 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.

otbase li	nventory	Q WORKSPACE →								💄 TaVon	ne Harris 🗸 🛛 🚱
©		🛄 demo.ot-base.com 🔒									
	otbase	Attack Surface Map									
CVE			only Vulnera	ble only							286 CVE
PROBLEMS			Fixed =	#Fixed =	#Vulnerable	#Affected ©	CVE ID 🗘	Severity \$	VScore \$	Base Score \$	Published =
				Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
AUDITS				0	183	184	CVE-2019-0708	CRITICAL	1793.4	9.8	2019-05-16
	Drag with me	ouse to move/rotate; mouse wheel to zoom; right-drag to pan; double click for profile		38		155	CVE-2017-8543	CRITICAL	1146.6	9.8	2017-06-15
				0		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
	Critical	Integer overflow in Skia in Google Chrome prior to 112.0.5615.137 allowed a remote attack		0	63	63	CVE-2023-2136	CRITICAL	604.8	9.6	2023-04-19
	Critical	Use after free in Indexed DB API in Google Chrome prior to 93.0.4577.82 allowed a remote		0	63	63	CVE-2021-30633	CRITICAL	604.8	9.6	2021-10-08
	Critical	Use after free in site isolation in Google Chrome prior to 86.0.4240.198 allowed a remote at		0	62	62	CVE-2020-16017	CRITICAL	595.2	9.6	2021-01-08
	Critical	Adobe Flash Player 21.0.0.226 and earlier allows remote attackers to execute arbitrary code		0	60	60	CVE-2016-4117	CRITICAL	588.0	9.8	2016-05-11
	Critical	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have a use after free		0	60	60	CVE-2018-15982	CRITICAL	588.0	9.8	2019-01-18
	Critical	A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This		0	60	60	CVE-2018-4878	CRITICAL	588.0	9.8	2018-02-06
	Critical	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier allows remote attacke		0	60	60	CVE-2016-4171	CRITICAL	588.0	9.8	2016-06-16
	Critical	Adobe Flash Player 21.0.0.197 and earlier allows remote attackers to cause a denial of serv		0	60	60	CVE-2016-1019	CRITICAL	588.0	9.8	2016-04-07
	Critical	Adobe Flash Player versions 29.0.0.171 and earlier have a Stack-based buffer overflow vulr		0	60	60	CVE-2018-5002	CRITICAL	588.0	9.8	2018-07-09
	Critical	A remote code execution vulnerability exists in Windows Domain Name System servers whe		1	52	53	CVE-2020-1350	CRITICAL	520.0	10	2020-07-14
	Critical	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlo		0	40	40	CVE-2020-1472	MEDIUM	220.0	5.5	2020-08-17
	Critical	A remote code execution vulnerability exists when Hyper-V RemoteFX vGPU on a host serv		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.

OTbase In	nventory		Q	INVEN	TORY -					Ralph Langner	• 0			
©	List Module:	s Products												
DEVICES	Location	> USA	> Flat Rock		>									
SOFTWARE	Device Group	>												
	Process	>												
SYSTEMS	Network	>												
	Stag	HMI/SCADA			Decommissioned									
NETWORKS		1/0												
LOCATIONS		Non-Realtime I/O					Top Types			Top Models				
Controllo		Office					Act	uator		1734-AENTR/B Ethernet Ada				
		Profibus		II Autor	nation/Allen-Bradley	PLC			2408 2086 ED22	_ 1783-ETAP/A				
	Automation & Pro	Realtime I/O												
IMPORT		Safety				Other	RT	U	PanelView Plus 7 Std 400W DLR	2405 D020 ED02				
EXTENDED		Switch Managemen	ıt			L2-Switch				2196-D020-ER35				
CATCHOLD														
SEARCH	Profile 🖷 I	10.130.11.0/24		Clone	Merge ZEdit ORei	move () Reset Filters	Req. Chg Case	e 🖣 Tags 💿 Mar	age Views Load View V		386 Devices			
	Location ¢	10.130.19.0/24			Address	Device ID -	Name \$	Type \$	Vendor \$	Model ¢	OS/Fin			
	Filter	10.130.193.0/24		•	Filter	Filter	Filter	Filter	Filter	Filter	Filter			
	Unit 4	BIW15	NCPVFM,NSZVAH,1	WHDZJ,N	10.2.30.61,192.168.21.203,1	FRKAHWNX099	TGLMD	Desktop	LENOVO	30BFS2PC01	Micr			
	Unit 1	BIW15	NRQOBS		10.2.84.4	FRKAIXTD030	OSRJN	Actuator	Rockwell Automation/Allen-Bradley	2198-S086-ERS3	9.3			
	Unit 6	BIW15	NRQOBS		10.2.84.107	FRKAOCIK043	PVEFS	Actuator	Rockwell Automation/Allen-Bradley	2198-S086-ERS3	9.3			
	Unit 2	BIW15	NCLWVA		10.2.28.82	FRKAREUF224	IWKPQ	RTU	Rockwell Automation/Allen-Bradley	1734-AENTR/B Ethernet Adapter	5.15			
	Unit 1	BIW15	NCPVFM		10.2.30.107	FRKARXGI248	VUQYF	RTU	HMS Industrial Networks AB	Anybus-S EtherNet/IP	2.4			
	Flat Rock					FRKASFYT334	EUBQR	L2-Switch	Siemens	Scalance X204-2				
	Unit 1	BIW15	NCLWVA		10.2.29.37	FRKAXLFW107	RSTCM	Operator Panel	Rockwell Automation/Allen-Bradley	PanelView Plus 7 Std 400W DLR	9.1			

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.

otb	use Device Profile FRKXI	DHMB210									~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
R Auto	PLC Rockwell Automation/Alle	IO (JYKTN) n-Bradley 1756-L71/B LOGIXS	5571								
> Ger	neral										
> Ext	ended										
> Tag	S										
> Har	dware										
∨ Rac	:k										
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 Pc
1.4	Rockwell Automation/Allen-Bradley	1756-OB16I/A DCOUT ISOL			3.3	0xC0191905			Active		Output Module,ControlLogix,DC Digital,16
1.5	Rockwell Automation/Allen-Bradley	1756-OB16I/A DCOUT ISOL			3.3	0xC01913F8			Active		Output Module,ControlLogix,DC Digital,16
1.6	Rockwell Automation/Allen-Bradley	1756-OW16I/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-IRT8I/A			2.12	0x4073FC7C			Active		RTD / Ohms / Thermocouple / mV Input Mc
1.10	Rockwell Automation/Allen-Bradley	1756-IRT8I/A			2.12	0x4073FE0A			Active		RTD / Ohms / Thermocouple / mV Input Mc
1.11	Rockwell Automation/Allen-Bradley	1756-IRT8I/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,Contr
4											•

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.

OTbase	nventory		<u>२</u> ४	ORKSPACE -									Ralph Langner 🔹 📀
	CVEs Vulnera	abilities Devices Softwa	are Chart Re	mediation Tasks	3								
	⊗ Scope												
	反 CVE Profile	Device Profile 🖷 Excel E	Export 🖉 Edit (CReset Filters	Tags Manage Views	Load View 🗸	KEV only						724847 Vulnerabilities
CHANGES	CVE -	Device ID \$	Name 0	Type 🗘	Vendor ‡	Model \$	Base Score 4	Risk Score ¢	Fixed 🗘	Relevance \$	Patched 0	Vulnerable	Comment
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter	Filter
	CVE-1999-0142	KWR-10.DT2	Bob's workstation	Desktop	innotek GmbH	VirtualBox	7.5		×	Yes	×	Yes	
	CVE-1999-0142	MDRZNIWJ007	YRFLT	Desktop	Dell Inc.	OptiPlex 780	7.5		×	Yes	×	Yes	
	CVE-1999-0142	abc.Desktop1	PC87BN1	Desktop	Rockwell Software, Inc.	RSLinx Server	7.5		×	Yes	×	Yes	
	CVE-1999-0153	KWR-10.DT2	Bob's workstation	Desktop	innotek GmbH	VirtualBox	5		×	Yes	×	Yes	
	CVE-1999-0249	KWR-10.DT2	Bob's workstation	Desktop	innotek GmbH	VirtualBox	7.2		×	Yes	×	Yes	
	CVE-1999-0293	KWR-10.L2-Switch1	Cisco2940	L2-Switch	Cisco	WS-C2940-8TT-S	7.5		×	Yes	×	Yes	
	CVE-1999-0293	KWR-10.L2-Switch7	CiscoSF300	L2-Switch	Cisco Systems, Inc.	SRW208-K9	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYBMAZQ404	CFYIJ	L2-Switch	Cisco	WS-C4506-E	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYOWIRB405	MPEUZ	L2-Switch	Cisco	WS-C4506-E	7.5		×	Yes	×	Yes	
	CVE-1999-0293	andreastimmW10.L2-Switch	Cisco2960	L2-Switch	Cisco Systems, Inc	WS-C2960CG-8TC-L	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYJFXRZ001	MDYTV	L2-Switch	Cisco Systems	WS-C6504-E	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYFMVJB112	ZGUDP	L2-Switch	Cisco Systems	WS-C6504-E	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYBHKML135	VWFAE	L2-Switch	Cisco	WS-C4506-E	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYDXOCA351	MGSFP	L2-Switch	Cisco	WS-C4506-E	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYRCFYV357	WJDZK	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYSAUGH359	DVREP	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYVNJML360	ZIUAC	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYEHBUA366	JORVI	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYKUHBZ369	RFJYS	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYBGCRU371	KXIQF	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		×	Yes	×	Yes	
	CVE-1999-0293	GBYYBUZF373	TPMKD	L2-Switch	Cisco Systems, Inc	WS-C3850-24S-E	7.5		×	Yes	×	Yes	

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!

OT base	Inventory		Q	WORKSPACE +					Ralph Langne	r• 0
©	CVEs Vu	abilities Device	es Software	Contemporaries Remediation Tasks						
	⊗ Scope									
CVE	D CVE Prom	evice Profile	Excel Expo	edit 🕐 Reset Filters 🕒 Tags @ Manage Views Load View 🗸 🗸 🗹 KEV only					8662 V	ulnerabilities
CHANGES	CVE 0	Attack Vector 0	Attack Complexity	Description	Criticality 0	Risk Score 4	Security 0	Device ID +	Name 0	Type ©
GIPHIGEO	Filter	Network ~	Low ~				Filter			
PROBLEMS	OVE-2013-0311	NEWIOIK	LOW	топъресние и чинетарину и лиоре с назит науст и порун то у о 202 ани 14 х, то х, ано то х инорун то о о 207 он типори	ENGINEERING		5	auc.Desktop300	1 COTDINUOU	DESKID
	CVE-2015-0313	Network	Low	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
AUDITS	CVE-2015-2424	Network		Microsoft PowerPoint 2007 SP3, Word 2007 SP3, PowerPoint 2010 SP2, Word 2010 SP2, PowerPoint 2013 SP1, Word 2013 SP1, an	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2015-3043	Network	Low	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2015-3113	Network	Low	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.296 and 14.x through 18.x before 18.0.0.194 on Windows an	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2015-8651	Network		Integer overflow in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and bef	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2016-0034	Network		Microsoft Silverlight 5 before 5.1.41212.0 mishandles negative offsets during decoding, which allows remote attackers to	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2016-0984	Network		Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2016-1010	Network		Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2016-1019	Network	Low	Adobe Flash Player 21.0.0.197 and earlier allows remote attackers to cause a denial of service (application crash) or po	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2016-4117	Network	Low	Adobe Flash Player 21.0.0.226 and earlier allows remote attackers to execute arbitrary code via unspecified vectors, as	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2016-4171	Network	Low	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier allows remote attackers to execute arbitrary code	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2016-7855	Network		Use-after-free vulnerability in Adobe Flash Player before 23.0.0.205 on Windows and OS X and before 11.2.202.643 on Linu	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2016-7892	Network		Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerab	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2017-11292	Network		Adobe Flash Player version 27.0 0.159 and earlier has a flawed bytecode verification procedure, which allows for an untr	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2018-0798	Network		Equation Editor in Microsoft Office 2007, Microsoft Office 2010, Microsoft Office 2013, and Microsoft Office 2016 allows	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2018-15982	Network	Low	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have a use after free vulnerability. Successful	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2018-4878	Network	Low	A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2018-5002	Network		Adobe Flash Player versions 29.0.0.171 and earlier have a Stack-based buffer overflow vulnerability. Successful exploita	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2019-0708	Network	Low	A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unau	ENGINEERING		3	abc.Desktop568	PC87BN568	Desktop
	CVE-2012-1856	Network		The TabStrip ActiveX control in the Common Controls in MSCOMCTL.OCX in Microsoft Office 2003 SP3, Office 2003 Web Compon	ENGINEERING		3	abc.Desktop569	PC87BN569	Desktop
	CVE-2012-1889	Network	Low	Microsoft XML Core Services 3.0, 4.0, 5.0, and 6.0 accesses uninitialized memory locations, which allows remote attacker	ENGINEERING		3	abc.Desktop569	PC87BN569	Desktop
	CVE-2012-5054	Network		Integer overflow in the copyRawDataTo method in the Matrix3D class in Adobe Flash Player before 11.4.402.265 allows remo	ENGINEERING		3	abc Desktop569	PC87BN569	Desktop
	CVE-2013-3346	Network	Low	Adobe Reader and Acrobat 9 x before 9.5.5.10 x before 10.1.7 and 11 x before 11.0.03 allow attackers to execute arbitr	ENGINEERING		3	abc Desktop569	PC87BN569	Desktop
	CVE-2014-8439	Network	Low	Adobe Flash Player before 13 0 0 258 and 14 x and 15 x before 15 0 0 239 on Windows and OS X and before 11 2 202 424 on	ENGINEERING		3	abc Desktop569	PC87BN569	Desktop
	CVE-2015-0310	Network	Low	Adobe Flash Player before 13.0.0.262 and 14 x through 16 x before 16.0.0.287 on Windows and OS X and before 11.2.202.438	ENGINEERING		3	abc Desktop569	PC87BN569	Desktop

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.

OTbase	nventory		Q	WORKSPACE -					Ģ	Ralph La	ingner 🔻	0
©	CVEs Vulnerabil	lities Devices	Software Chart	Remediation Tasks								
	⊗ Scope											
CVE	Profile 🗟 Exce	el Export 🛛 🖉 Edit	() Reset Filters	🔓 Req. Chg Case 🛛 🔍 Tags 💿 Man	age Views Load View 🗸 🗸	KEV only					538 Devi	vices
CHANGES	Device ID \$	Name \$	Type \$	Vendor ‡	Model \$	OS/Firmware \$	Criticality \$	Exposure \$	#CVE ≑	VScore	RScore -	
	Filter	Filter	Filter	Filter	Filter	Filter	Filter	~	Filter	Filter	Filter	
PROBLEMS	KWR-10.Desktop3	eng-station-b52	Desktop	Gigabyte Technology Co., Ltd.	GA-MA69G-S3H	Microsoft Windows 7 Professional	ENGINEERING	Public	107	867.4	5204.4	Â
	CLTBSPWI182	JVTOK	Virtual Machine	Rockwell Software, Inc.	RSLinx Server	Microsoft Windows 7 Enterprise	ENGINEERING		175	1472.5	2945.0	
AUDITS	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	
	CLTIRGQM183	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	PQGEO	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	
	DUREGPWI213	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	HEBRQ	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	
	FRKUGHTZ269	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.



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.

			Vulnerabilit	ies							√ Filters	@ >>	Visualizations	>>	Fields
130	1214	33	ID	Description				Priority	KEV Base Score	# Devices	A ,O Search		Format visual	Ø	₽ Search
CVEs	Vulnerabilities	Devices	CVE-2017- 16740	A Buffer Overflow issue was discovered Series B and C	in Rockwell Automation Allen	-Bradley MicroLogix 1400 Cont	rollers,	Critical	No 10.00	2	Filters on this vis	ual		S.	✓ ■ Devices (FR)
CVLS	Vullerabilities	Devices	CVE-2020- 14516	In Rockwell Automation FactoryTalk Ser implementa	vices Platform Versions 6.10.0	0 and 6.11.00, there is an issue	with the	Critical	No 10.00	10	Count of Priorit Is (All)	α.	Visual Genera		Desc
ority 🗌 🖓	Base Se	core (bins)	CVE-2019-1365	An elevation of privilege vulnerability et	ists when Microsoft IIS Server	fails to check the length of a b	uffer prior	Critical	No 9.90	15	Priority Is (All)			-	Devi
	204		CVE-2019-1384	A security feature bypass vulnerability e sign messa	xists where a NETLOGON me	sage is able to obtain the sessi	on key and	Critical	No 9.90	15	Add data	fields here	> Y-asis		End Expe
	206	_	CVE-2020-1112	An elevation of privilege vulnerability et modul	rists when the Windows Backg	round Intelligent Transfer Servi	ice (BITS) IIS	Critical	No 9.90	15			> Legend	A (000)	Hos
an in inter	рі ОК		CVE-2021- 28476	Hyper-V Remote Code Execution Vulne	rability			Critical	No 9.90	15	Filters on this pa	ge	> Small multiples		D ID
Medio criere Co	0	5	CVE-2013-6647	A use-after-free in AnimationController	endAnimationUpdate in Goo	gle Chrome.		Critical	No 9.80	11	Add 6ata	tielps nere	Cristian		🗌 last,
wn Exploitat	tion		CVE-2016-0132	Microsoft .NET Framework 2.0 SP2, 3.0 unspeci	5P2, 3.5, 3.5.1, 4.5.2, 4.6, and 4	.6.1 mishandles signature valid	ation for	Critical	No 9.80	11	Filters on all pag	e	> Zoom slider	(0.07)	Life
.09K (0.15%) —			CVE-2016-3236	The Web Proxy Auto Discovery (WPAD) Server 2008 SP2 and	protocol implementation in N	ficrosoft Windows Vista SP2, W	indows	Critical	No 9.80	5	Add data	fields here	> Columns		Loca
	к	EV .	CVE-2016-7182	The Graphics component in Microsoft V SP1; Windows 8.1; W	Vindows Vista SP2; Windows S	Server 2008 SP2 and R2 SP1; Wi	ndows 7	Critical	No 9.80	5			> Data labels		Mor
		No	CVE-2017-0028	A remote code execution vulnerability e memory. The	xists when Microsoft scripting	engine improperly accesses of	bjects in	Critical	No 9.80	1			> Total labels		Nam
	•	162	CVE-2017-0252	A remote code execution vulnerability e	xists in Microsoft Chakra Core	in the way JavaScript engines	render	Critical	No 9.80	1			> Plot area backgr	ound	
	- 1 10V (2 010/)			when handling											
	└─ 1.13K (2.01%)		CVE-2017- 11771	when handling The Microsoft Windows Search compor SP1, Windows 8.1, Wind	ient on Microsoft Windows Se	erver 2008 SP2 and R2 SP1, Win	dows 7	Critical	No 9.80	15	~				Profi Refe
int of Date Pu	ublished by Year		CVE-2017- 11771	when handling The Microsoft Windows Search compor SP1, Windows 8.1, Wind	ient on Microsoft Windows Se	over 2008 SP2 and R2 SP1, Win	dows 7	Critical	No 9.80	15	*				Profi Refe Refe Refe Refe
int of Date Pu	⊔ 1.13K (2.01%)		CVE-2017- 11771 Devices	when handling The Microsoft Windows Search compor SP1, Windows 8.1, Wind Vendor	ent on Microsoft Windows Se Model	rver 2008 SP2 and R2 SP1, Win	dows 7	Critical	No 9.80	15	v.				Profi
nt of Date Pu	⊔ 1.13k (2.01%)	\wedge	CVE-2017- 11771 Devices Type	When handling The Microsoft Windows Search compor SP1, Windows 8.1, Wind	ent on Microsoft Windows Se Model	rver 2008 SP2 and R2 SP1, Win Location	dows 7 SAP ID	Critical Criticality	No 9.80 MTTR (hours)	15 Lifecycle	v IA				Profi Refe Refe Safe SAP
nt of Date Pu	Lished by Year	\wedge	CVE-2017- 11771 Devices Type Virtual Machine Desktop	when handling The Microsoft Windows Search compor SP1, Windows 8.1, Wind Vendor VMware, Inc. LENOVO	ent on Microsoft Windows Se Model VMware7,1 308F52PC01	Iver 2008 SP2 and R2 SP1, Win Location USA / Flat Rock USA / Flat Rock / Body in	dows 7 SAP ID 256625 279882	Critical Criticality	No 9.80 MTTR (hours) 33 34	15 Lifecycle	Y In				Prof Refe Refe Safe Safe Safe Sag Sag
nt of Date Pu	2018	2020 2022	CVE-2017- 11771 Devices Type Virtual Machine Desktop RTU	when handing The Microsoft Windows Search compor SPI, Windows 8.1, Wind Vendor VMware, Inc. LENGWO WIGO Kontakttechnik GmbH & Co.	ent on Microsoft Windows Se Model VMware?,1 308F52PC01 750-830	Location USA / Flat Rock / Body in white / Unit 4 USA / Flat Rock / Body in white / Unit 4	dows 7 SAP ID 256625 279882 493232	Critical Criticality BCONTINUITY	No 9.80 MTTR (hours) 33 34 7 34	15 Lifecycle	* In				Prof. Rafa Rafa Safa Safa Safa Sag Sag Ven
nt of Date Pu 00 00 0 2016 2.00 7000	2018	2020 V C 2022	CVE-2017- 11771 Devices Type Virtual Machine Desktop RTU Virtual Machine	when handling. The Microsoft Windows Search compor SPI, Windows 8.1, Wind Vendor VMware, Inc. LENOVO WAGO Kontakteehnik GmbH & Co. KG VMware, Inc.	ent on Microsoft Windows Se Model VMware7,1 308FS2PC01 750-830 VMware Virtual Platform	Location USA / Flat Rock USA / Flat Rock / Body in white / Unit A USA / Flat Rock / Body in white / Unit A	dows 7 SAP ID 256625 279882 493232 791861	Critical Criticality BCONTINUITY	MTTR (hours) 33 34 34 34 34	15 Lifecycle	in .				Profi Refe Refe Refe Safe Safe Safe Sug Sug Venc Venc Zon
nt of Date Pu 00 00 00 2016 3 (0.78%)	2018	2020 و 2022 کر کی 2022	CVE-2017- 11771 Devices Type Virtual Machine Desktop RTU Virtual Machine Virtual Machine	when handling. The Microsoft Windows Search compor SPI, Windows 8.1, Wind Vendor VMware, Inc. LENOVO WAGO Kontakteehnik GmbH & Co. KG VMware, Inc. VMware, Inc.	ent on Microsoft Windows Se Model VMware/,1 306f22/C01 750-830 VMware Virtual Platform VMware Virtual Platform	Ver 2008 SP2 and R2 SP1, Win USA / Har Rock USA / Har Rock USA / Flat Rock USA / Flat Rock USA / Flat Rock / Body in white / Unit 1 USA / Flat Rock / Body in	dows 7 SAP ID 256625 279882 493232 791861 451874	Critical Criticality BCONTINUITY SAFETY	No 9.80 MTTR (hours) 33 34 34 34 41	15 Lifecycle	In				 ○ Prof. Refe Refe Safe Safe Sag Type Vens Vens Vens Zons > Imacharan
nt of Date Pu 0 0 2016 3 (0.78%)	2018	2020 v @ 2022	CVE-2017- 11771 Devices Type Virtual Machine Desktop RTU Virtual Machine Desktop	when handling. The Microsoft Windows Search compor SPI, Windows 8.1, Wind Vendor VMware, Inc. LENOVO WAGO Kontakteehnik GmbH & Co. KG VMware, Inc. VMware, Inc. Siemens	ent on Microsoft Windows Se Model VMware/,1 306f22/201 750-830 VMware Virtual Platform VMware Virtual Platform Simatic IPC 847E	Ver 2008 SP2 and R2 SP1, Win USA / Har Rock USA / Har Rock USA / Flat Rock USA / Flat Rock / Body in white / Unit 1 USA / Flat Rock / Body in white / Unit 1 USA / Flat Rock / Body in white / Unit 4	dows 7 SAP ID 256625 279882 493232 791861 451874 980155	Critical Criticality BCONTINUITY SAFETY	No 9.80 MTTR (hours) 33 34 34 34 34 41 47	15 Lifecycle End of Life	in .				 Profil Refer Refer Refer Selet <l< td=""></l<>
nt of Date Pu 0 0 2016 3 (0.78%)	2018	2020 2022 viticality BCONTILIUL	CVE-2017- 11771 Devices Type Virtual Machine Desktop RTU Virtual Machine Virtual Machine Desktop Virtual Machine	when handling The Microsoft Windows Search compor SPI, Windows 8.1, Wind Vendor VMware, Inc. LENOVO WAGO Kontakttechnik GmbH & Co. KG VMware, Inc. VMware, Inc. Siemens VMware, Inc.	ent on Microsoft Windows Se Model VMware7,1 306f52PC01 750-830 VMware Virtual Platform VMware Virtual Platform Simatic IPC 847E VMware Virtual Platform	Ver 2008 SP2 and R2 SP1, Win USA / Hat Rock USA / Hat Rock USA / Hat Rock USA / Hat Rock USA / Hat Rock / Body in white / Unit 1 USA / Hat Rock / Body in white / Unit 1 USA / Hat Rock / Body in white / Control room USA / Flat Rock / Body in	dows 7 SAP ID 256625 279882 493232 791861 451874 980155 218318	Critical Criticality BCONTINUITY SAFETY SAFETY	No 9.80 MTTR (hours) 33 34 34 34 41 47 48	15 Lifecycle End of Life	En .				 Pool Refe Refe Refe Refe Sele <l< td=""></l<>
nt of Date Pu 2010 3 (0.78%)	2018	2020 2022 Viticality BCONTILUI SAFETY	CVE-2017- 11771 Devices Type Virtual Machine Desktop Virtual Machine Desktop Virtual Machine	when handling The Microsoft Windows Search comport SPI, Windows E.1, Wind Vendor VMware, Inc. LENOVO WMGO Kontaktechnik GmbH & Co. KG VMware, Inc. Siemens VMware, Inc.	ent on Microsoft Windows Se Model VMware7,1 306/52/PC01 750-830 VMware Virtual Platform VMware Virtual Platform Simatic IPC 847E VMware Virtual Platform 100-000 Platform Platform	USA / Flat Rock / Body in With Christ Rock / Body in White / Unit 4 USA / Flat Rock / Body in White / Unit 4 USA / Flat Rock / Body in White / Unit 1 USA / Flat Rock / Body in White / Control room USA / Flat Rock / Body in White / Control room USA / Flat Rock / Body in White / Unit 3	dows 7 SAP ID 256625 279882 493232 493232 493232 493232 218318 218318 47000	Critical Criticality BCONTINUITY SAFETY SAFETY	MTTR (hours) 33 34 34 41 47 48 r	15 Lifecycle End of Life	× In				
ont of Date Pu 00 0 2016 3 (0.78%)	2018	2020 ⊋ @ 2022 riticality BECONTILJUL SAFETY	CVE-2017- 11771 Devices Type Virtual Machine Desktop Virtual Machine Desktop Virtual Machine	when handling the Microsoft Windows Search compore SPI, Windows & 1, Wind Vendor VVMoare, Inc. LENOVO WMGO Kontaktechnik GmbH & Co. KG VVMware, Inc. Siemens VVMware, Inc. 1184	ent on Microsoft Windows Se Model Whave?1 308752PC01 750-830 VMware Virtual Platform Simatic IPC 847E VMware Virtual Platform 184-ware Virtual Platform	Location USA / Flat Rock USA / Flat Rock USA / Flat Rock USA / Flat Rock / Body in white / Unit A USA / Flat Rock / Body in white / Unit 1 USA / Flat Rock / Body in white / Unit 1 USA / Flat Rock / Body in white / Cont / Rody in	dows 7 SAP ID 256625 279882 493232 493232 493232 493232 218318 218318 475501	Critical Criticality BCONTINUITY SAFETY SAFETY	No 9.80 MTTR (hours) 33 34 34 34 41 47 48 r	15 Lifecycle End of Life	n N				Prof. Refer Refer Refer Refer Refer Refer Status Status Status Status Status Status Status Status Vend
nt of Date Pu 00 0 2016 3 (0.78%)	2018	2020 2022 Viticality BCONTI(JUL SAFETY	CVE-2017- 11771 Devices Type Virtual Machine Desktop Virtual Machine Desktop Virtual Machine Virtual Machine	when handling The Microsoft Windows Search compor SPI, Windows 8.1, Wind Vendor VMMare Inc. LINOVO WMGO Kontaktechnik GmbH & Co. KG VMware, Inc. Siemens VMware, Inc.	ent on Microsoft Windows Se Model VMware/1 306F22C01 750-830 VMware Virtual Platform VMware Virtual Platform Simatic IPC 847E VMware Virtual Platform 19.0-xxx1/idual Platform	Ver 2008 SP2 and R2 SP1, Win Location USA/ Har Rock USA/ Har Rock USA/ Flat Rock / Body in white / Unit 4 USA/ Flat Rock/ Body in white / Unit 4 USA/ Flat Rock/ Body in white / Chart I com USA/ Flat Rock/ Body in white / Chart I com USA/ Flat Rock/ Body in white / Chart I com	dows 7 SAP ID 256625 279882 493232 791861 451874 980155 218318 476504	Critical Criticality BCONTINUITY SAFETY SAFETY	No 9.80 MTTR (hours) 33 34 34 41 47 48 r	15 Lifecycle End of Life	*				Profit Profi
nt of Date Pu 00 0 2016 3 (0.78%)	2018	2020 2022 2022 2022 2022 riticality BCONTI[JUI SAFETY	CVE-2017- 11771 Type Virtual Machine Deaktop Virtual Machine Virtual Machine Virtual Machine Virtual Machine Cestop Virtual Machine	when handling The Microsoft Windows Search comport SPI, Windows & I, Wind Vendor ViMware, Inc. LINOVO WMCO Kontaktechnik GmbH & Co. KG VMware, Inc. Siemens VMware, Inc.	ent on Microsoft Windows Se Model VMware/1 308/52PC01 750-830 VMware Virtual Platform VMware Virtual Platform Simatic IPC 847E VMware Virtual Platform	Ver 2008 SP2 and R2 SP1, Win USA / Flat Rock USA / Flat Rock USA / Flat Rock / Body in white / Link 4 USA / Flat Rock / Body in white / Link 1 USA / Flat Rock / Body in white / Link 1 USA / Flat Rock / Body in white / Link 1 USA / Flat Rock / Body in white / Link 5 UFA / Flat Rock / Body in white / Link 5	dows 7 SAP ID 256625 279882 493232 791861 451874 980155 218318 476501	Critical Criticality BCONTINUITY SAFETY SAFETY	No 9.80 MTTR (hours) 33 34 34 34 41 47 48 r	15 Lifecycle End of Life	v				> Prof. - Refs. - Refs. - Refs. - Refs. - Setter
nt of Date Pu 00 00 00 00 00 00 00 00 00 00 00 00 00	2018	2020 v i i i i 2022 v i i i i i i i i i i i i i i i i i i i	CVE-2017- 11771 Devices Type Virtual Machine Desitop RTU Virtual Machine Desitop Virtual Machine Desitop Virtual Machine	Wen handling The Microsoft Windows Search compor SPI, Windows & J, Wind Vendor VUMoare, Inc. LENOVO WWGO Kontaktechnik GmbH & Co. KG VUMware, Inc. Siemens VUMware, Inc.	ent on Microsoft Windows Se Model VMware/1 308752PC01 750-830 VMware Virtual Platform VMware Virtual Platform Simatic IPC 847E VMware Virtual Platform	Ver 2008 SP2 and R2 SP1, Win LOCATION USA/ Flat Rock USA/ Flat Rock	SAP ID 256625 279882 493232 791861 451874 980155 218318 476504	Critical Criticality BCONTINUITY SAFETY SAFETY	No 9.80 MTR (hours) 33 34 34 34 34 34 34 34 34 34 34 34 34	15 Lifecycle End of Life	v				 Prof. Prof. Ref. Ref. Ref. Ref. Serie Ser
nt of Date Pu 00 0 2016 3 (0.78%)	2018	2020 2022 V D Initicality BCONTILIUI SAFETY	CVE-2017- 11771 Type Virtual Machine Desktop RrU Virtual Machine Virtual Machine Desktop Virtual Machine	when handling The Microsoft Windows Search comport SPI, Windows E.1, Wind Vendor VMware, Inc. LENOVO WKGK Sontaktechnik GmbH & Co. KG VMware, Inc. Siemens VMware, Inc.	ent on Microsoft Windows Se Model VMware/,1 306/52/PC01 750-830 VMware Virtual Platform Simatic IPC 847E VMware Virtual Platform 1978-see Virtual Platform	Ver 2008 SP2 and R2 SP1, Win USA / Har Rock USA / Har Rock / Body in white / Unit 1 USA / Har Rock / Body in white / Unit A USA / Har Rock / Body in white / Control from white / Unit A USA / Har Rock / Body in white / Unit A	dows 7 SAP ID 256625 279882 493232 791861 451874 980155 218318 476504	Critical Criticality BCONTINUITY SAFETY SAFETY	No 9.80 33 34 34 34 47 47 48 47 48	15 Lifecycle End of Life					Prof Arriver Arriver Arriver Arriver Serie Ser
nt of Date Pt 00 0 2016 3 (0.78%)	2018	2020 ⊋ @ 2022 riticality BECONTILJUL SAFETY	CVE-2017- 11771 Type Virtual Machine Desktop RTU Virtual Machine Desktop Virtual Machine Desktop Virtual Machine	when handling The Microsoft Windows Search compor SPI, Windows & 1, Wind Vendor V/Mware, Inc. LENOVO WKGG Contaktechnik GmbH & Co. KG V/Mware, Inc. Siemens V/Mware, Inc.	ent on Microsoft Windows Se Model Whate?1 308752PC01 750-830 VMare Virtual Platform Simatic IPC 847E VMare Virtual Platform 1984-res Virtual Platform	USA / Flat Rock USA / Flat Rock USA / Flat Rock USA / Flat Rock / Body in white / Unit A USA / Flat Rock / Body in white / Unit A USA / Flat Rock / Body in white / Unit A USA / Flat Rock / Body in white / Unit A USA / Flat Rock / Body in white / Cont / Rody in white / Cont /	dows 7 SAP ID 256625 279882 493232 791861 451874 980155 218318 476504	Critical Criticality BCONTINUITY SAFETY SAFETY	No 9.00 33 33 34 34 34 4 34 4 41 4 42 4 43 4 44 4 45 4 46 4	15 Lifecycle End of Life	v				 Profit Refer Refer Refer Refer Selection Sele

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.**

