



A Comprehensive Guide to Industrial Device Patching

Costs vs. Benefits Insights from the Research Lab

A SCADAfence Research Original Publication

Ofer Shaked, Co-Founder and CTO, SCADAfence

Ofer Shaked – Speaker Profile

- ☰ Co-Founder & CTO of SCADAfence
- ☰ 13 years background in SCADA / Industrial Security
- ☰ Ex-officer in the Israeli Intelligence Elite Cyber Unit
- ☰ Architect in the OTCSA
- ☰ Advisory Board member at ManuSec
- ☰ Speaker at ICS Security Conferences



Table of Contents

01



Chapter 1

The Costs of Patching
Vulnerability
Discovery
Patching Devices

02



Chapter 2

The Benefits of
Patching

03



Chapter 3

Conclusions

04

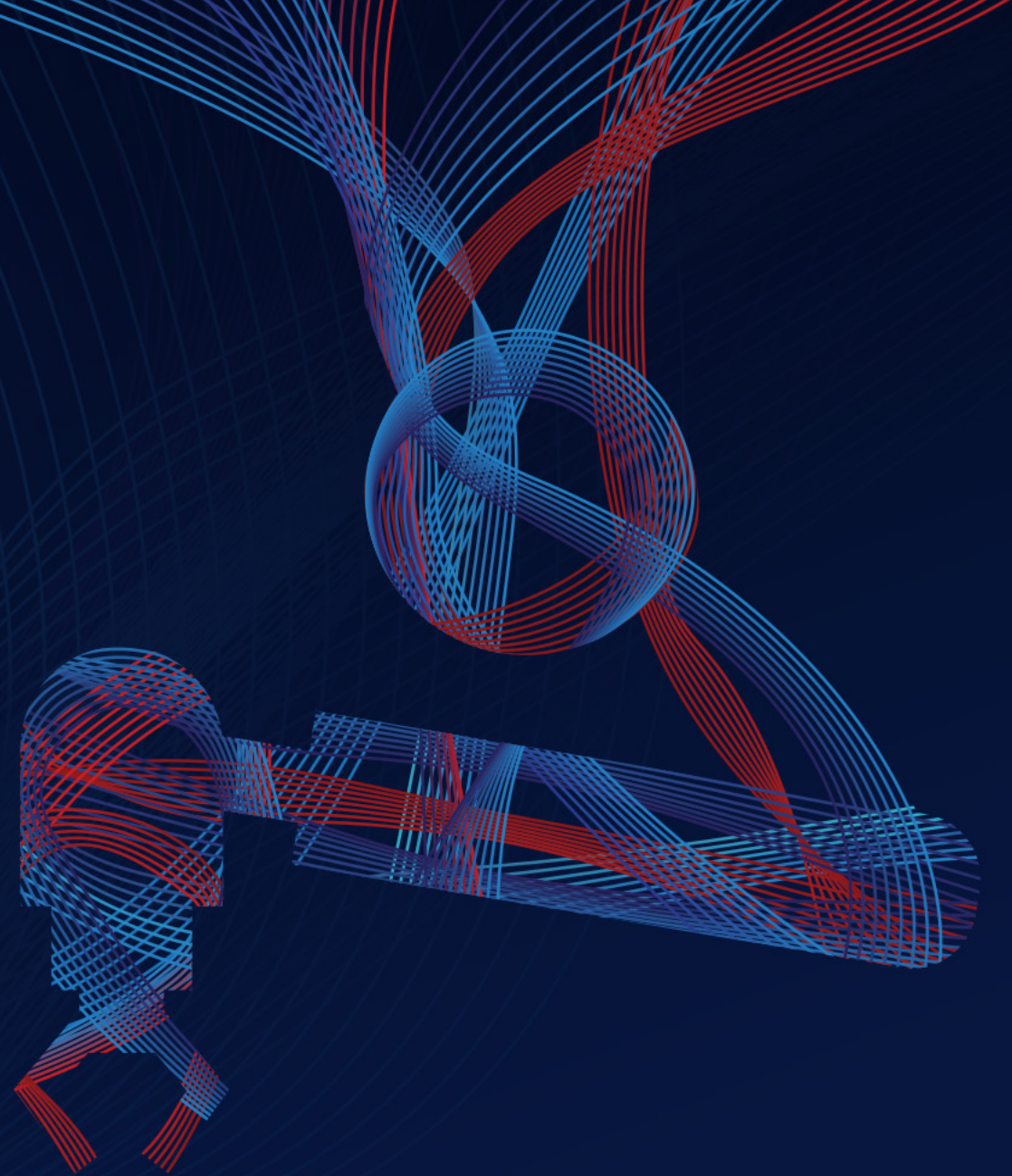


Chapter 4

A Decision Making Tool
for Vulnerability
Management

The Cost of Patching

Step 1: Vulnerability Discovery



Industrial Device Vulnerability Management Processes

To know if you have a vulnerability, you first need to discover all your assets. You then need to assess them for vulnerabilities.



Case Studies: Vulnerability Scanning

Case Study #1

Automotive Manufacturer in Germany

Critical servers crashed in production from scanning for one critical vulnerability. The servers were a key part of the manufacturing process and their failure caused downtime.

Cause: The scanner opened 13 sockets while the servers only supported up to 4 sockets in parallel.

Case Study #2

BMS Operator in the US

Over 50% of the building automation systems crashed as a result of a network-wide scan using one of the top 3 Vulnerability Scanners.

Fixing it required calling technicians from multiple vendors to the affected sites.

Monetary cost to repair - \$1Million.

Cause: The scanner triggered a functionality that isn't in common use and wasn't properly tested on the target devices by the vendors.

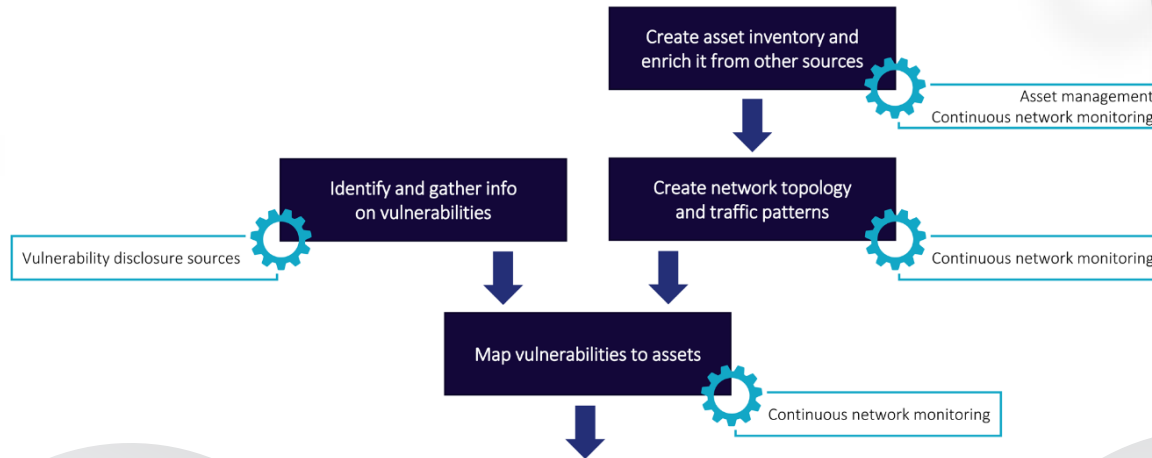
Conclusion

Vulnerability scanning is unfit for scanning in OT.



Four Steps To Safe Vulnerability Discovery

Step 1:
Create an Asset
Inventory
(passive & active
sources).



Step 2:
Perform Network
Mapping to
understand which
assets are
reachable and
from where.

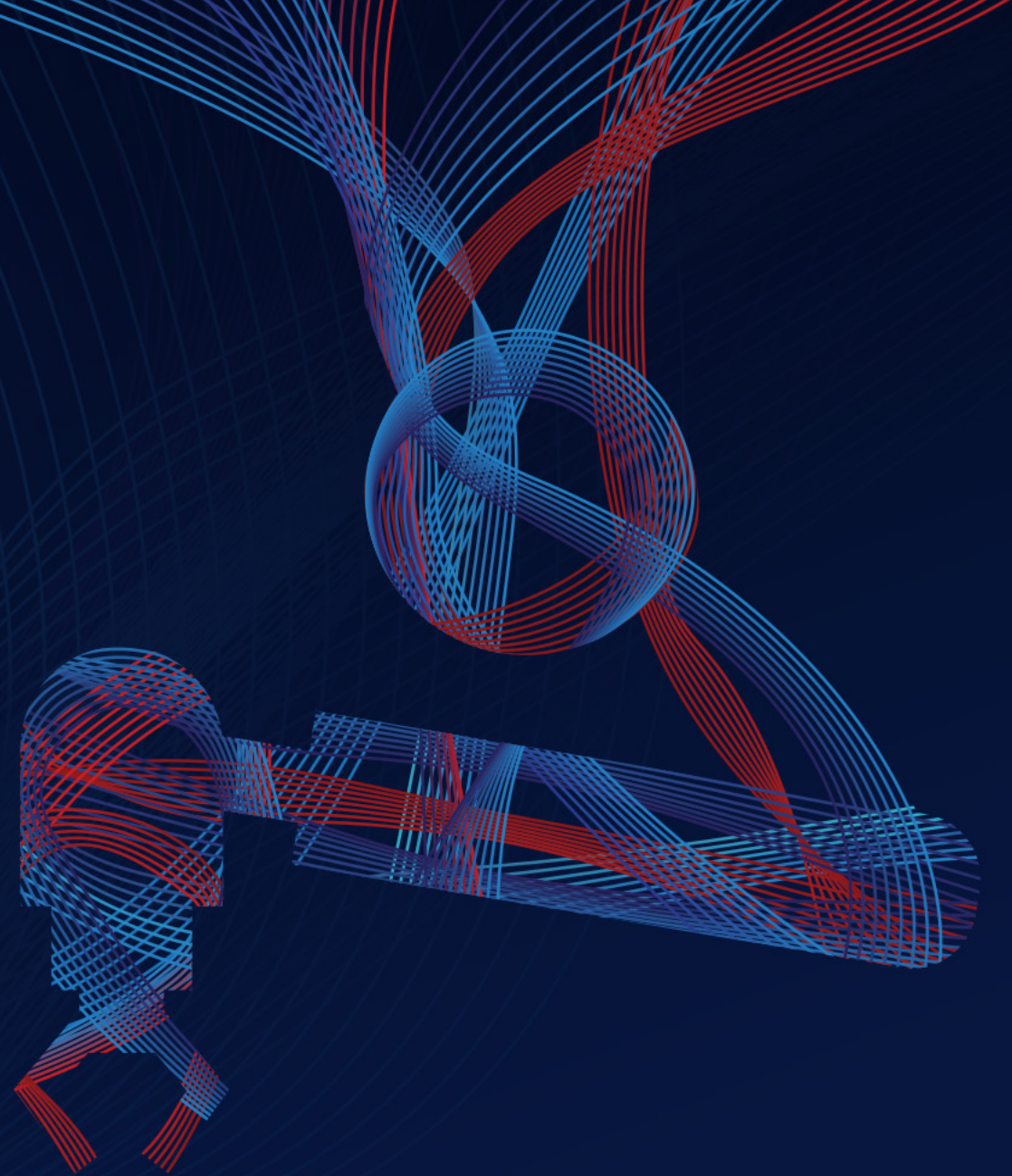
Step 3:
Gather
vulnerabilities
from vulnerability
disclosure
sources.

Step 4:
Map
vulnerabilities
to assets.

Source: OTCSA Position Paper: "Vulnerability Management for Operational Technology"

The Cost of Patching

Step 2: Patching Devices



How Many Patches are Required Per Device?

Case Study: Siemens SIMATIC S7-1500 CPU

The screenshot shows the Siemens Security Advisories search interface. The search term 's7-1500 cpu' is entered in the search bar. The results table shows 23 entries, with the first 15 displayed. The second entry, 'Denial-of-Service Vulnerabilities in SIMATIC S7-1500 CPU Family', is highlighted. The search results are filtered to show 15 of 23 entries.

ID	CVSS Score	Document Title	Info	Version	Last Update	Download
SSA-179516	5.9	OpenSSL Vulnerability in Industrial Products	i	V1.6	2020-02-10	PDF TXT
SSA-180635	7.5	Denial-of-Service Vulnerabilities in SIMATIC S7-1500 CPU Family	i	V1.1	2020-02-10	PDF TXT
SSA-307392	7.5	Denial-of-Service in OPC UA in Industrial Products	i	V1.6	2020-03-10	PDF TXT
SSA-616472	6.5	ZombieLoad and Microarchitectural Data Sampling Vulnerabilities in Industrial Products	i	V1.6	2020-03-10	PDF TXT

Showing 1 - 15 from 23 entries (Filtered)

Source: Siemens Security Advisories



23 Security Advisories

Siemens SIMATIC S7-1500 CPU – 23 security advisories

83% Require Patching

19 out of the 23 Entries are CPU vulnerabilities that require patching

Multiple Vulnerabilities

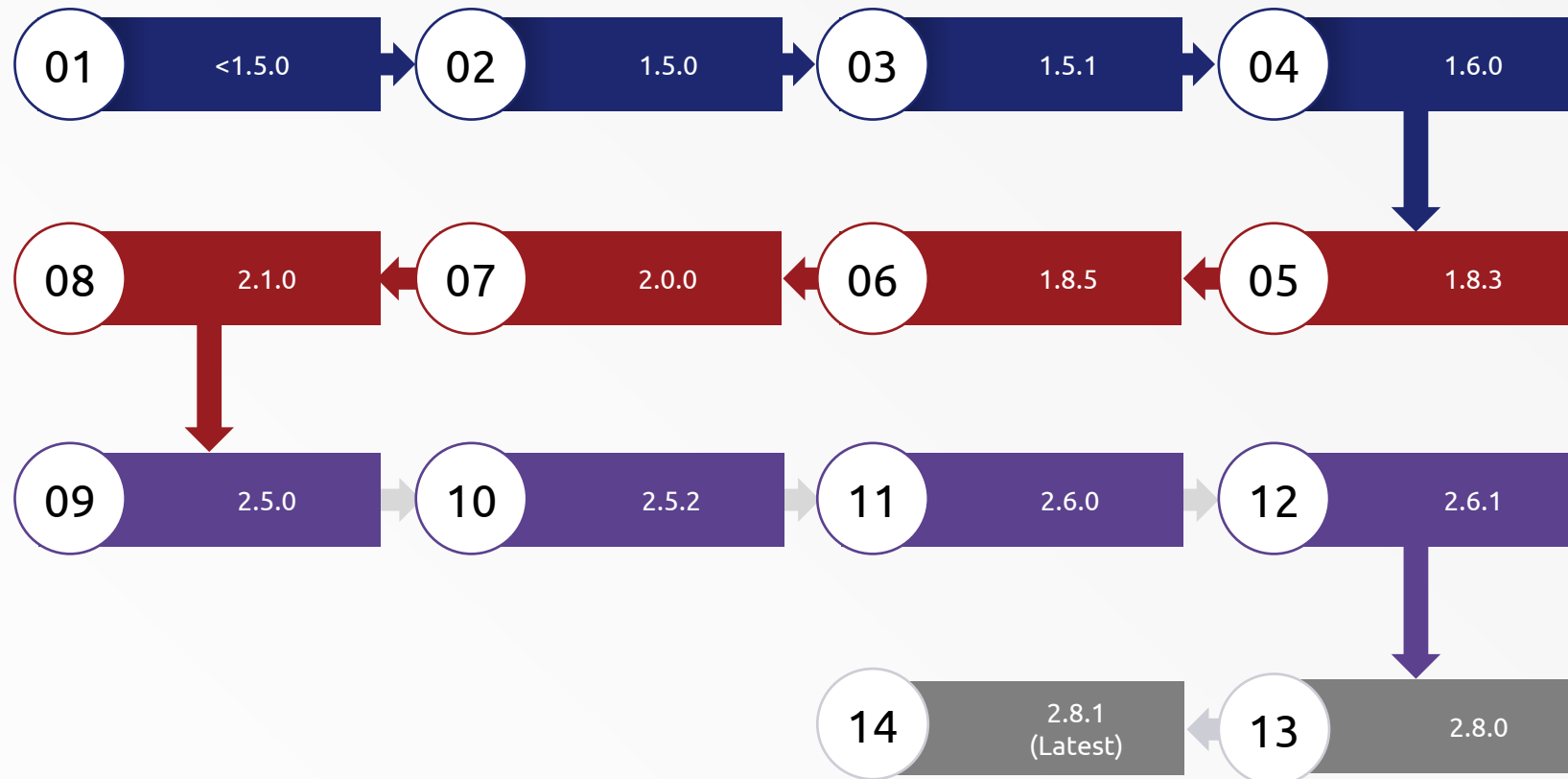
Some of the 19 entries contain multiple vulnerabilities

Notice

The product is used as an example to an industry-wide problem, it is not specific to one product or vendor.

Siemens SIMATIC S7-1500 CPU – Required Security Patches

In 7 years since its launch, 13 updates per S7-1500 device were required, in order to stay fully patched.



Conclusion: Staying fully patched requires frequent attention per device.


The Cost of Applying Patches - #1

Upgrade Failure

A user tried to upgrade the firmware on a Siemens SIMATIC S7-1500 CPU, resulting in an error in downloading programming into the PLC.


Downgrade Failure

When the user tried to downgrade – he bricked the device.



11/28/2013 1:37 PM ▶ Rate ☆☆☆☆☆ (0)

Red John



Advanced Member

Joined: 3/7/2013
Last visit: 4/28/2020
Posts: 30
Rating: ☆☆☆☆☆ (0)

Hi

i have a S7 1500 with TP 900 and a ET200 mp.

i recently upgraded the firmware which then didnt allow me to download anything to the PLC.
i then tried to downgrade to my inital firmware and now the PLC is unresponsive.

It appears to be wiped clean with no trace of any parameters.
and now it does not want to update my inital firmware.

Please help

Tyger! Tyger! burning bright
In the forests of the night...

> Suggestion > To thank Answer Quote ^

The Cost of Applying Patches - #2

Loss of Communication

Another user tried to patch a Rockwell Automation / Allen Bradley Micro830 PLC device and lost communication with the device.

Loss of Time & Money

That cost him \$200 & wasted his time. The cost for an enterprise rolling out a large patch and – could end up costing millions!



Vladimir Romanov • 2nd
McGill MBA 2021 | Control Systems & Automation Consultant | Electrical Engi...
1h • 🌐

I had a very interesting experience with a Micro830 PLC from Rockwell Automation today.

After reading so many positive reviews from my colleagues, I decided to go ahead and purchase a unit for myself. Before receiving the unit, I installed the software (which is free) and downloaded the proper firmware revising of ControlFlash.

Once the PLC arrived, I plugged it in over USB (No EtherNet on the micro830), initiated a firmware flash just as I've done countless times and the flash failed.

Sure enough, the PLC was still visible in the RSLinx tree, but I could no longer flash or communicate with it.

Upon searching on the web, it was clear that there is a "common occurrence" of such events when flashing over USB. There seems to be no indication as to why this occurs or solution from the manufacturer.

I am now an extremely disappointed owner of a 200\$ paperweight.

Are these just as unreliable in the field?

#controls #PLC #automation #Rockwell

The Conclusion

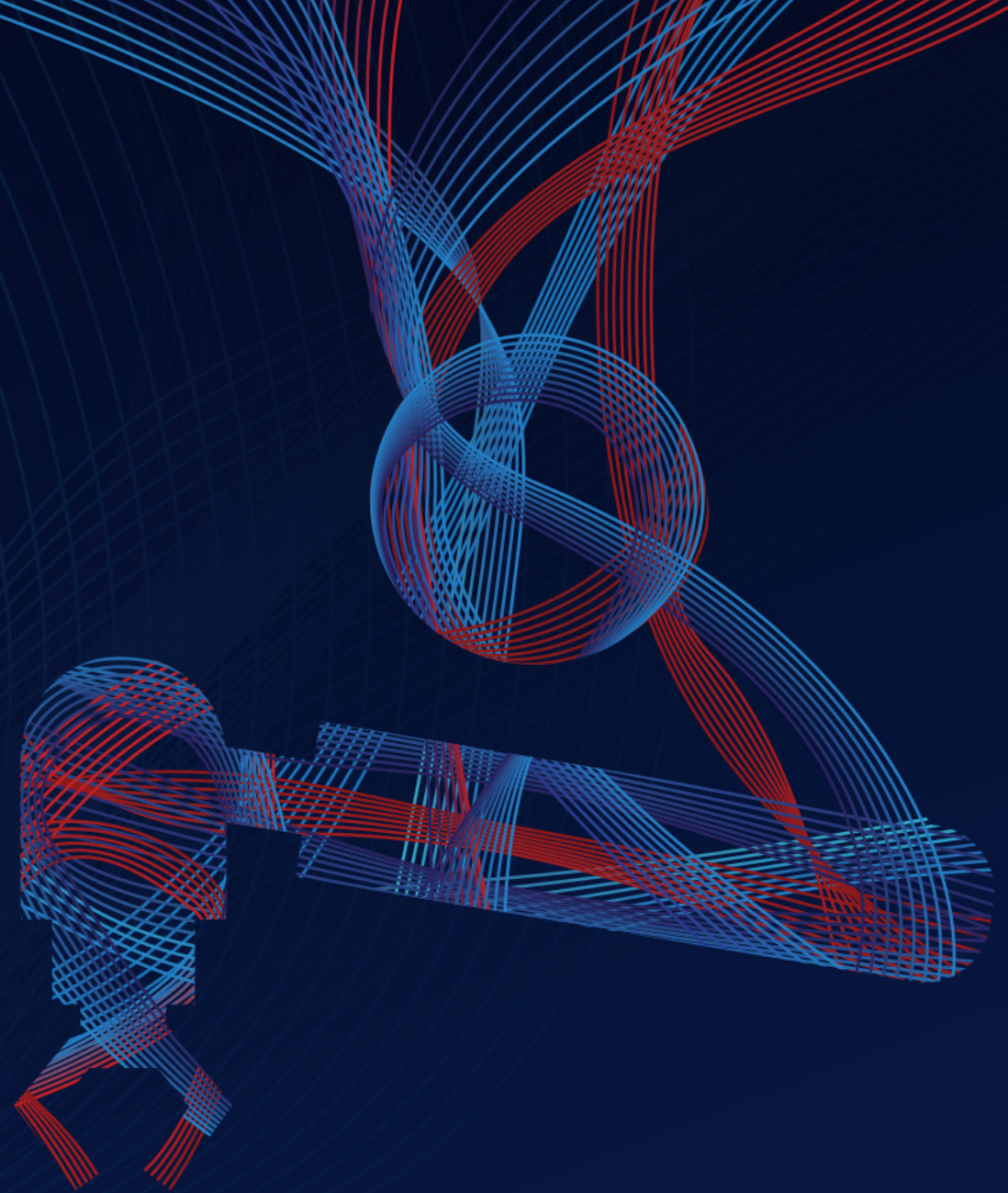
The Cost of Applying Patches

Applying patches carries the risk of bricking the devices or causing synchronization issues.

This causes downtime – exactly what the users wanted to prevent by patching!



The Benefits of Patching



Insights from the Research Lab

Part 1

1

SCADAfence's offensive research arm, discovered vulnerabilities in industrial products such as [CVE-2020-13238](#) and [CVE-2020-12117](#).

2

"We found a vulnerability in an industrial component.

After the vendor released a patch, we tested it and found a similar vulnerability in the patched component.

This reduces the overall effectiveness of patching."

– Ofer Shaked, Co-Founder & CTO of SCADAfence

3

Conclusion

Patches are all too often too specific, leaving plenty of room for similar vulnerabilities to be discovered and exploited.

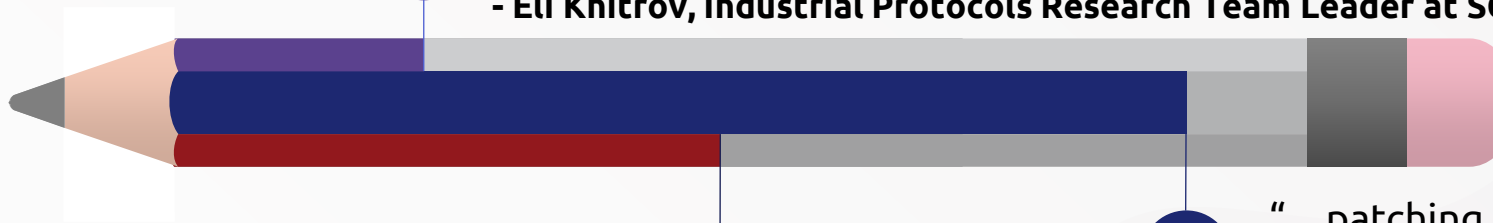
Insights from the Research Lab

Part 2

"Many industrial devices lack basic means of security in their proprietary protocols, causing patches on them to be ineffective.

Authentication is rarely implemented so an attacker can directly perform any action they wish, without exploiting any undocumented vulnerabilities."

- Eli Khitrov, Industrial Protocols Research Team Leader at SCADAfence



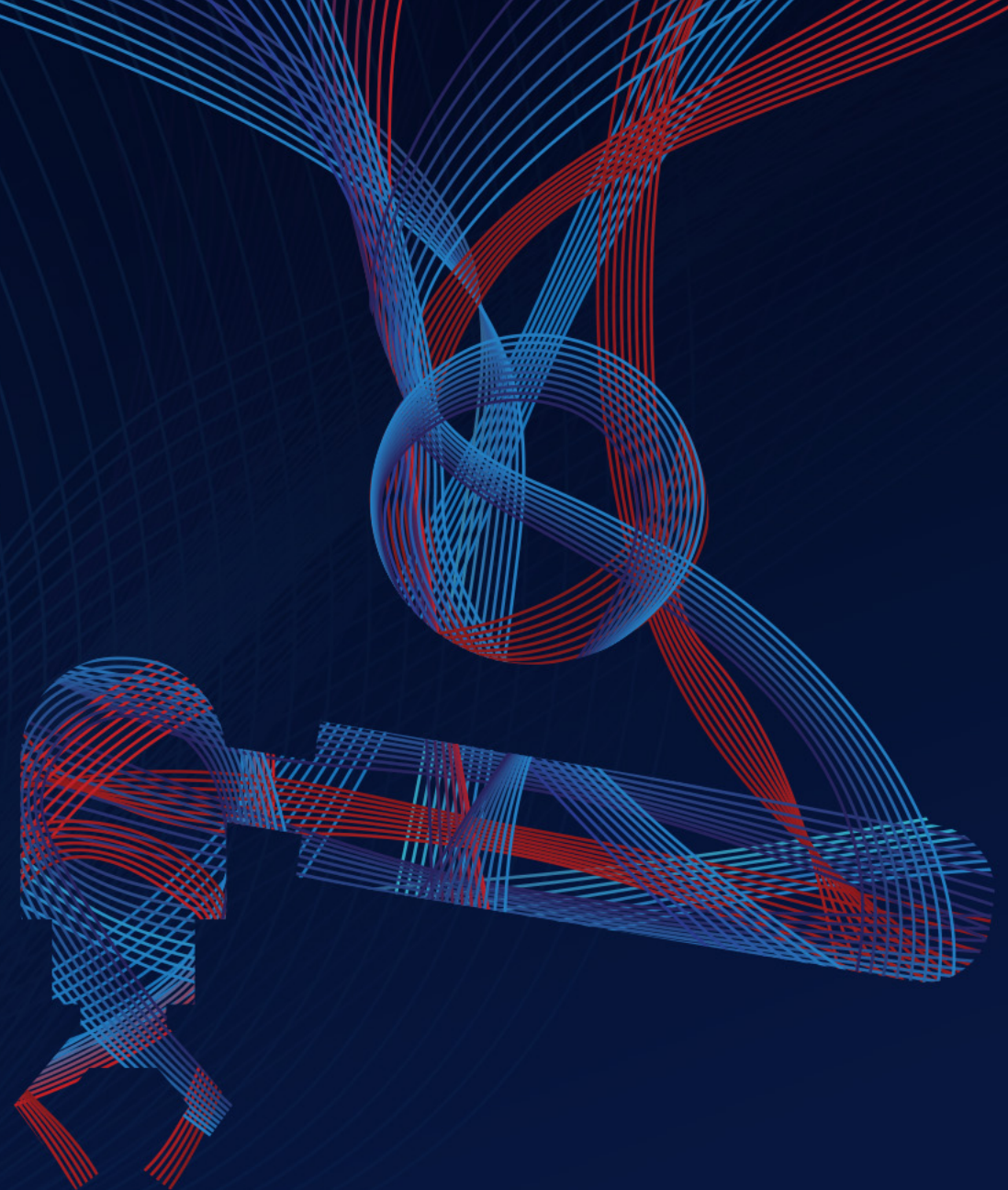
"...patching an insecure by design cyber asset usually results in trivial risk reduction because everything the adversary needs and wants is a documented feature."

- Dale Peterson in "A Fool's Errand: Trying to patch everything in your ICS"

Conclusion:

Patches can be completely ineffective if the target devices lack basic security measures such as authentication.

Conclusions



Conclusions

Maintain an Asset Inventory

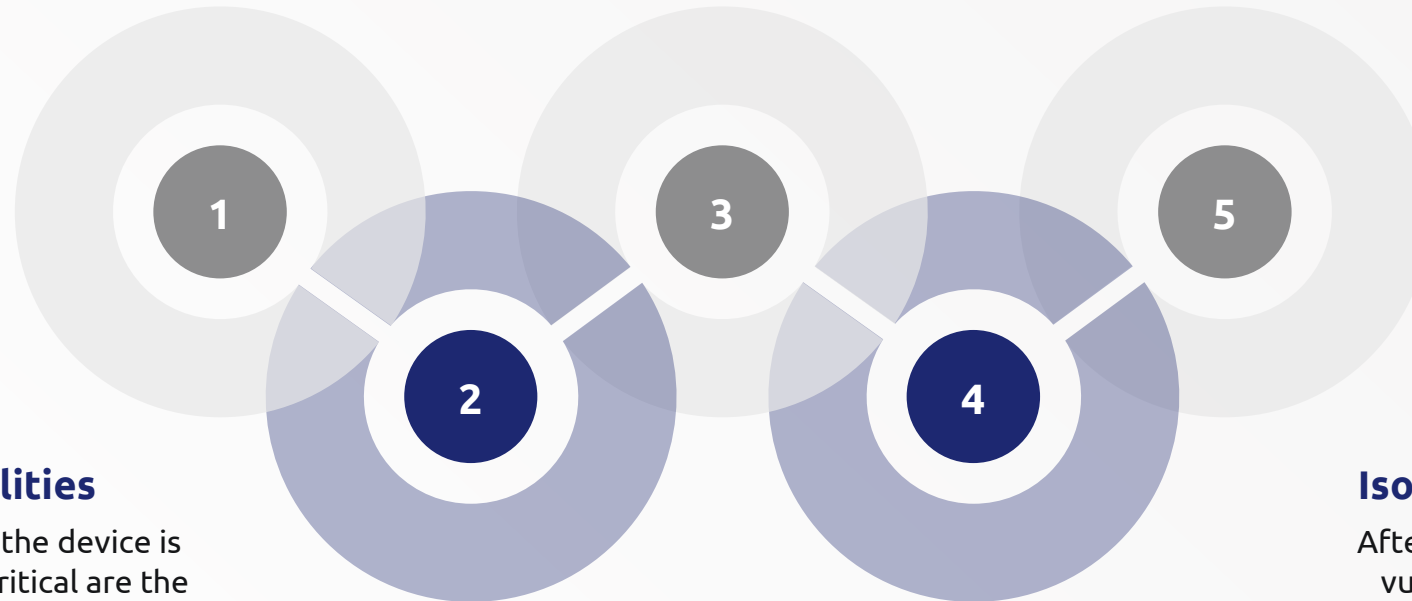
An automated, up-to-date, passive & active asset inventories provide the most comprehensiveness.

Map Vulnerabilities to Assets

Map vulnerabilities to assets by matching vulnerability disclosure sources with your asset inventory. Avoid scanning for vulnerabilities to prevent downtime due to instability of industrial devices.

Detect Exploitation

Realize that some devices will remain temporarily or permanently unpatched. Deploy means to detect exploitation of vulnerabilities in your network.



Prioritize Vulnerabilities

Understand how exposed the device is to network threats, how critical are the device and the vulnerability, and the effectivity of the patch.

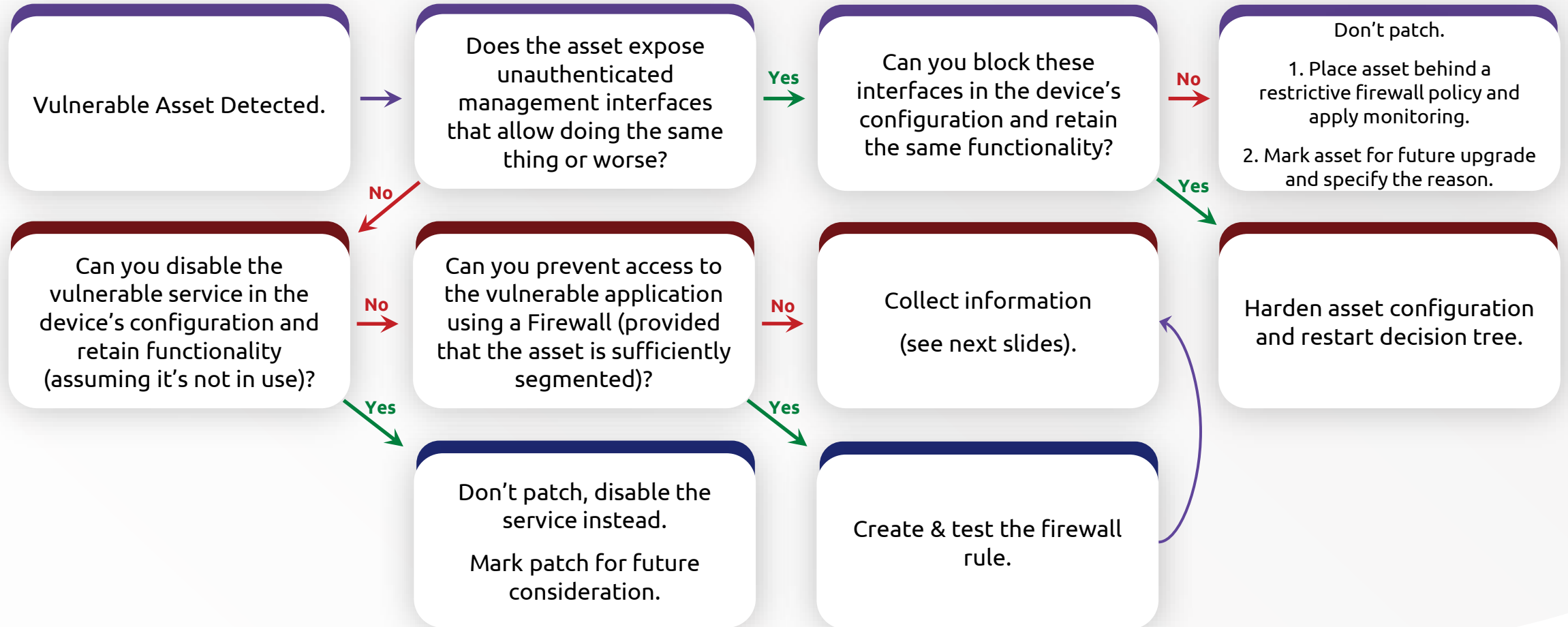
Isolate Vulnerable Devices

After discovering which devices are vulnerable, consider placing them behind firewalls, limiting their interfaces to the network to reduce your attack surface.

A Decision Making Tool for Industrial Vulnerability Management Teams



The Decision Making Tool For Industrial Vulnerabilities



● Yes ● No

Decision Making Tool – Vulnerability Information Collection

	Question	Answer (From 1-3)	Answer Meaning
Immediate Impact	What is the immediate safety/environmental/business impact if this vulnerability is exploited?	1-3	1-Low 2-Medium 3-High/Critical
Other Impact	If the vulnerability is exploited, what is the impact to other assets?	1-3	1-No impact to other assets 2-Partial network compromise 3-Substantial network compromise
Exposure	How exposed are the affected assets to different attack vectors (network-based attacks, physical access)?	1-3	1-High security zone 2-Privileged/internal zone 3-Internet facing / public / guest zone
Likelihood	How easy is it to exploit?	1-3	1-Unlikely to be exploited 2-Likely to be exploited 3-Already widely exploited
Total	12/12	<p>A higher score means higher risk of not patching the vulnerability</p>	

Decision Making Tool – Patch Information Collection

	Question	Answer (From 1-3)	Answer Meaning
Timing	What is the cost of downtime involved in patching immediately (assuming patching is successful)?	1-3	1-Little to no downtime 2-Significant downtime (manageable) 3-Requires higher management approval
Errors	What will be the business impact if some devices (not more than 10%) lose functionality due to applying the patch?	1-3	1-Little to no impact 2-Significant impact 3-Hard to tolerate
Stability	How sure are you of the patch stability, based on the following factors: 1. What is the reliability of the vendor supplying the patch? 2. Is the patch modifying a core or a peripheral component? 3. How many versions are you jumping through (more versions - more room for error)?	1-3	1-Pretty confident 2-Unsure 3-High likelihood of errors
Scope	How many devices are you planning to patch? The more devices, the higher the chance of failure in at least some of them.	1-3	1-One or just a few 2-10-50 3-More than 50
Recovery	What is your ability to restore functionality (e.g. from backups), in case some devices lose functionality?	1-3	1-Easy (e.g. I have backups and spare devices) 2-Substantial effort 3-Extremely hard (e.g. having to call a vendor on-site or device is discontinued / hard to replace)

Total 15/15

A higher score means a higher risk of patching

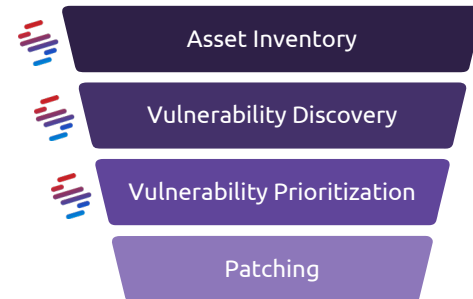
Example Policies – Using the Decision Making Tool

Vulnerability Information	Patch Information	Policy
Exposure == 3 and Likelihood >= 2	Any	Patch Now
Total >= 10	Total <= 7	Patch Now
Total == 4	Total >= 7	Document, don't patch

Add your own policies based on your risk tolerance

Maturity Model – Vulnerability Management Programs

Low Maturity – Basic Program



High Maturity – Advanced Program



Additional Reading

Check Out These Articles

Carnegie Mellon University
Software Engineering Institute

PRIORITIZING VULNERABILITY RESPONSE: A STAKEHOLDER-SPECIFIC VULNERABILITY CATEGORIZATION

Jonathan M. Spring, Eric Hattback, Allen Householder, Art Manion, & Deana Shick†
November 2019

https://resources.sei.cmu.edu/asset_files/WhitePaper/2019_019_001_636391.pdf

ICS Security Patching: Never, Next, Now

Published on February 14, 2019



Dale Peterson

Founder & Program Chair of S4 Events, Writer, Speaker, Podcaster, ICS Security [94 articles](#)
Consultant since 2000

✓ Following

<https://www.linkedin.com/pulse/ics-security-patching-never-next-now-dale-peterson/>

A decorative graphic on the left side of the slide consists of several overlapping, rounded rectangular brush strokes. The strokes are arranged diagonally from the top-left towards the bottom-right. The colors transition from a bright red at the top, through shades of pink and purple, to a vibrant blue at the bottom. The background is a solid, dark navy blue.

Thank You!