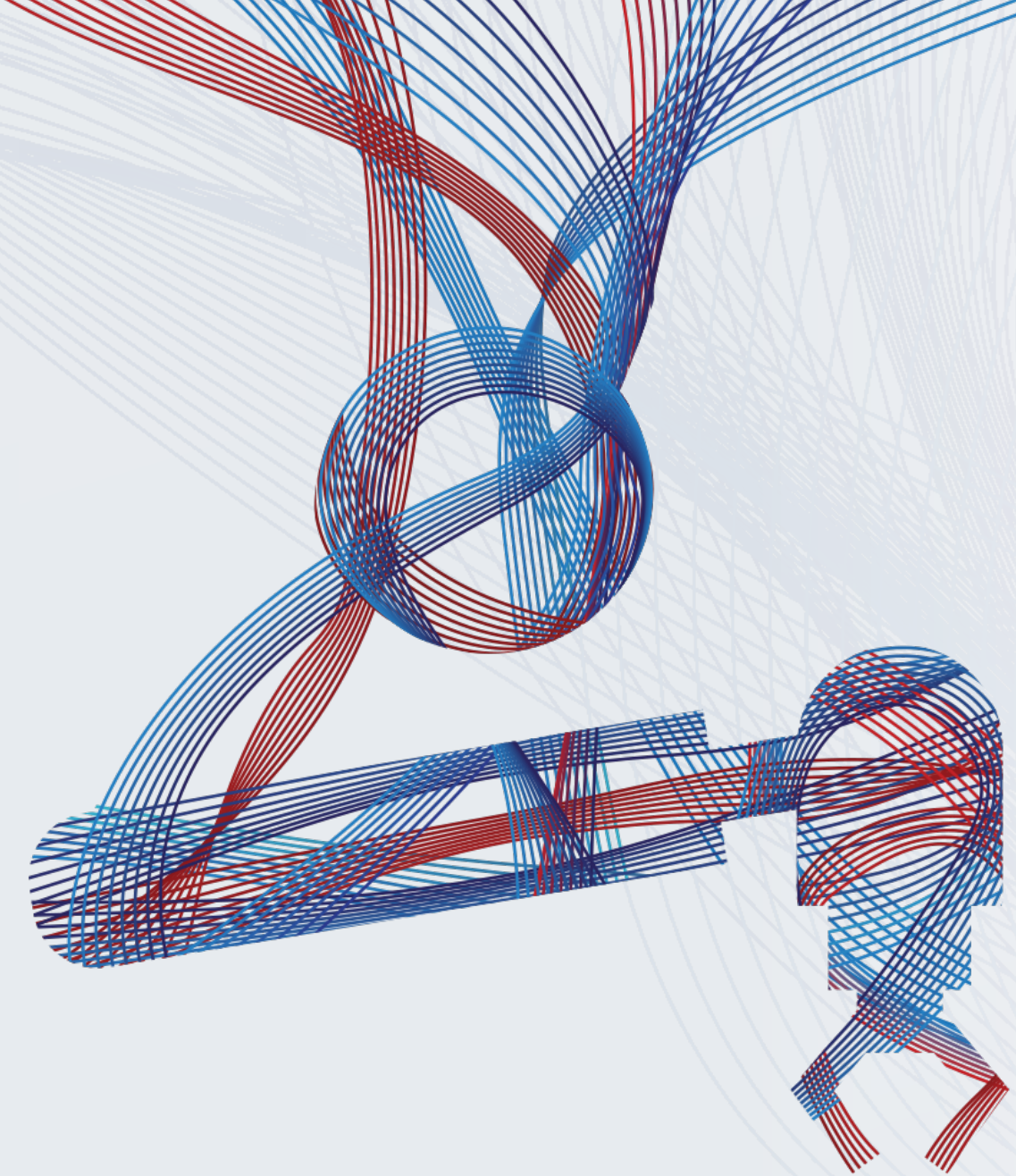


SCADAfence

A Comprehensive Guide to Industrial Device Patching

--- Public Preview ---

A SCADAfence Research Original Publication

Ofer Shaked, Co-Founder and CTO, SCADAfence

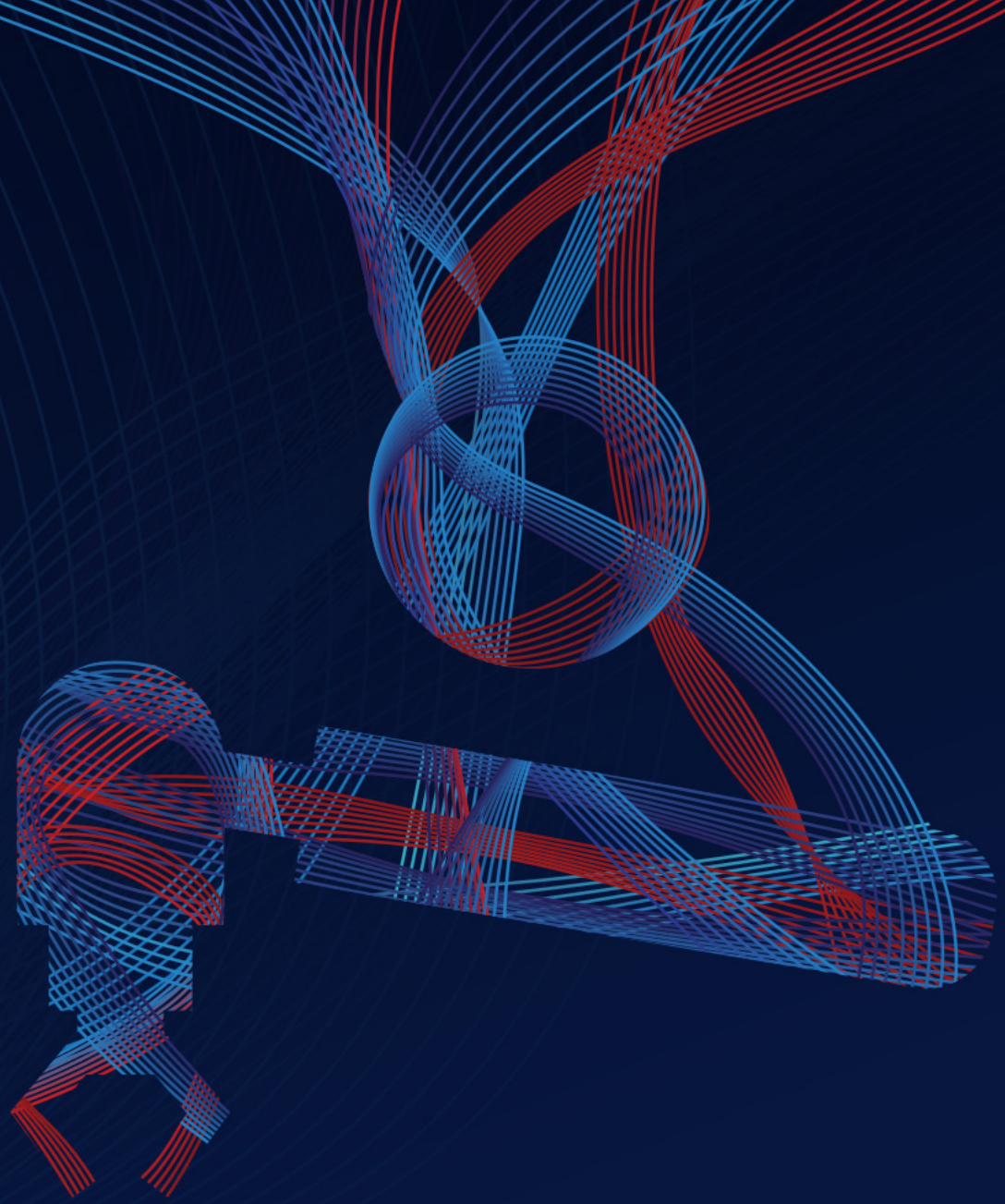
Ofer Shaked – Speaker Profile

- 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

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.

SCADAfence

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.

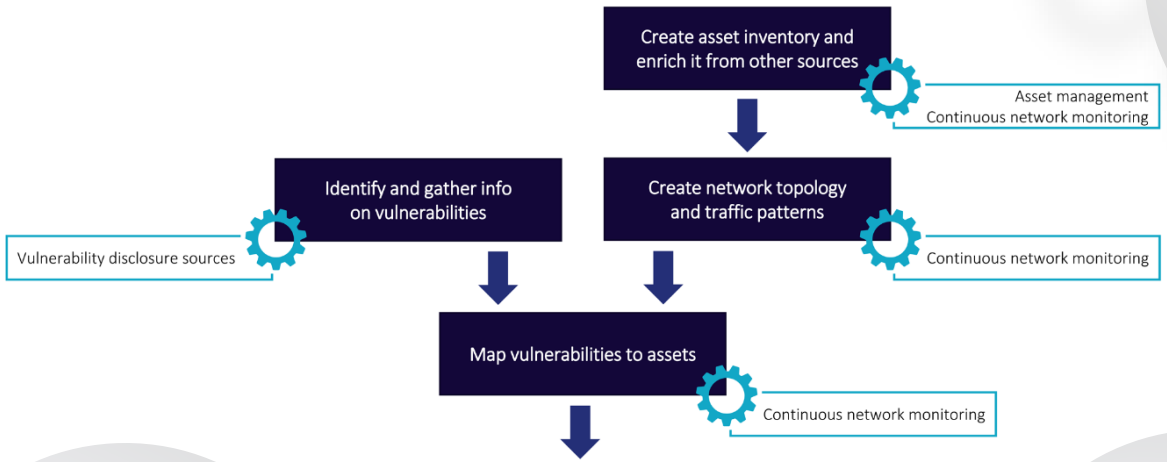
Conclusion

Vulnerability scanning is unfit for scanning in OT.

SCADAfence

Four Steps To Safe Vulnerability Discovery

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



Source: OTCSA Position Paper: “Vulnerability Management for Operational Technology”

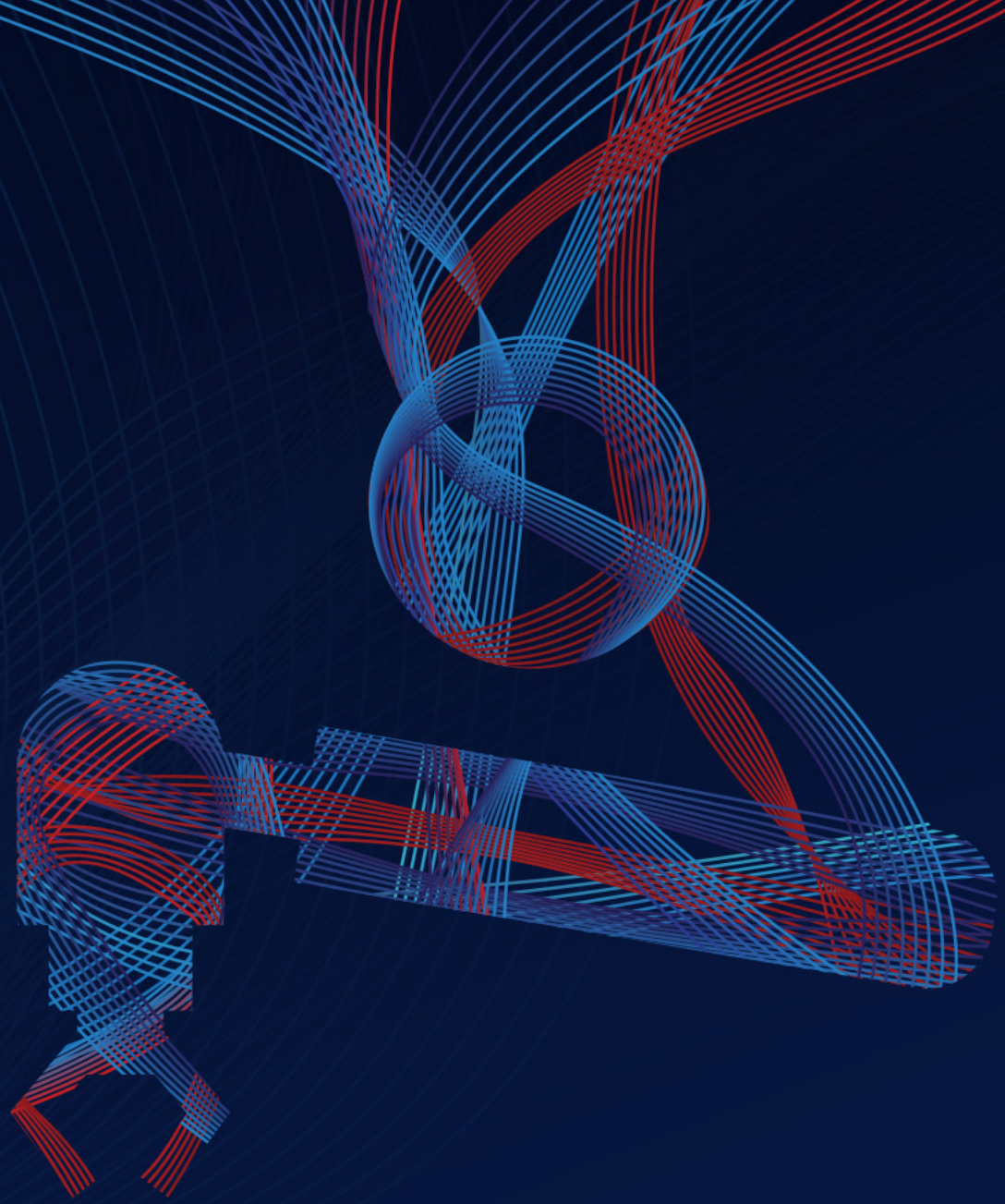
Step 2:
Perform Network Mapping to understand which assets are reachable and from where.

Step 3:
Gather vulnerabilities from vulnerability disclosure sources.

Step 4:
Map vulnerabilities to assets.

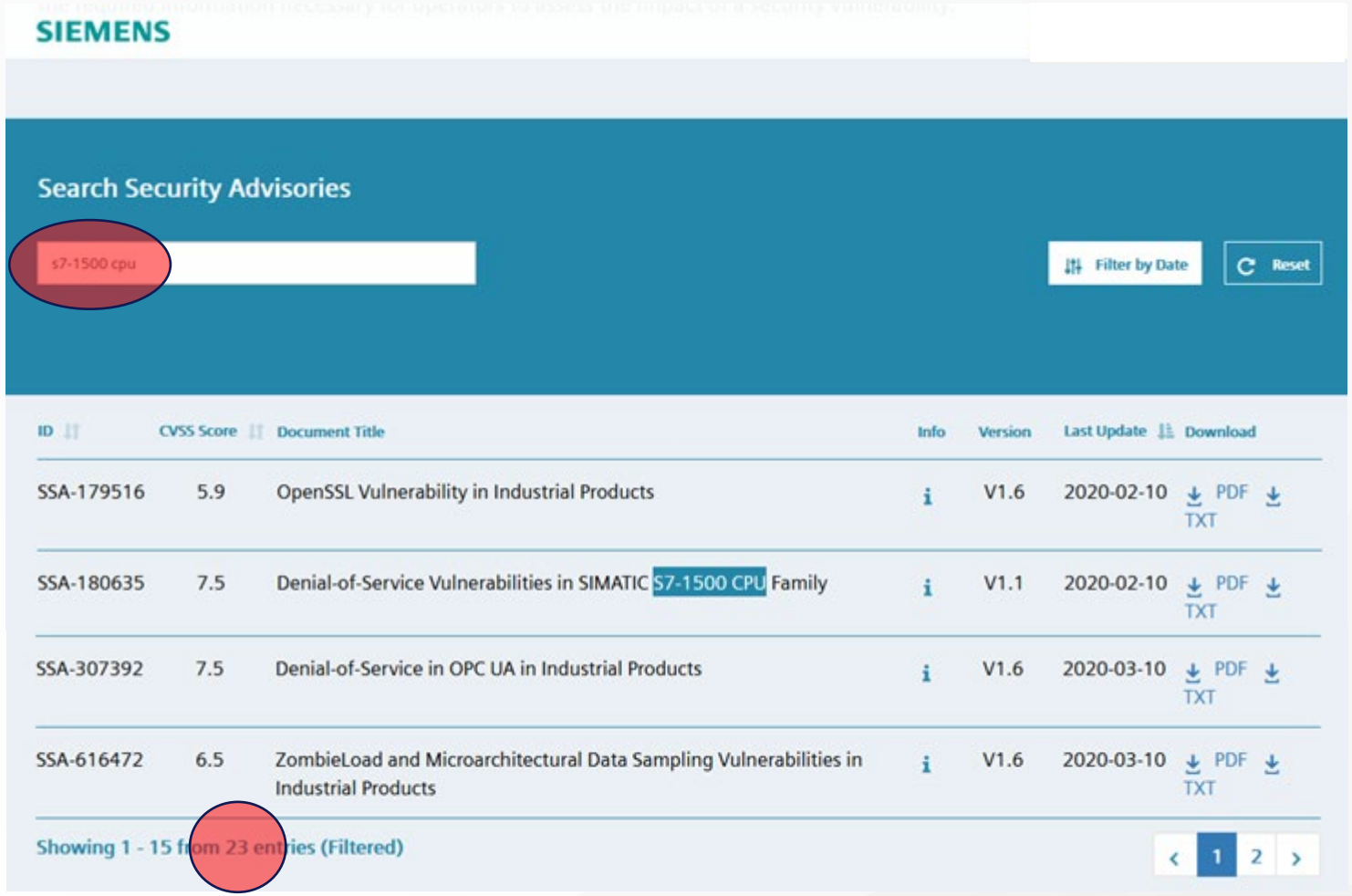
The Cost of Patching

Step 2: Patching Devices



How Many Patches are Required Per Device?

Case Study: Siemens SIMATIC S7-1500 CPU



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

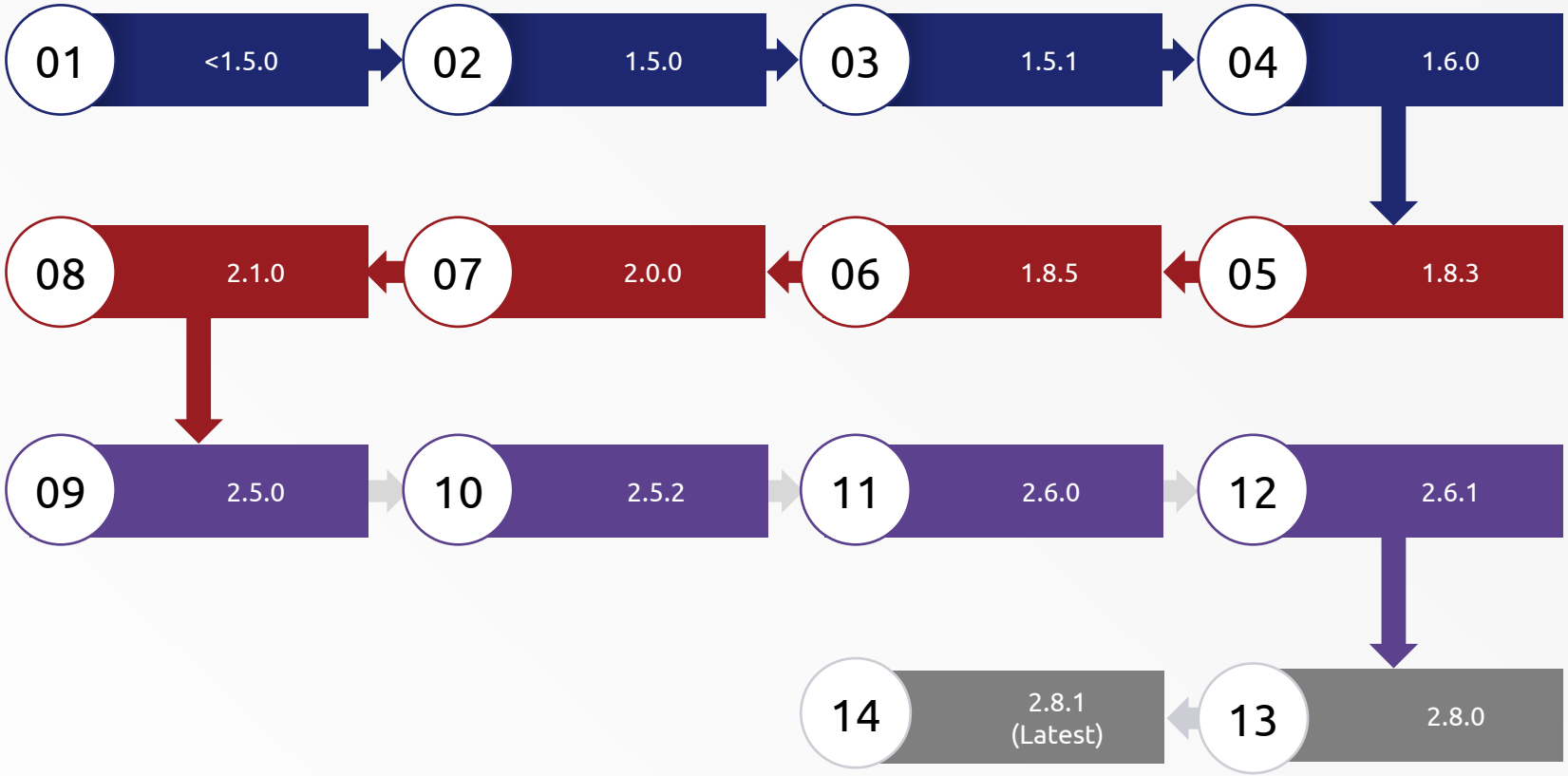
Notice

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

SCADAfence

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.

SCADAfence

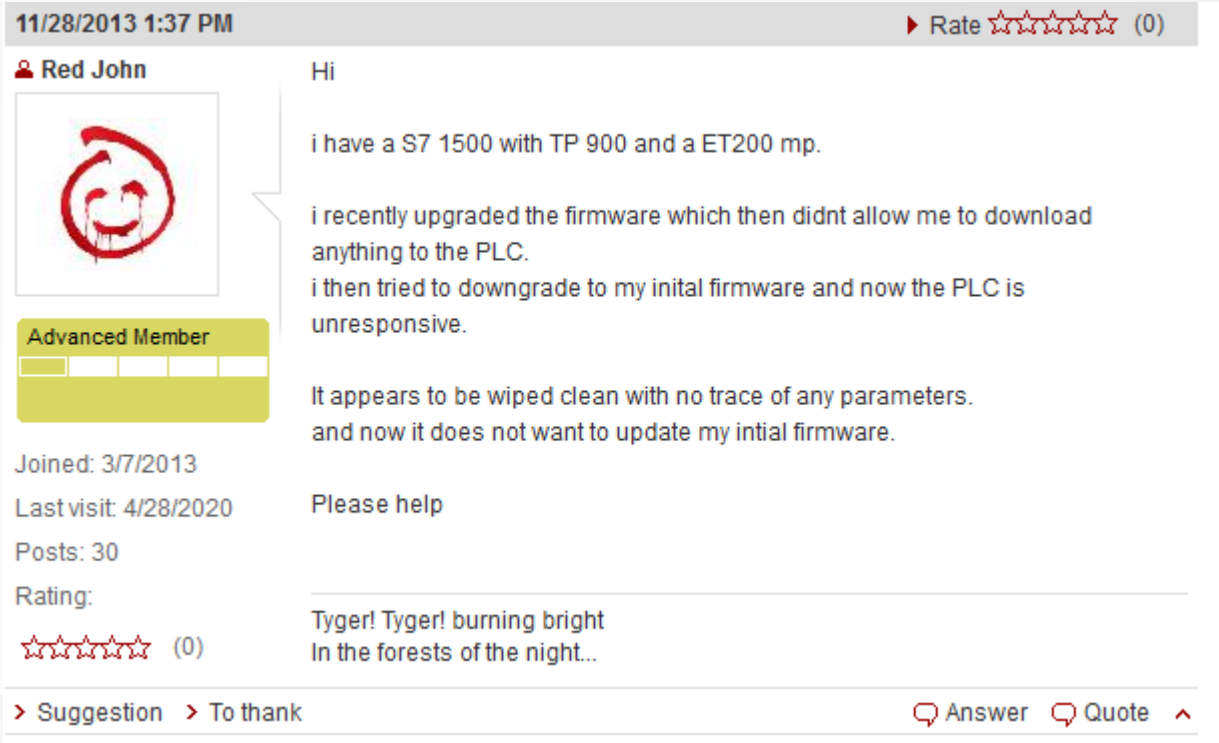
The Cost of Applying Patches - #1

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.



SCADAfence

Interested in learning more?

Get the full guide & 3 Decision Making tools here for free:

https://l.scadafence.com/industrial-device-patching-costs-vs-benefit