A Pirate's Guide to Snake Oil & Security

HD MOORE | MAY 15, 2025

<spoken>

Welcome aboard!

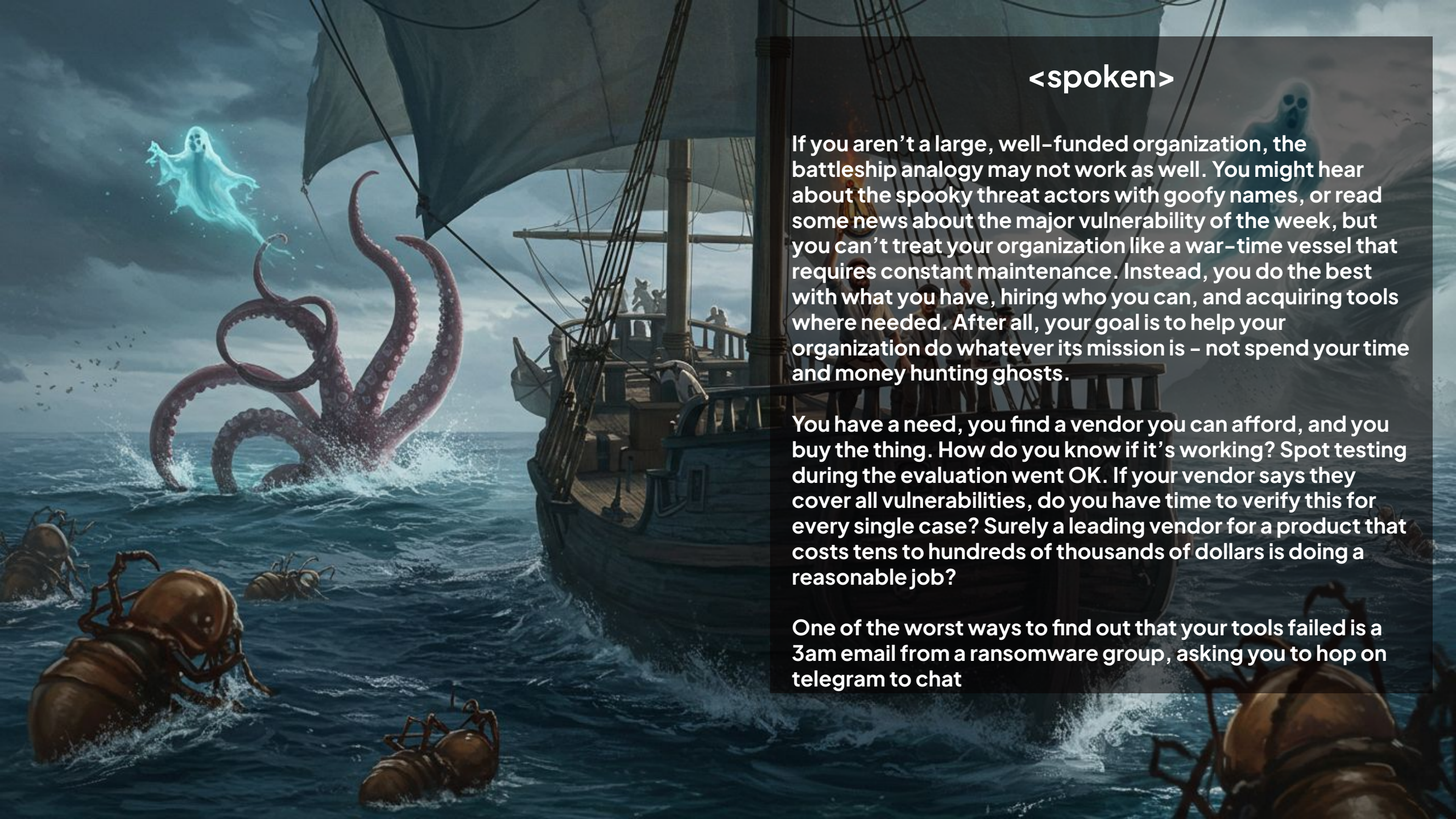
I've spent most of my life researching vulnerabilities, breaking into systems, and writing security tools. I created the Metasploit project, found and reported hundreds of vulnerabilities, and helped build a few commercial products.

Today, I'd like to show you how to benchmark your vulnerability management tools using public data sources.

Disclaimer: All commercial product data & screenshots were sourced from public web sites & videos

<spoken>

I like to imagine my organization's security as a battleship – navigating the rough seas of the internet. Why a ship? It's under constant stress. If you aren't performing continuous maintenance, you will sink. The internet is a hostile place; doing nothing at all means your ship is rusting, taking on water, and and becoming more difficult to fix every day. It's not the most cheerful perspective, compared to IT security, even that analogy feels optimistic. All software rots, all hardware eventually goes out of support. If you aren't actively pushing back, you are falling behind.

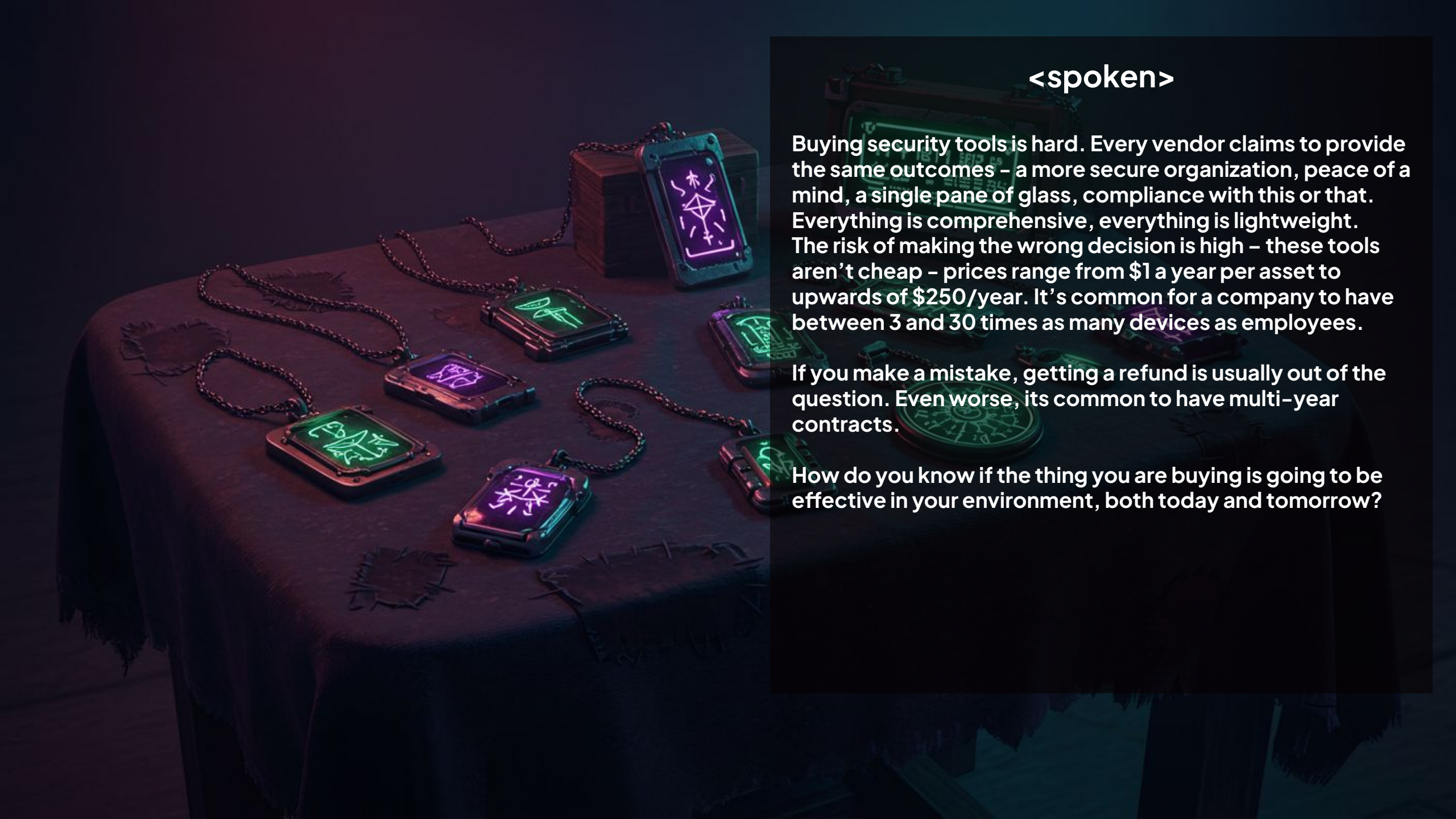


<spoken>

If you aren't a large, well-funded organization, the battleship analogy may not work as well. You might hear about the spooky threat actors with goofy names, or read some news about the major vulnerability of the week, but you can't treat your organization like a war-time vessel that requires constant maintenance. Instead, you do the best with what you have, hiring who you can, and acquiring tools where needed. After all, your goal is to help your organization do whatever its mission is – not spend your time and money hunting ghosts.

You have a need, you find a vendor you can afford, and you buy the thing. How do you know if it's working? Spot testing during the evaluation went OK. If your vendor says they cover all vulnerabilities, do you have time to verify this for every single case? Surely a leading vendor for a product that costs tens to hundreds of thousands of dollars is doing a reasonable job?

One of the worst ways to find out that your tools failed is a 3am email from a ransomware group, asking you to hop on telegram to chat

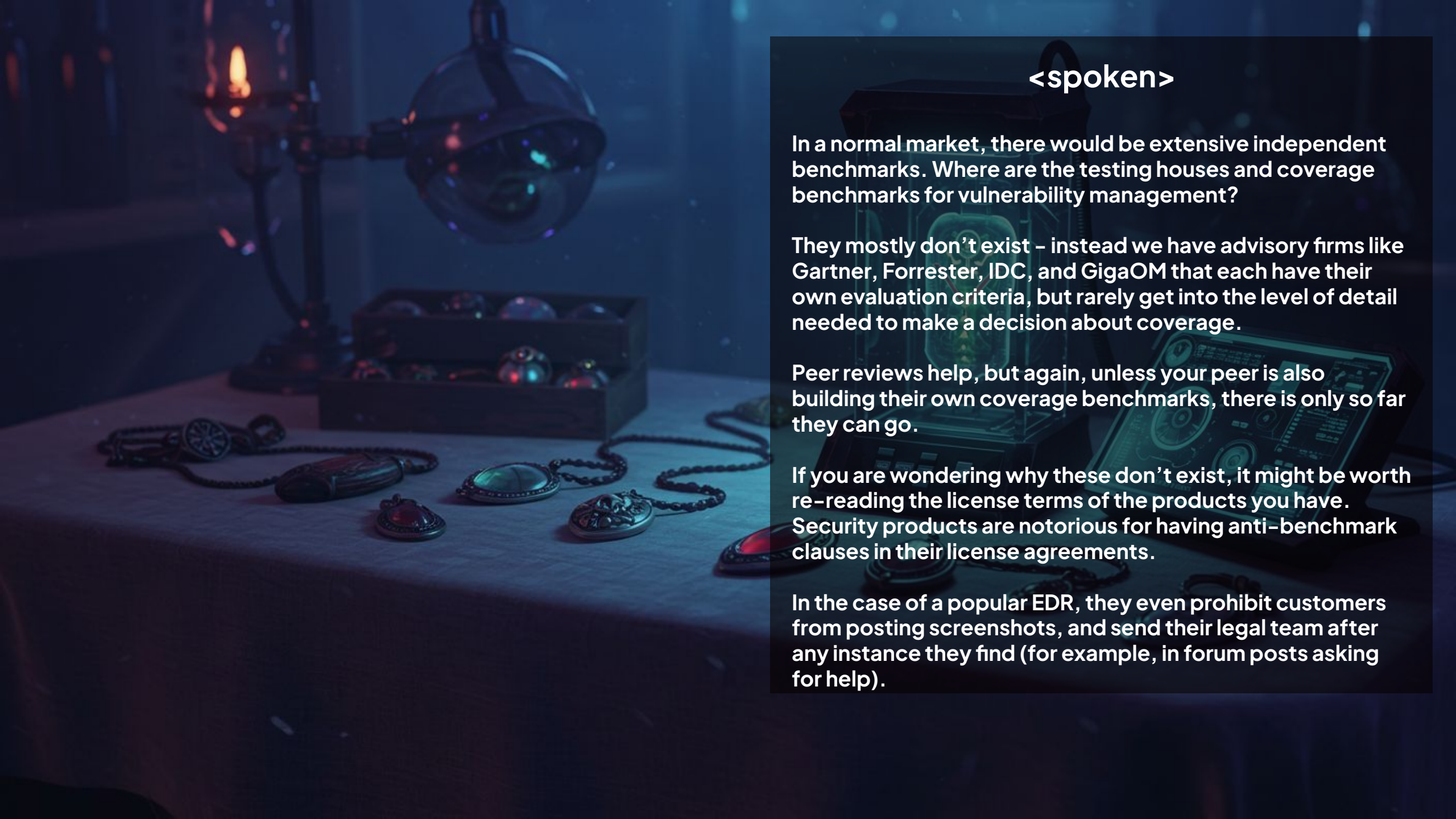


<spoken>

Buying security tools is hard. Every vendor claims to provide the same outcomes – a more secure organization, peace of a mind, a single pane of glass, compliance with this or that. Everything is comprehensive, everything is lightweight. The risk of making the wrong decision is high – these tools aren't cheap – prices range from $1 a year per asset to upwards of $250/year. It's common for a company to have between 3 and 30 times as many devices as employees.

If you make a mistake, getting a refund is usually out of the question. Even worse, its common to have multi-year contracts.

How do you know if the thing you are buying is going to be effective in your environment, both today and tomorrow?



<spoken>

In a normal market, there would be extensive independent benchmarks. Where are the testing houses and coverage benchmarks for vulnerability management?

They mostly don't exist – instead we have advisory firms like Gartner, Forrester, IDC, and GigaOM that each have their own evaluation criteria, but rarely get into the level of detail needed to make a decision about coverage.

Peer reviews help, but again, unless your peer is also building their own coverage benchmarks, there is only so far they can go.

If you are wondering why these don't exist, it might be worth re-reading the license terms of the products you have. Security products are notorious for having anti-benchmark clauses in their license agreements.

In the case of a popular EDR, they even prohibit customers from posting screenshots, and send their legal team after any instance they find (for example, in forum posts asking for help).

PenTest-Tools.com

- A rare public benchmark
- Focused on vulhub targets
- Highlights open source
- Maybe slightly biased

Methodology for this network scanners benchmark

Testing period: January 2024
Detections: all scanners were updated with the latest detections as of January 2024.

167 vulnerable environments tested

17 instances used in the testing setup

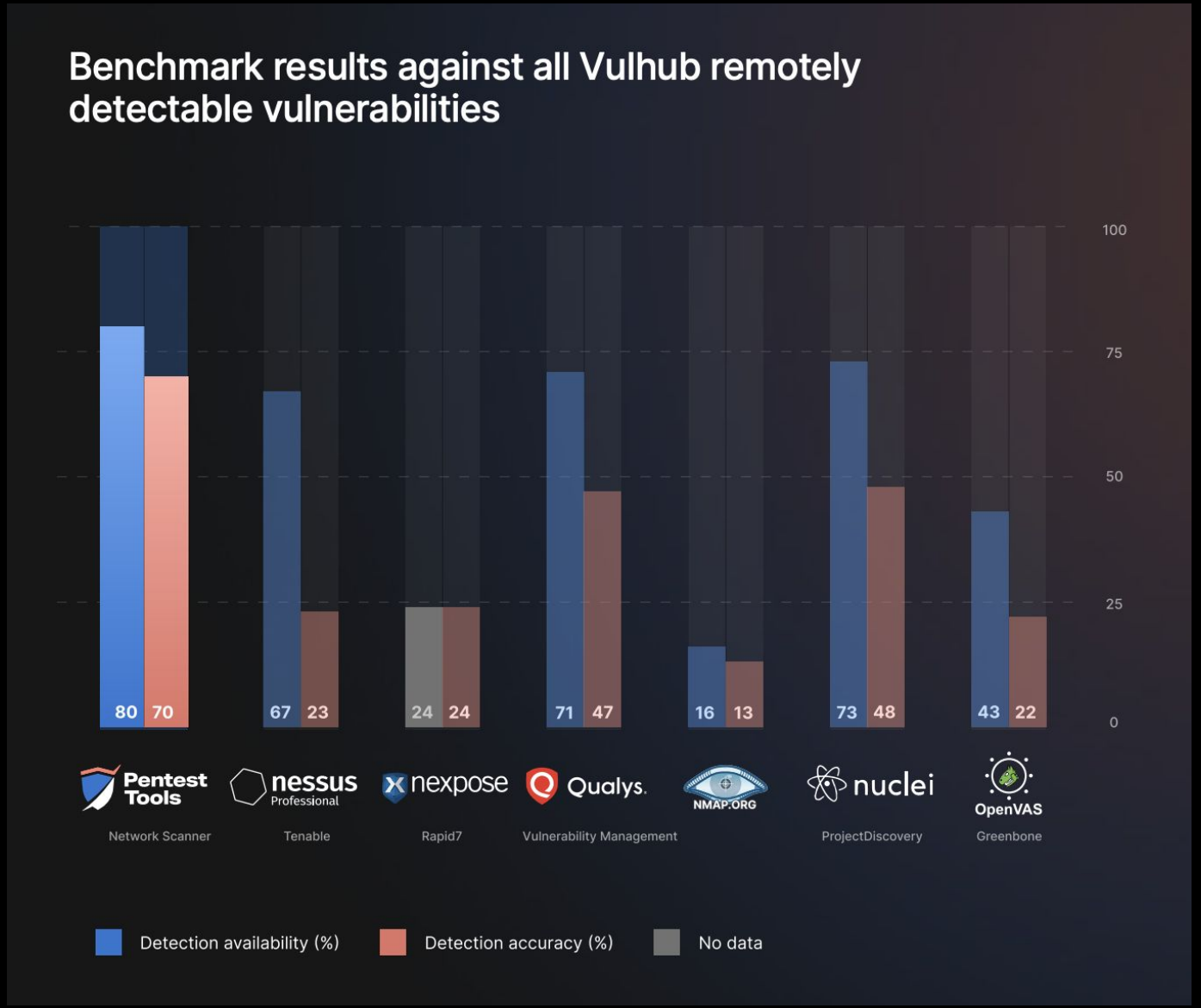
7 popular network scanners evaluated

128 environments with remotely detectable CVEs

39 environments with non-remotely detectable CVEs

2 criteria detection availability and accuracy

https://github.com/vulhub/vulhub



https://pentest-tools.com/benchmarks/network-vulnerability-scanners

Criteria For Evaluating Coverage

- Response time for the highest-risk vulnerabilities
- Total number of unique checks
- Total number of unique CVEs
- Detection method differences
  - Installed Agent
  - Authenticated Scan
  - Unauthenticated Scan
  - Passive Traffic Analysis

2023

26,477
new vulnerabilities were disclosed in 2023

2%
(570) were actively exploited

25% were weaponized on **Day 1**

75% were under active exploit within **19 days**

23 days
average lag time between an exploit publication & formal CVE assignment

9 days
average time to roll out patches once CVEs are assigned

Of the most critical vulnerabilities on the CISA KEV list:

- Only **15%** are patched **within 30 days**
- **50%** by **Day 55**
- **80%** by **Day 180**

https://www.qualys.com/forms/tru-research-report/confirm/

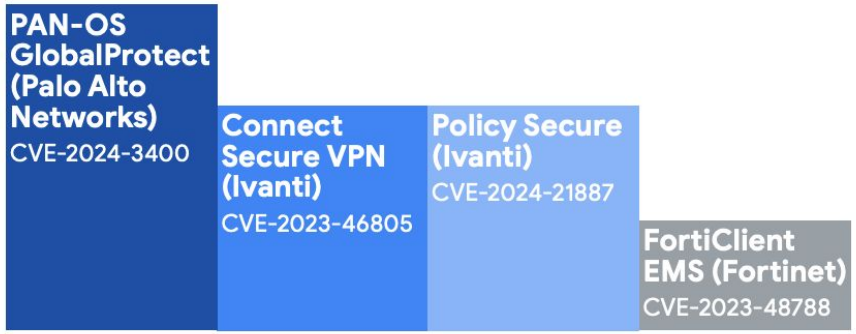
Source: 2023 Qualys Trurisk Research Report

2024

Most Frequently Exploited Vulnerabilities

Among the Mandiant incident response investigations performed in 2024, the most frequently exploited vulnerabilities affected security devices, which are, due to their function, typically placed at the edge of the network. Three of the four vulnerabilities were first exploited as zero-days. While a broad selection of threat actors have recently targeted edge devices, Mandiant also specifically noted an increase[3] in targeting from Russian[4] and Chinese[5]cyber espionage actors.

Most Frequently Exploited Vulnerabilities



Mandiant (Google) M-Trends 2025 Report

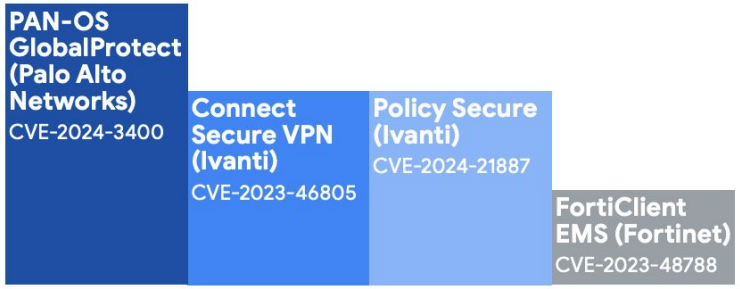
Product Response

- Popular product coverage for the top 4 exploits
- How quickly did each product respond?
- What detection methods are supported?
  - U: Unauthenticated Scan
  - A: Authenticated scan
- Unauthenticated same-day coverage is ideal

Most Frequently Exploited Vulnerabilities

Among the Mandiant incident response investigations performed in 2024, the most frequently exploited vulnerabilities affected security devices, which are, due to their function, typically placed at the edge of the network. Three of the four vulnerabilities were first exploited as zero-days. While a broad selection of threat actors have recently targeted edge devices, Mandiant also specifically noted an increase[3] in targeting from Russian[4] and Chinese[5]cyber espionage actors.

Most Frequently Exploited Vulnerabilities



CVE Vendor	CVE	Public	KEV	Tenable (U)	Tenable (A)	Rapid7 (U)	Rapid7 (A)	Qualys (U)	Qualys (A)	GreenBone (U)	GreenBone (A)	Nuclei (U)
Palo Alto Networks	CVE-2024-3400	2024-04-12	2024-04-12	2024-05-21	2024-04-12	2024-04-12	2024-04-12	2024-04-17	2024-04-12		2024-04-12	2024-04-16
Ivanti	CVE-2023-46805	2024-01-10	2024-01-10	2024-01-10		2023-01-15		2024-02-08	2024-01-11	2024-01-11		2024-01-16
Ivanti	CVE-2024-21887	2024-01-10	2024-01-10	2024-01-10		2023-01-15		2024-02-08	2024-01-11			2024-01-16
Fortinet	CVE-2023-48788	2024-03-12	2024-03-25		2024-03-14		2024-11-20	2025-01-21	2024-03-18	2024-03-22	2024-03-13	2024-11-30

* Dates and coverage statuses are estimates are based on publicly available data

Timely Coverage	Late Coverage	Missing	Covered by Unauth	Timely Auth Coverage

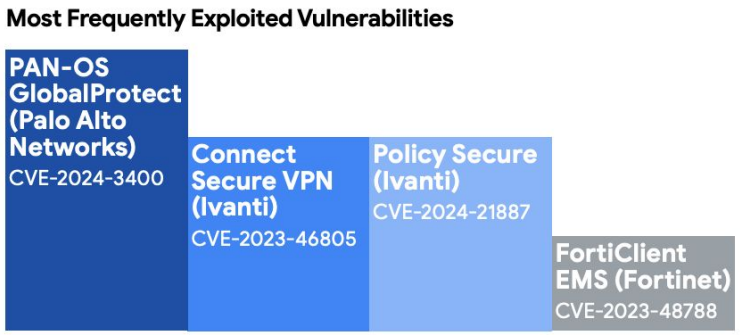
Product Response

- No perfect scores for unauthenticated scans
- Qualys and Nuclei get really close
- Are these four CVEs outliers?

Let's review a more recent vulnerability

Most Frequently Exploited Vulnerabilities

Among the Mandiant incident response investigations performed in 2024, the most frequently exploited vulnerabilities affected security devices, which are, due to their function, typically placed at the edge of the network. Three of the four vulnerabilities were first exploited as zero-days. While a broad selection of threat actors have recently targeted edge devices, Mandiant also specifically noted an increase[3] in targeting from Russian[4] and Chinese[5]cyber espionage actors.



CVE Vendor	CVE	Public	KEV	Tenable (U)	Tenable (A)	Rapid7 (U)	Rapid7 (A)	Qualys (U)	Qualys (A)	GreenBone (U)	GreenBone (A)	Nuclei (U)
Palo Alto Networks	CVE-2024-3400	2024-04-12	2024-04-12	2024-05-21	2024-04-12	2024-04-12	2024-04-12	2024-04-17	2024-04-12		2024-04-12	2024-04-16
Ivanti	CVE-2023-46805	2024-01-10	2024-01-10	2024-01-10		2023-01-15		2024-02-08	2024-01-11	2024-01-11		2024-01-16
Ivanti	CVE-2024-21887	2024-01-10	2024-01-10	2024-01-10		2023-01-15		2024-02-08	2024-01-11			2024-01-16
Fortinet	CVE-2023-48788	2024-03-12	2024-03-25		2024-03-14		2024-11-20	2025-01-21	2024-03-18	2024-03-22	2024-03-13	2024-11-30

* Dates and coverage statuses are estimates are based on publicly available data

Timely Coverage	Late Coverage	Missing	Covered by Unauth	Timely Auth Coverage

CVE-2025-23006

SONICWALL®

SMA1000 Pre-Authentication Remote Command Execution Vulnerability

Approximately ~3,500 affected systems connected to the public internet

Exploitation limited to AMC/CMC consoles (port 8443, only ~90 exposed)

Announcement Timeline

202?-??-??
Microsoft Threat Intelligence Center (MSTIC) observes exploitation

202?-??-??:
MSTIC reports the issue to SonicWall PSIRT

202?-??-??:
SonicWall & MSTIC coordinate the release

2025-01-22:
SonicWall releases advisory and patch

2025-01-24:
CISA adds to the Known Exploitation Vulnerabilities list

CVE-2025-23006

SONICWALL®

Product Response

2025-01-23
Tenable provides technology-based search query for SMA

2025-01-23:
runZero provide technology-based search query for AMC/CMC

2025-01-23:
GreenBone publishes direct vulnerability check for OpenVAS

2025-01-24:
Tenable publishes direct vulnerability check

2025-01-30:
Rapid7 publishes direct vulnerability check

Authenticated scans don't appear to be implemented for SonicWall devices.

Let's dig into specifics.

CVE-2025-23006

SONICWALL®

What's Missing? (2025-05-15)

- Qualys skipped coverage (but includes most other SonicWall CVEs)
- Tenable's check requires non-default options (Paranoid & Thorough)
- GreenBone did not include check in the Community Edition feed
- Nuclei does not have coverage yet (and many products use Nuclei)
- SonicWall 8200v installer is still unpatched (with manual updates)
- Still no public exploit or PoC

CVE Vendor	CVE	Public	KEV	Tenable (U)	Tenable (A)	Rapid7 (U)	Rapid7 (A)	Qualys (U)	Qualys (A)	GreenBone (U)	GreenBone (A)	Nuclei (U)
SonicWall	CVE-2025-23006	2025-01-22	2025-01-24	2024-01-24		2025-01-30		Missing	Missing	2025-01-23		Missing

Timely Coverage	Late Coverage	Missing	Covered by Unauth	Timely Auth Coverage

Winning The Zero-Day Race

Zero-day exploitation at the edge has become the new normal

Attackers are exploiting vulnerabilities are lightning speed

Attackers already know their targets before exploitation

Every minute matters for public-facing systems

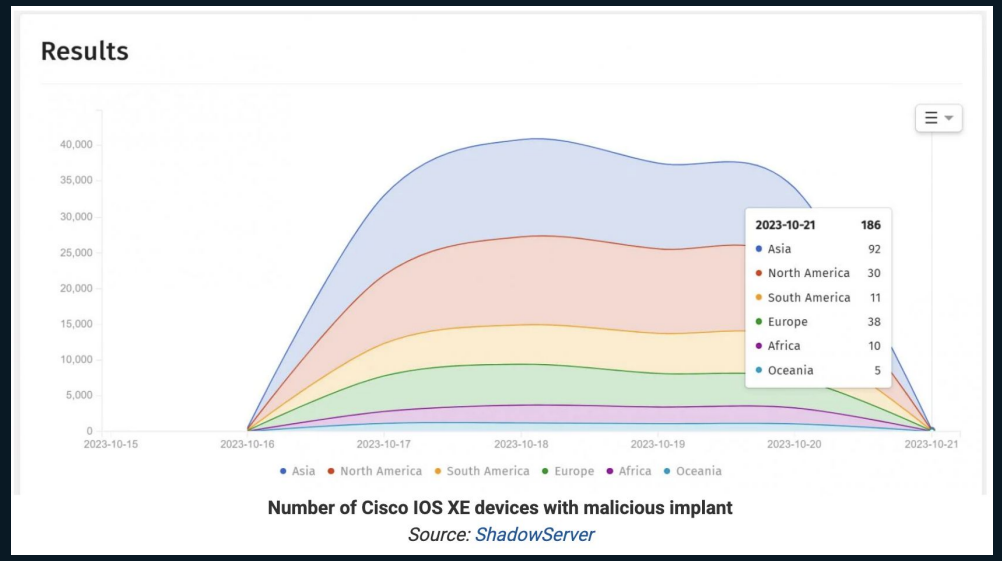
Every part of the response takes time

- You need to be aware of the issue in the first place
- You need to identify all affected assets ASAP
- You need to mitigate before compromise

CVE-2023-20198

Cisco IOS XE Web UI – Multiple Vulnerabilities

Approximately ~145k affected systems connected to the public internet



Number of Cisco IOS XE devices with malicious implant

Source: ShadowServer

https://www.bleepingcomputer.com/news/security/hackers-update-cisco-ios-xe-backdoor-to-hide-infected-devices/

Timeline

2023-09-28
Cisco TAC identifies exploits in the wild, starting on 2023-09-18

2023-10-16
Cisco releases advisory & provides IoCs

2023-10-17
~ 30k devices confirmed as backdoored

2023-10-18
~ 35k devices confirmed as backdoored

2023-10-19
~ 40k devices confirmed as backdoored

2023-10-20
~ 60k devices confirmed as backdoored

2023-10-21
Attackers update the backdoor to require authentication

2023-10-22
Cisco releases an updated firmware with the fix

2023-10-23
~ 38k devices confirmed with the updated backdoor

Real-World Response Times

Exploits in the wild take time for defenders to detect and understand

Security product teams need to triage, build, and test detection

You need to apply the product update

You may need to rescan the network

Scans may be slow to finish

Reporting can be convoluted

Remediation is even slower

Criteria For Evaluating Coverage

- Response time for the highest-risk vulnerabilities
- Total number of unique checks
- Total number of unique CVEs
- Detection method differences
  - Installed Agent
  - Authenticated Scan
  - Unauthenticated Scan
  - Passive Traffic Analysis

Product Coverage Estimates

Product Vendor	Total Checks	Total Unique CVEs	2024 Unique CVEs	No-CVE Checks	Remote Unauth CVE Checks
Qualys VMDR	217k	111k	13k	14k	12k
Tenable Nessus	211k	99k	N/A	29k	14k
Rapid7 InsightVM	233k	79k	7k	N/A	N/A
GreenBone OV	206k	N/A	N/A	21k	32k
Nuclei	11k	3k	0.4k	8k	3k

* As of 2025-05-13 there were 294k allocated CVEs total
* These statistics are only estimates based on publicly available data
* These statistics focus on the VM scanner products and not the entire platform (ex: web, OT, passive)

Checks vs CVEs

Product Vendor	Total Checks	Total Unique CVEs
Qualys VMDR	217k	111k
Tenable Nessus	211k	99k
Rapid7 InsightVM	233k	79k
GreenBone OV	206k	N/A
Nuclei	11k	3k

- A single vulnerability may require differents test for every OS and detection method
- Many checks are auto-generated and look for patch installation via WMI, SSH, or SNMP
- Specific CVE coverage differs widely by tool based on what products they focus on, even if they have similar counts

2024 Was a Banner Year for CVEs

Product Vendor	Total Unique CVEs	2024 Unique CVEs
Qualys VMDR	111k	13k
Tenable Nessus	99k	N/A
Rapid7 InsightVM	79k	7k
GreenBone OV	N/A	N/A
Nuclei	3k	0.4k

- Mature vulnerability management tools cover CVEs all the way back to the late 1990s
- The ratio of CVEs covered in 2024 versus the total is absurd, with 12% of Qualys, 9% of Rapid7, and 13% of Nuclei

Many Critical Exposures Have No CVE

Product Vendor	Total Checks	No CVEs Checks
Qualys VMDR	217k	14k
Tenable Nessus	211k	29k
Rapid7 InsightVM	233k	N/A
GreenBone OV	206k	21k
Nuclei	11k	8k

- CVE allocation requires coordination and time on the part of the researcher and vendor; it's not perfect, but it is the best we have today
- Exposures related to insecure system configuration, weak authentication, and missing access controls rarely have CVEs assigned
- Other examples include widely shared encryption keys and the use of insecure older protocols, like SMB v1
- M-TRENDS points to exploits as 30% of initial access, the rest is much more important

Unauthenticated Scanning is Hard

Product Vendor	Total Checks	Remote Unauth CVE Checks
Qualys VMDR	217k	12k
Tenable Nessus	211k	14k
Rapid7 InsightVM	233k	N/A
GreenBone OV	206k	32k
Nuclei	11k	10k

- Unauthenticated checks make up between 5% and 15% of the mature products
- OpenVAS with GreenBone has almost double the number of unauthenticated CVE-reporting checks compared to Qualys and Tenable (and likely Rapid7 too)
- Nuclei is the exception, with almost all checks implemented as unauthenticated and remote
- In many environments, more than 60% of all assets do not support authenticated scanning

Interested in Vulnerability Scoring & Exploitability Prediction?

Join the talk at Salle Ville-Marie

Vulnerability Haruspicy: Using Woo to Confirm Your Biases

Presented by Tod Beardsley, VP of Security Research

Day 2 • 11:30 – 12pm EDT

"This talk will dig into the strengths, weaknesses, and absurdities of CVSS, EPSS, and SSVC, comparing them to the reality of how security teams actually handle vulnerabilities. Tod will explore where these models help, where they mislead, and whether any of them are meaningfully better than rolling a D20 saving throw vs exploitation. Expect debate, disagreements, and plenty of astrology jokes."

Criteria For Evaluating Coverage

- Response time for the highest-risk vulnerabilities
- Total number of unique checks
- Total number of unique CVEs
- **Detection method differences**
  - Installed Agent
  - Authenticated Scan
  - Unauthenticated Scan
  - Passive Traffic Analysis

Tools Use a Mix of Detection Types

Installed persistent agent software for reporting vulnerabilities

Authenticated assessment via WMI, SMB, SSH, SNMP, and APIs

Dissolvable agents delivered through authenticated scans

Unauthenticated network scans with various safety levels

Passive traffic analysis

Installed Agents

Agent software often reports vulnerabilities as a secondary feature

EDR and MDM tools can be used to enumerate software & versions

Some agents go further and provide deep security scanning

Most agent-based vulnerability scans are incomplete

- Minimal functionality and scope
- Missing network context

Scariest result = Only reporting out-of-date software

Authenticated Scans

Remote scanning through authenticated management protocols

Required by PCI for internal scans as of 2024

Can get close to agent-level system details

Limited by the management protocol

Sprays credentials across the network

Scariest result = “Could not authenticate” and EOL warnings

Unauthenticated Scans

Remote exposure detection through version checks and behavioral testing

Time-intensive to develop, but match the attacker's perspective

Limited test coverage given the difficulty of development

Not every check is safe to run on every target

Scariest result = Less hosts online after the first scan

Passive Traffic Analysis

Arguably the safest, but also significantly limited, and slow to return data

Network communication that indicates vulnerability status is rare

Obtain comprehensive traffic flows is resource intensive

Less useful in a TLS-everywhere world

Scariest result = Missing hosts

Recommendations

Know the weaknesses and strengths of each tool in your arsenal

Have at least one authenticated or agent-based VM source

Use at least one unauthenticated network scanner

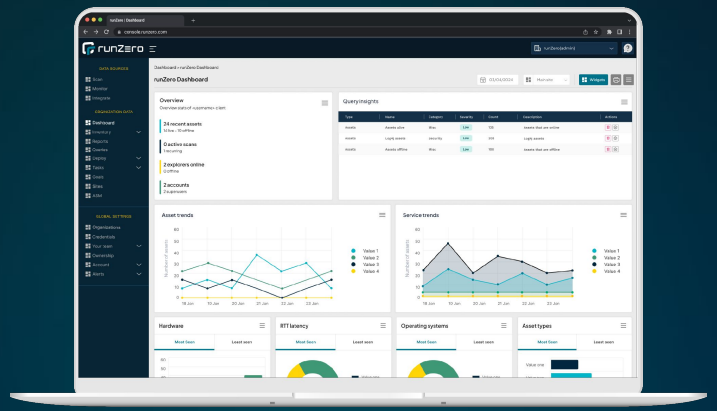
Track which systems are missing auth or agents

Verify default setting coverage

Table-top exercises help

- See Wendy Nather's keynote tomorrow!

Thank you!



runZero.com

runZero RESEARCH

research@runZero.com

References

Reports

- https://www.qualys.com/forms/tru-research-report/confirm/
- https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2025
- https://pentest-tools.com/benchmarks/network-vulnerability-scanners

Data Sources

- https://www.tenable.com/plugins/search
- https://secinfo.greenbone.net/nvts
- https://www.qualys.com/vulnerability-detection-pipeline/
- https://github.com/projectdiscovery/nuclei-templates
- https://www.rapid7.com/db/