Sentinelcore-Ai

WHITEPAPER · VULNERABILITY MANAGEMENT

Vulnerability Management That Survives a NIS2 Audit

From CVE firehose to risk-based remediation: prioritising with exploitation data and asset context, and keeping the records that prove it.

By Harsukh Singh

Eight years in security engineering, information security governance and identity

September 2026 · sentinelcore-ai.com

Free to share with attribution

EXECUTIVE SUMMARY

You can't patch everything. You can explain what you patched first.

Tens of thousands of new CVEs are published every year, and a typical estate matches far more of them than any team can fix. Sorting by CVSS score alone produces a queue that is both too long and wrongly ordered, because severity describes how bad a vulnerability could be, not how likely it is to be used against you.

NIS2 names vulnerability handling explicitly, and auditors increasingly ask not just 'are you patching?' but 'how do you decide what to patch first, and can you show it?'. This paper sets out a risk-based model built on three free, public signals, plus asset context, and the records that make it auditable.

What NIS2 expects

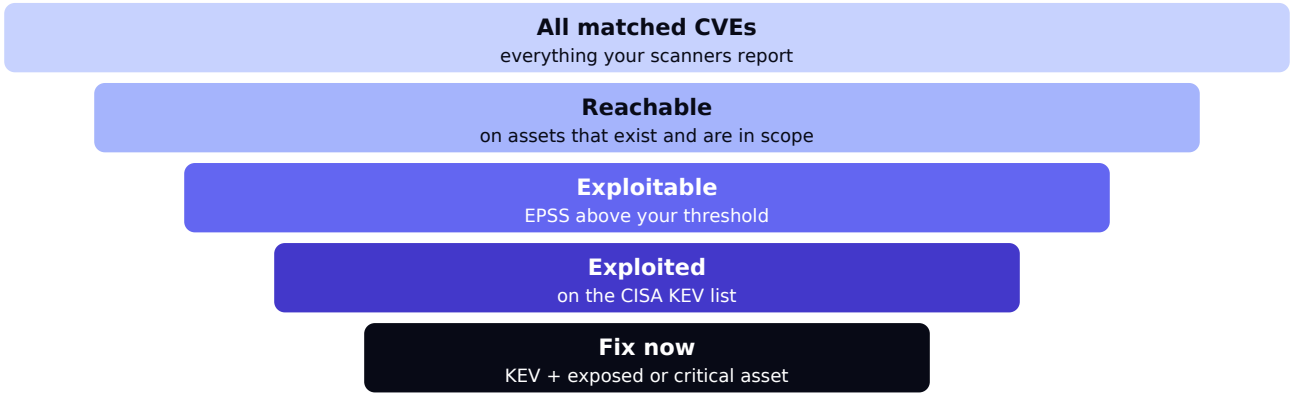
Article 21(2)(e) of Directive (EU) 2022/2555 lists 'security in network and information systems acquisition, development and maintenance, including **vulnerability handling and disclosure**' among the minimum measures. Article 21(2)(f) adds policies and procedures to assess the effectiveness of risk-management measures, and Article 12 establishes coordinated vulnerability disclosure and a European vulnerability database run by ENISA. In ISO/IEC 27001:2022 the corresponding control is Annex A 8.8, management of technical vulnerabilities.

> **What auditors look for**
> A complete asset inventory; a defined intake of vulnerability data; a documented prioritisation rule; remediation timelines by priority; exceptions with owner, reason and expiry; and evidence that the process runs continuously, not just before the audit.

Three signals that change the order

Signal	Maintained by	Question it answers
CVSS base score	FIRST (specification); NVD and vendors (scores)	How severe is this vulnerability in the worst case?
EPSS	FIRST	How likely is exploitation activity in the next 30 days? (a probability from 0 to 1)
Known Exploited Vulnerabilities (KEV)	CISA	Is there reliable evidence this is being exploited in the wild today?

Used together, these signals reorder the queue dramatically. A KEV-listed vulnerability on an internet-facing system is an emergency regardless of its CVSS score; a critical-scored vulnerability with a very low EPSS on an isolated test server can usually wait for the normal patch cycle.



Risk-based funnel: each layer removes noise, so the top of the queue is short and defensible.

Asset context: the fourth signal

The same vulnerability means different things on a public web server and on a lab laptop. Enrich every finding with the asset's exposure (internet-facing or not), criticality, the data it holds and its owner. This is where vulnerability management meets the asset register and the risk register: a vulnerability on an asset linked to a high-impact risk deserves a shorter deadline.

A practical prioritisation rule

Priority	Condition (first match wins)	Target
P1 — Emergency	On the KEV list and internet-facing, or on a critical asset	Days
P2 — High	On the KEV list; or EPSS high and CVSS high/critical	Weeks
P3 — Normal	CVSS high/critical with low EPSS	Next patch cycle
P4 — Low	Everything else	Routine maintenance

Set the actual deadlines in your own policy, approved by management, and apply them consistently. The point is a written, repeatable rule.

Better data in: fewer false positives, no duplicates

- **Use package-aware sources for software you build.** Open-source ecosystems (npm, PyPI, Maven, Go, crates and others) are better matched through OSV than through CPE strings.
- **Use your EDR's view for endpoints.** Defender for Endpoint, CrowdStrike and similar tools already know the installed versions on every device.
- **De-duplicate by CVE and product.** The same CVE reported by two sources, or on 300 laptops, is one decision with a device list, not 300 tickets.
- **Close automatically.** When a complete rescan no longer sees a vulnerability, resolve it and record when; reopen it if it returns. Never auto-close from a partial scan.

Remediation that leaves a trail

Remediation plans should state the fix (update, configuration change or compensating control), how it will be deployed (for example through Intune, SCCM or a package manager), how success will be verified, and how to roll back. Test on a representative device or a pilot group before broad deployment; automation drafts plans, it does not replace review.

Exceptions are part of the process

Some vulnerabilities cannot be fixed on time: a vendor has no patch, or a system cannot be restarted. Record a risk acceptance with a reason, a compensating control, an owner, and an expiry date, and review it when the expiry arrives. An exception register is strong evidence of a mature process, not a weakness.

The evidence pack

- ☐ Vulnerability management policy with the prioritisation rule and target timelines, approved by management.
- ☐ Asset inventory with owners, criticality and exposure.
- ☐ Scan coverage report: which sources, how often, which assets were included.
- ☐ Current findings by priority, with age, and the trend over the last 90 days.
- ☐ Sample of remediated findings with fix date and verification (rescan) evidence.
- ☐ Exception register with reasons, compensating controls and expiry dates.
- ☐ Coordinated vulnerability disclosure contact published for your own products.

How Sentinelcore-Ai helps

Sentinelcore-Ai merges findings from OSV and NVD, Microsoft Defender for Endpoint, CrowdStrike Spotlight and Azure, de-duplicates them by CVE, enriches each with CISA KEV and FIRST EPSS, groups device findings with their affected machines, auto-resolves findings a complete scan no longer sees, and drafts remediation plans for your deployment tools, always marked for testing before rollout. Findings flow into corrective actions and the evidence pack above.

References

Directive (EU) 2022/2555 (NIS2), Articles 12 and 21 · ISO/IEC 27001:2022, Annex A 8.8 · FIRST: Common Vulnerability Scoring System and Exploit Prediction Scoring System · CISA Known Exploited Vulnerabilities catalog · OSV (Open Source Vulnerabilities) · NIST SP 800-40 Rev. 4, Guide to Enterprise Patch Management Planning.

About the author

Harsukh Singh has spent eight years in hands-on cybersecurity work across security engineering, information security governance, and identity and access management. That work has meant building and running information security management systems to ISO/IEC 27001:2022, auditing them against the standard, and designing identity and access controls on Microsoft Entra ID, from conditional access and privileged roles to access reviews. Harsukh founded Sentinelcore-Ai to give security and compliance teams the tooling that work called for: posture measured against vendor baselines, findings tied to risks and corrective actions, and evidence an auditor can follow.