

VULNERABILITY
MANAGEMENT.

The continuous process of finding, prioritizing, and closing weaknesses before adversaries can use them. A **CVSS score alone** doesn't tell you what to fix first — exploitability and business context do.

- CVSS V4.0
- CISA KEV CATALOG
- EPSS
- PATCH SLAS

01 THE MECHANISM



Discovery & inventory
Asset discovery and continuous scanning surface every exposed service, package, and configuration — you can't patch what you don't know exists.



Risk-based prioritization
Severity, exploit availability, and asset criticality combine to separate the handful of vulnerabilities that matter from the thousands that don't.



Remediation & verification
Patching, configuration changes, or compensating controls close the gap — then a **rescan confirms the fix worked**.

02 THE FLOW

The Scan Cycle CONTINUOUS · DAILY / WEEKLY

1

Automated scanners and agents sweep the environment for **known CVEs, misconfigurations, and missing patches**.

2

Findings are **deduplicated and enriched with asset context** — internet-facing, crown-jewel, or isolated.

3

Results feed a **prioritized backlog** ranked by exploitability and business impact, not raw CVSS alone.

The Remediation Cycle PER SLA WINDOW

1

Tickets route to the asset owner with a **due date set by severity-based SLA** (e.g., Critical = 15 days).

2

The fix is applied — **patch, config change, or compensating control** — in a maintenance window.

3

A **verification scan closes the loop**, confirming the finding is resolved before it's marked closed.

03 SEVERITY & RESPONSE WINDOWS

SEVERITY	TYPICAL REMEDIATION SLA
Critical (CVSS 9.0–10.0 or KEV-listed)	15–24 days, often expedited further for internet-facing assets.
High (CVSS 7.0–8.9)	30 days from detection to verified fix.
Medium (CVSS 4.0–6.9)	90 days, typically bundled into a scheduled patch cycle.
Low (CVSS 0.1–3.9)	Best effort — closed at the next routine patch cycle.

04 PRIORITIZATION SIGNALS COMPARED

SIGNAL	SUFFICIENT ALONE?	WHAT IT MISSES
CVSS Base Score	No	Real-world exploitability and asset exposure context.
EPSS Score	No	The business impact of the affected asset.
KEV Catalog Membership	No	Asset criticality — confirms exploitation, not what it costs you.
Asset Criticality Alone	No	Whether the vulnerability is exploitable at all.
Combined Risk Score (CVSS + EPSS + KEV + Asset)	Yes	Blends severity, real-world exploitability, and business impact into one signal.

VULNERABILITY MGMT.

OPERATE · GOVERN · COMMUNICATE

05 PROGRAM OPERATIONS

Scan coverage must be continuous.

Point-in-time scans miss vulnerabilities introduced between cycles — agents and continuous discovery close that gap.

SLA breaches are a KPI, not a footnote.

Time-to-remediate against the SLA window is the metric that tells leadership whether the program works.

Exceptions need an owner and an expiration.

A risk acceptance without a review date becomes a permanent, forgotten exposure.

Rescan before you close.

A ticket marked "fixed" without verification is just an assumption.

06 CONTROL MAPPING

NIST SP 800-40

Guide to enterprise **patch management** planning and program structure.

CISA KEV CATALOG

Directive-backed list of vulnerabilities under **active, confirmed exploitation**.

PCI DSS V4.0

Requires **quarterly internal / external scanning** and risk-ranked remediation.

FIRST CVSS V4.0

Industry-standard **scoring framework** for vulnerability severity.

07 WHAT SCANNING DOES NOT SOLVE

Zero-days

Vulnerabilities with **no CVE or signature** yet are invisible to signature-based scanners by definition.

Business logic flaws

Application-level errors like price manipulation **don't appear in a CVE database**.

Shadow IT & unmanaged assets

You can't scan what your **asset inventory doesn't know exists**.

Third-party & supply chain

A vulnerable dependency in a vendor's code sits **outside your own scan scope** entirely.

08 MYTHS VS. REALITY

MYTH	REALITY
"A high CVSS score means fix it first."	A 9.8 on an isolated, non-internet-facing dev box is lower real-world risk than a 6.5 on a customer-facing system.
MYTH	REALITY
"Scanning once a quarter is enough."	New CVEs and exploits emerge daily — infrequent scans leave weeks of blind exposure between cycles.
MYTH	REALITY
"Patching everything eliminates risk."	Not every finding can be patched immediately; compensating controls and segmentation manage risk when patching isn't possible.
MYTH	REALITY
"If it's not in the CVE database, it's not a vulnerability."	Misconfigurations, weak credentials, and logic flaws create real exposure without ever getting a CVE ID.
MYTH	REALITY
"Vulnerability management is a security-team-only job."	SLAs are only met when asset owners across IT and engineering are held accountable to them.

09 SPEAK THE THREAT — KEY TERMS

CVSS

Common Vulnerability Scoring System — standardized **severity score from 0-10** for a vulnerability.

EPSS

Exploit Prediction Scoring System — estimates the **probability of exploitation** in the next 30 days.

KEV

Known Exploited Vulnerabilities catalog — CISA's list of CVEs with **confirmed real-world exploitation**.

CVE

Common Vulnerabilities and Exposures — the **unique identifier** assigned to a disclosed vulnerability.

SLA

Service Level Agreement — the **maximum allowed time** to remediate a finding based on severity.

ATTACK SURFACE

The complete set of **exposed assets, services, and entry points** an attacker could target.