

S202 SECURE & GOVERN · PRACTITIONER

Exposure Management

Prioritizing what attackers can reach and exploit, and reducing the attack surface itself.

FORMAT

Knowledge pack · 13 slides

FOR

Security leaders and teams

LEVEL

Practitioner



THE PREMISE

Patching alone cannot keep pace with an expanding attack surface

Vulnerability volume grows faster than remediation capacity. Exposure management concentrates effort on what is **reachable, exploitable and consequential**, and removes exposure that does not need to exist.

Reachable

On a path an attacker can use.

Exploitable

Exploited already, or likely to be.

Consequential

Critical systems and sensitive data.

CONTEXT

Vulnerability data and policy changed in 2026

263%

growth in CVE submissions between 2020 and 2025. NIST enriched nearly 42,000 in 2025, a record, but could not keep pace.

NIST, April 2026

3 groups

Since April 2026, NIST prioritizes enrichment of CVEs in KEV (target: one business day), in federal-use software and in critical software; others are not scheduled for immediate enrichment.

NIST, April 2026

BOD 26-04

CISA replaced BOD 22-01 and BOD 19-02 with federal deadlines, as short as three days, set by asset exposure, KEV status, exploit automation and technical impact.

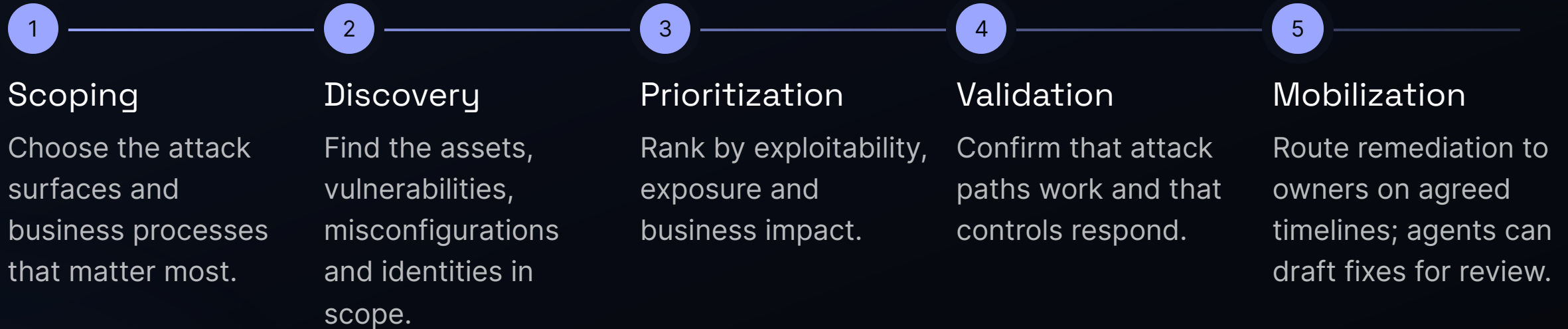
CISA, June 2026

NVD no longer routinely adds its own severity score where the CNA has provided one. Combine CNA and vendor data, exploitation evidence and your own context.

METHOD

Continuous threat exposure management in five stages

Introduced by Gartner in 2022. Each round of mobilization feeds the next round of scoping.



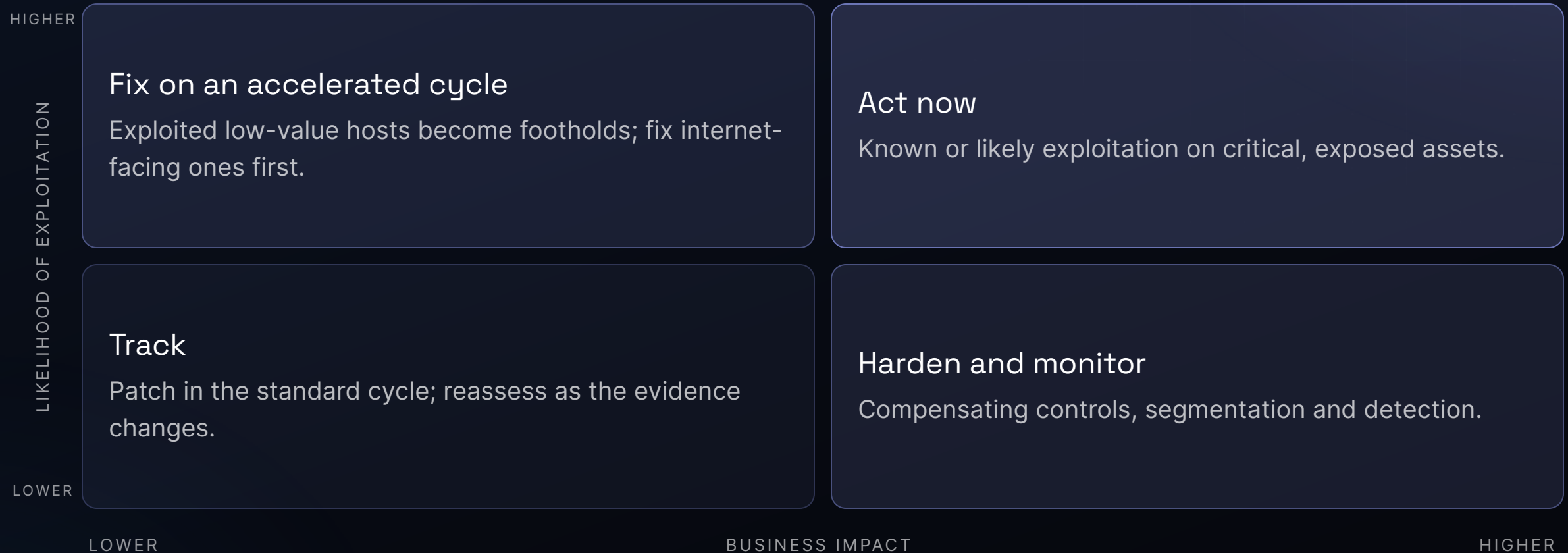
PRIORITIZATION

Prioritize with evidence, not severity alone

SIGNAL	WHAT IT TELLS YOU	SOURCE
CVSS	Base score: technical severity of the flaw, not risk in your environment	Vendor, CNA, NVD
EPSS	Probability of exploitation in the wild within 30 days	FIRST (version 5, 2026)
KEV	Exploitation has been observed in the wild	CISA catalog
Reachability	Whether the vulnerable code or service can be reached	Code analysis, exposure scans
Business context	Criticality of the asset and sensitivity of its data	Asset inventory, CMDB, data classification
SSVC	A decision in CISA’s tree: Track, Track*, Attend or Act	CISA and CERT/CC

DECISION

Combine likelihood and impact into action



ATTACK SURFACE

The attack surface is larger than the CVE list

Unknown assets

Internet-facing systems that IT does not know it runs.

Misconfigurations

Open storage, permissive policies, exposed management interfaces.

Non-human identities

Service accounts, keys and tokens, often over-privileged and long-lived.

Third-party connections

OAuth grants and integrations into SaaS and partners.

Software supply chain

Dependencies, build systems and update channels.

AI systems and agents

Agents and MCP servers that hold credentials and act on other systems.

IDENTITIES

Non-human identities need a lifecycle

The OWASP Non-Human Identities Top 10 (2025) begins with improper offboarding and secret leakage.

- ✓ **Inventory**
Every service account, key, token, certificate and agent identity.
- ✓ **Least privilege**
Permissions matched to actual use.
- ✓ **Secret hygiene**
No secrets in code, logs or tickets.
- ✓ **No reuse**
One identity per workload, and none used by people.
- ✓ **Ownership**
A named owner for each identity.
- ✓ **Short-lived secrets**
Rotation, or credentials issued per session.
- ✓ **Environment isolation**
Separate identities for production and test.
- ✓ **Offboarding**
Removed with the system or integration it served.

SUPPLY CHAIN

Know what you run, and where it came from

SBOM

A machine-readable list of components. Current releases: CycloneDX 1.7 and SPDX 3.0.1.

Minimum elements

Joint 2026 guidance replaces NTIA's 2021 list, adding component hashes, licenses and SBOM author signatures.

VEX

Per-product status: not affected (with a justification), affected, fixed or under investigation.

AI bills of materials

Models, datasets and their provenance; G7 minimum elements (May 2026); in CycloneDX since 1.5 and SPDX since 3.0.

STRUCTURAL REDUCTION

Remove exposure that serves no purpose

Retire

Applications that no longer serve a necessary purpose.

Disable

Unused features, APIs and protocols.

Consolidate

Overlapping platforms with fragmented controls.

Revoke

Unused privileges and stale identities.

Remove

Integrations that have outlived their process.

Modernize

End-of-support software and devices that no longer receive patches.

MEASUREMENT

Measure exposure removed and validated

Time to remediate KEV

On internet-facing assets, by asset criticality.

Validated exposure

Share of critical assets whose attack paths were tested.

Exposure removed

Assets retired, privileges revoked, integrations removed.

Inventory accuracy

Share of discovered assets that were already known.

Expired exceptions

Risk acceptances past their expiry date.

Identity hygiene

Non-human identities with an owner and rotation.

PITFALLS

Why vulnerability programs plateau

✗ Prioritizing by CVSS alone

✓ Add exploitation evidence and context

✗ Reporting ticket closures

✓ Report exposure reduced on critical assets

✗ Tickets without context

✓ Route to owners with the evidence and the fix

✗ Permanent exceptions

✓ Every acceptance expires and is reviewed

✗ Ignoring identities

✓ Manage non-human identities as exposure

✗ Defending what is unnecessary

✓ Retire it, and remove the obligation

SUMMARY

Key takeaways

- 01 Focus on what is reachable, exploitable and consequential.
- 02 Run exposure management as a cycle: scope, discover, prioritize, validate, mobilize.
- 03 Prioritize with EPSS, KEV, reachability and business context alongside CVSS.
- 04 Treat non-human identities and the supply chain as part of the attack surface.
- 05 Retiring unneeded systems, access and integrations removes exposure permanently.

NEXT COURSE · O201

AI in IT Operations

Operate · Practitioner