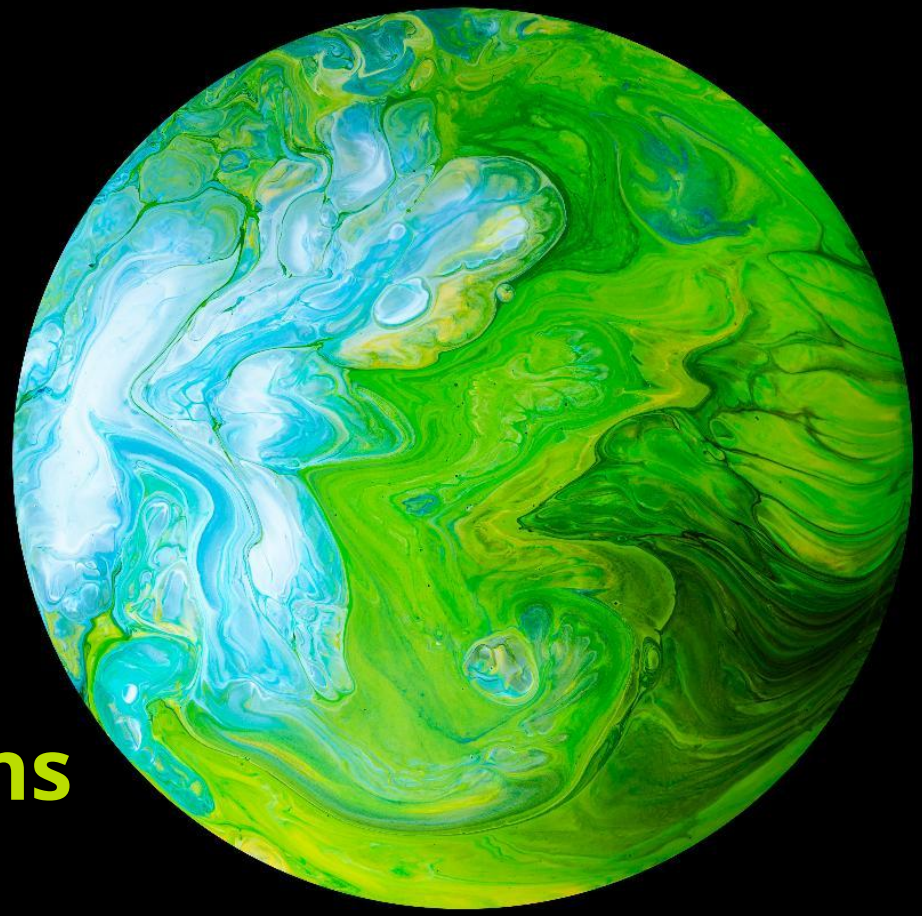
Deloitte.

Together makes progress



Deloitte Cyber

Machine Speed, Human Decisions

Enterprise Cyber in the Age of AI Led Vulnerability Discovery

May 2026

The inflection point

Machine Speed, Human Decisions — Enterprise Cyber in the Age of Artificial Intelligence (AI) Led Vulnerability Discovery

The assumption that bought you time is no longer valid.

Current vulnerability management processes assume you have days or weeks between discovery and exploitation. With the latest developments in AI led vulnerability discovery, the scale and pace of discoveries has increased thereby increasing downstream cyber risks.

What HASN'T changed

Existence of vulnerabilities in enterprise systems

What HAS changed

The window between discovery and exploitation has collapsed →
from months to hours

Why this is different?

Discovery speed

AI models find critical flaws rapidly, increasing volume and velocity exponentially

Organisational readiness

VM programs were designed for a world of scarce findings. That architecture does not scale.

Regulatory Expectations

Regulators and boards will likely increase the bar for disclosures and accountability: "when did you know it?", "how fast did you act?"

Why this matters to you

Organisation will likely have to manage the gaps between vulnerability identification, remediation and acceptance – and at scale and pace.

Discovery vs remediation gap: AI finds critical vulnerabilities in hours, while enterprises still take weeks to fix them.

Organisational constraints dominate: Testing, approvals, deployment, and legacy environments—not discovery—now limit risk reduction.

Risk accumulates downstream: The widening gap between finding and fixing vulnerabilities is where enterprise cyber risk concentrates.

What this demands

Responding to AI-accelerated vulnerability discovery is not just about tools. It requires rethinking how the entire cyber operating model absorbs, prioritises, and acts on a fundamentally higher volume and velocity of findings.

PEOPLE

From finding to deciding

- As AI scales discovery, the **talent premium shifts from finding issues to making fast, business-aware decisions** on what risks matter most.
- Security teams must be staffed and **upskilled for decision velocity** - able to triage at scale, assess business impact, and communicate priorities clearly

PROCESS

From quarterly cycles to continuous response

- **Traditional** periodic **VM cycles break down under** continuous, **high-volume discovery**.
- **Organisations need processes that enable decisions within ~48 hours**, supported by clear escalation paths, explicit risk criteria, SBOM visibility, and rapid third-party coordination.

TECHNOLOGY

From scanning to orchestration

- The **challenge is no longer scanning, but orchestrating and prioritising remediation** from a flood of AI-generated findings.
- This **requires** near **real-time** asset **intelligence**, exploitability **validation**, threat intelligence **correlation**, and **remediation** workflows

The case for investing now

- Frontier **AI can find** critical **vulnerabilities**, but **layered defenses are still needed to help prevent** successful **exploitation**.
- **Defense in depth**—segmentation, boundary hardening, and access controls—**has proven resilient** even **against advanced AI**.
- **Organisations that invested early** in hardening, remediation maturity, and visibility **are better positioned to protect themselves**; laggards face accelerating risk.

How should organisations respond

The response cannot only be a tool buy or just a patch sprint — it is a holistic rethink

Every organisation's starting point is different. Organisations should get out of the trap of reacting to signals and establish a strategic approach to redesign their vulnerability and attack surface management programs.

The following questions provide a framework that organisations can use to evaluate their response:

PRIORITY	KEY QUESTIONS
Visibility & Inventory	Do you know what software runs in your environment, what's inside it, and who owns it? Can you produce a current software bill of materials for your critical systems?
Decision Velocity	Can your organisation move from 'new critical finding' to 'risk accepted or remediated' in 48 hours? Who has authority to make that call, and does the escalation path actually work under pressure?
Remediation Velocity	What is your honest mean time to remediate for critical vulnerabilities? Can you shrink it materially? Are your SLAs and change control processes built for the volume and speed that's coming?
Segmentation & Hardening	For systems you cannot patch quickly—legacy applications, OT environments, critical infrastructure—are compensating controls, segmentation, and boundary hardening sufficient to contain the blast radius of a compromised component?
Pipeline Integration	Are your development and deployment pipelines prepared to host AI-driven security assessment as a native step—not a quarterly bolt-on? Shifting security left is no longer aspirational; it's operational necessity.
Board & Regulatory Readiness	Can you articulate your vulnerability posture, remediation strategy, and risk acceptance decisions to your board and regulators in clear terms? As disclosure velocity increases, so does accountability.

Its not about speed, its about velocity.

The most resilient organisations are not the ones that move fastest, but the ones that move fast with a purpose and built the right foundations.

How to get started

Pragmatic, phased, and focused on building for resilience

DO NOW – Next 30 days

Risk Surface and Quick Wins

- Close the patch gap – based on your business priorities
  - Establish emergency change procedures
- Inventory your attack surface - visibility into your highest-risk exposures based on business impact
- Fix identity fundamentals – eliminate static credentials, fix MFA and make it hard for the attacker
- Compliance and regulatory implications mapped to your environment

DO NEXT – Next 90 days

Rapid remediation and exposure reduction

- Scale vulnerability management program for 10X volumes
- Build software composition visibility – SBOMs for critical systems
- Shift security left into CI/CD
- Reassess third party risks and exposure through vendor systems
- Proactively scan your own code – AI led scanning and vulnerability management

DO LATER – Next 180 days

Strategic reset and resilient capabilities

- AI for cyber transformation – beginning with a AI augmented security operations
- Extend zero trust architectures – the age of micro authentication and micro cryptography is here
- Implement continuous autonomous red teaming
- Multi-incident IR readiness, materiality and disclosure playbooks
- Technical resilient architectures and infrastructure

What you walk away with

Clear visibility into your **risk posture**, **demonstrable outcomes in reducing exposure** and a **roadmap to transform the risk governance** for your organisation – not just a framework.

How we can help

Deloitte can provide end to end services to evaluate and strengthen vulnerability management operating models for the AI era

Executive support

Board/CISO briefing pack

Translate technical exposure into business scenarios, decision points, and near-term funding asks.

Executive tabletop refresh

Run scenario where newly discovered flaw in core system is weaponised before normal change windows are complete.

Critical asset & software supply chain

Crown-jewel / Minimum Viable Company (MVC) exposure map

Assess critical business processes, systems, apps , identities, and vendors whose compromise would create outsized business or regulatory impact.

Software and dependency visibility review

inventory high-risk open-source dependencies, inherited components, and unsupported software in priority environments.

Detection and defense

AI enabled threat hunt

Identify existing threats within the environment impacting prioritised business assets

SOC defense review

Upgrade your cyber defenses within the SOC to detect and respond to these types

Vulnerability response

Vulnerability response recalibration

Compare current SLAs to a faster exploit environment and reset thresholds for critical internet-facing assets.

Why Deloitte

The partner who sees the whole enterprise — and knows how to move it

Decades of experience

Deloitte has built vulnerability management programs and security frameworks across Fortune 500 enterprises in every major industry. We know what works in complex, regulated environments.

Cross-functional reach

Deloitte connects cyber, engineering, compliance, risk, supply chain, and operations in one conversation. We can find what others may miss when they only look at one function.

We know the industry

Deloitte is actively working with ecosystem players across frontier model providers, hyper-scalers, startups and academia to bring a holistic approach to you. Some of our representative relationships include:

- Anthropic
- AWS
- Google
- Nvidia
- Cisco
- Palo Alto
- CrowdStrike
- SailPoint
- Ping Identity
- ServiceNow

Business-first approach

Deloitte understands your constraints — regulatory obligations, existing investments, operational realities. We build solutions that fit your business, not a generic playbook.

Ready now

Deloitte has stood up a dedicated team to respond to this moment. We can mobilise quickly, deliver early value in three weeks, and give you a full picture in six weeks.

Connect with us

Sathish Gopalaiah
President, Consulting
Deloitte South Asia
sathishtg@deloitte.com

Gaurav Shukla
Partner and Leader - Cyber
Deloitte South Asia
shuklagaurav@deloitte.com

Anand Tiwari
Partner
Deloitte India
anandtiwari@deloitte.com

Ashish Sharma
Partner
Deloitte India
sashish@deloitte.com

Santosh Jinugu
Partner
Deloitte India
sjinugu@deloitte.com

Lakshmi Allamsetty
Partner
Deloitte India
lallamsetty@deloitte.com

Srimant Acharya
Executive Director
Deloitte India
srimacharya@deloitte.com

Deloitte.