FS-ISAC

Where Trust Meets Action

# Sector Risk Advisory:
# Preparing the Enterprise for AI-Enabled Vulnerability Discovery

19 April 2026

TLP WHITE

FS-ISAC
Where Trust Meets Action

# Sector Risk Advisory

Preparing the Enterprise for AI-Enabled Vulnerability Discovery

Recent announcements of AI frontier models' advanced vulnerability discovery and chaining capabilities to create exploits indicate an important change in the risk landscape for financial services. Traditional assumptions and approaches for vulnerability management no longer hold. FS-ISAC recommends the following as part of a fundamental shift in operations to manage cybersecurity and resilience risks:

## 1. Aggressively remediate known risk

*Start with what you already know and remediate with urgency*

- Patch external systems first, then move to internal systems
- Eliminate long-standing exceptions where patches exist – don't assume compensating controls suffice
- Treat vulnerability backlogs as operational risk, not compliance debt
- Set expectations across business, technology, cybersecurity, and resilience leadership that prioritize burn-down over non-critical updates, upgrades, and product launches

> **Why this matters:** Clear the decks. More vulnerabilities are coming - do not fall further behind. We have an unknown window before threat actors have access to the new capabilities and we need to move with speed to address what is known while preparing to change our processes for the long haul.

## 2. Harden the perimeter

*Make it harder for adversaries to get in and buy more time for detection*

- Put more distance between attackers and systems by using content delivery networks (CDNs), managed hosting, and cloud edge controls
- Strengthen front-line defenses by expanding Web Application Firewalls (WAF) capabilities and modernizing perimeter defenses
- Introduce controlled delay in adopting new open-source software or models to allow time to detect and remediate vulnerabilities prior to deployment
- Consider internal tripwires/deception to detect novel intrusion methods

> **Why this matters:** AI tools allow adversaries to rapidly cross-reference known, published vulnerabilities against specific software versions and immediately


 

> attempt exploits. Vulnerability backlogs can become a roadmap for targeted attacks. They are likely to get further, faster than ever before.

## 3. Realign vulnerability prioritization and compress patch timelines

*Assume exploit in vulnerability prioritization processes*

- Update vulnerability prioritization processes to assume active or imminent exploitation of every vulnerability default
- Assign greater weight to externally facing vulnerabilities regardless of ease or known past exploitation, moving beyond CVSS-only scoring
- Build or optimize automated test harnesses to embed, automate, and test every code change or deployment across all applications
- Participate in vendor programs, where available, to gain early or private access to fixes before they are released publicly
- Compress remediation service level agreements (SLAs) to days, not weeks, and automate prioritization decisions to ensure the most severe findings get to the right teams immediately

> **Why this matters:** Traditional vulnerability scoring and remediation timelines were designed when exploit development took longer and adversaries had to make choices about where to focus effort. AI eliminates these constraints, including weaponizing vulnerabilities that were previously considered low priority. Prioritization logic that hasn't been updated to reflect this reality will direct attention too slowly and to the wrong problems.

## 4. Validate and update critical asset inventories and third parties

*Ensure a clear and current picture of your systems*

- Maintain a real-time asset inventory, including dependencies and connections, to support same-day decisioning as risks emerge
- Know the internet-facing exposures, including third parties


 

> **Why this matters:** AI gives adversaries the ability to map an institution's external attack surface quickly and systematically. Investing in internal visibility with the same urgency applied to external defenses will close the response gap during an exploit.

## 5. Replace end-of-life technology

*If it is no longer actively supported, remove it*

- Update software and hardware to current versions
- Replace unsupported or end-of-life technologies with an actively maintained version
- Set a minimum freshness standard for internal systems and for third-party software to fall no more than two major versions behind (N-2)

> **Why this matters:** AI-assisted tools can rapidly identify which software versions an organization is running and immediately cross-reference known vulnerabilities for those versions. Outdated systems are essentially pre-labeled targets. Staying current removes the easiest attack surface before adversaries can exploit it.

## 6. Shift mindset from vulnerability management to exploit prevention

*Contain and block attacks before they spread*

- Implement network segmentation, access controls, and isolation between systems to limit internal movement of breaches
- Block exploits in progress through WAFs, intrusion prevention systems, runtime application protection, and other controls that intervene, not just observe
- Update playbooks where necessary to reflect quick containment of exploits that may result in service disruptions

> **Why this matters:** AI-assisted attacks move faster than human response teams can track. Strategies dependent on detection and reactive remediation will fall behind. Shifting the emphasis to prevention and pre-planned containment reduces dependence on response speed and ensures that – when an attack does succeed – its impact is contained before the response team has fully assembled.


 

## 7. Use available AI models for risk identification and remediation

*Fight AI with AI and use what you can get*

- Use AI to triage, monitor, and respond to security alerts at machine speed
- Train and empower cyber defenders to leverage AI to enhance vulnerability detection and remediation, red teaming, and testing
- Empower developers to leverage AI to detect and remediate vulnerabilities prior to code deployment
- Use predefined threat conditions to trigger automated containment, such as isolating affected systems, blocking malicious traffic, and revoking compromised credentials
- Implement governance over the use of AI tools to include defined guardrails with human oversight

> **Why this matters:** Each generation of model will likely find more vulnerabilities, faster and more creatively than the prior generation. There is still value in using what is available to reduce the exposure prior to general availability of the new state-of-the-art.

## 8. Align accountability and expectations across teams

*Faster threats require clearer ownership and stronger coordination*

- Build security metrics into team objectives, measuring system owners' patch velocity and platform currency on par with system performance
- Treat remediation speed as a reliability metric, reporting to governance committees and the Board of Directors as part of operational risk
- Reset expectations across business, technology, cybersecurity, and resilience leaders that this fundamental shift in the risk landscape will mean a new approach to business as usual

> **Why this matters:** Stakeholders across institutions – from technology teams to business leaders who control resource allocations – need to carry explicit, measured responsibility for the security of what they own and fund. Embedding accountability within performance objectives across functional teams will help turn security policy into security outcomes.


 

## 9. Embrace collaboration

*Don't go at it alone*

- Share threat intelligence through FS-ISAC's platforms to support and benefit from information sharing of emerging risks across financial services
- Proactively engage with FS-ISAC, collaborating with peer institutions and supply chain partners to identify vulnerabilities, and developing and testing remediations prior to vulnerability disclosures
- Coordinate through FS-ISAC to support a rapid, collective response and contain impact, improving resilience for the financial system

> **Why this matters:** AI innovation is advancing rapidly, creating new opportunities and challenges for financial institutions. No single organization has the visibility to see the full range of emerging threats or the ability to respond quickly and comprehensively on its own. Collective action helps rebalance the advantage away from the attacker and towards the cybersecurity and resilience of the financial system. The suppliers are going to be busier than ever and need the leverage of scale that the FS-ISAC offers to share critical intelligence across the sector.


 