



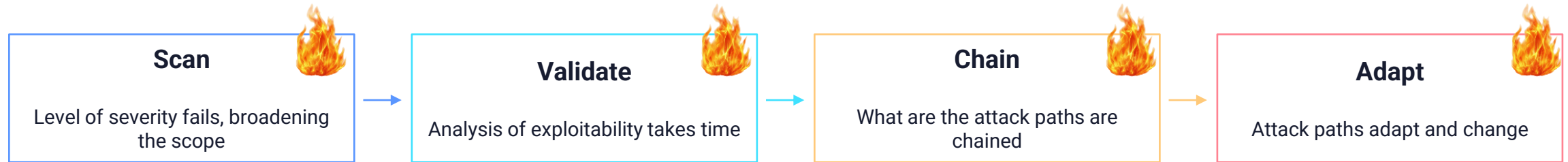
Punching through the noise.

What AI vulnerability detection really changes, and what it doesn't.

Karine Goris

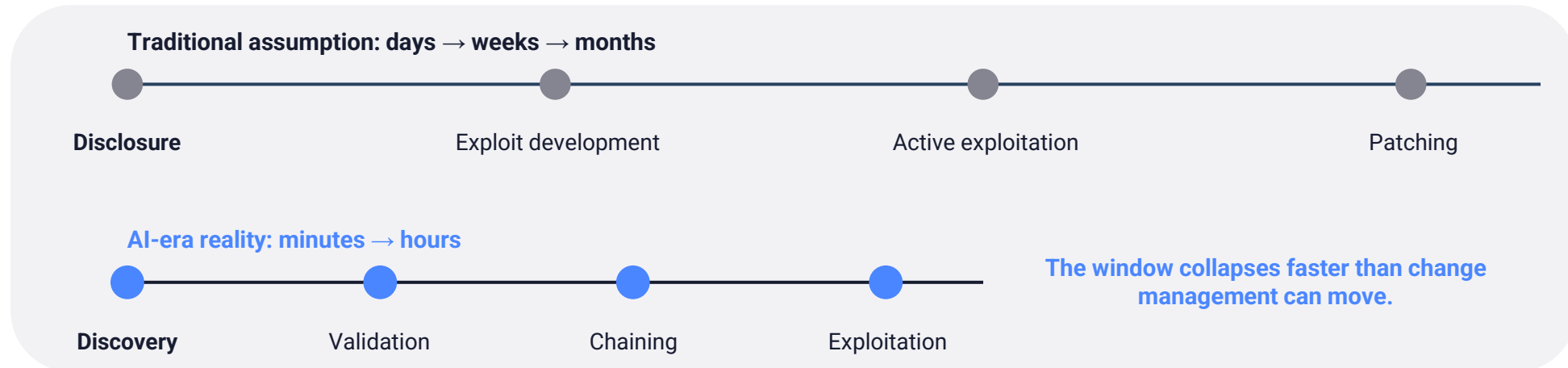
What AI-driven vulnerability discovery changes: From assistance to autonomy

The technique is familiar. The operating speed is not.



The result: continuous, persistent exploitation pressure across the whole environment.

This is not a new class of cyberattack. It is an **increase** in **scale**, **speed** and **persistence**.



What AI-driven vulnerability discovery changes: traditional operations under pressure

Speed

Discovery, triage and evidence move faster.

Scale

More assets, suppliers, code and configurations to be analyzed.

Sophistication

Weak signals can be correlated into attack paths and exploitability.

Collaboration

Enlarging the scope to the end-to-end ecosystem.

A practical response model: four streams of action

1

Cybersecurity foundations

AI makes execution more urgent

2

Perimeter vulnerability management

Understand the exposure continuously

3

Third-party vulnerability management

Look beyond the perimeter into the ecosystem

4

Frontier AI vulnerability testing

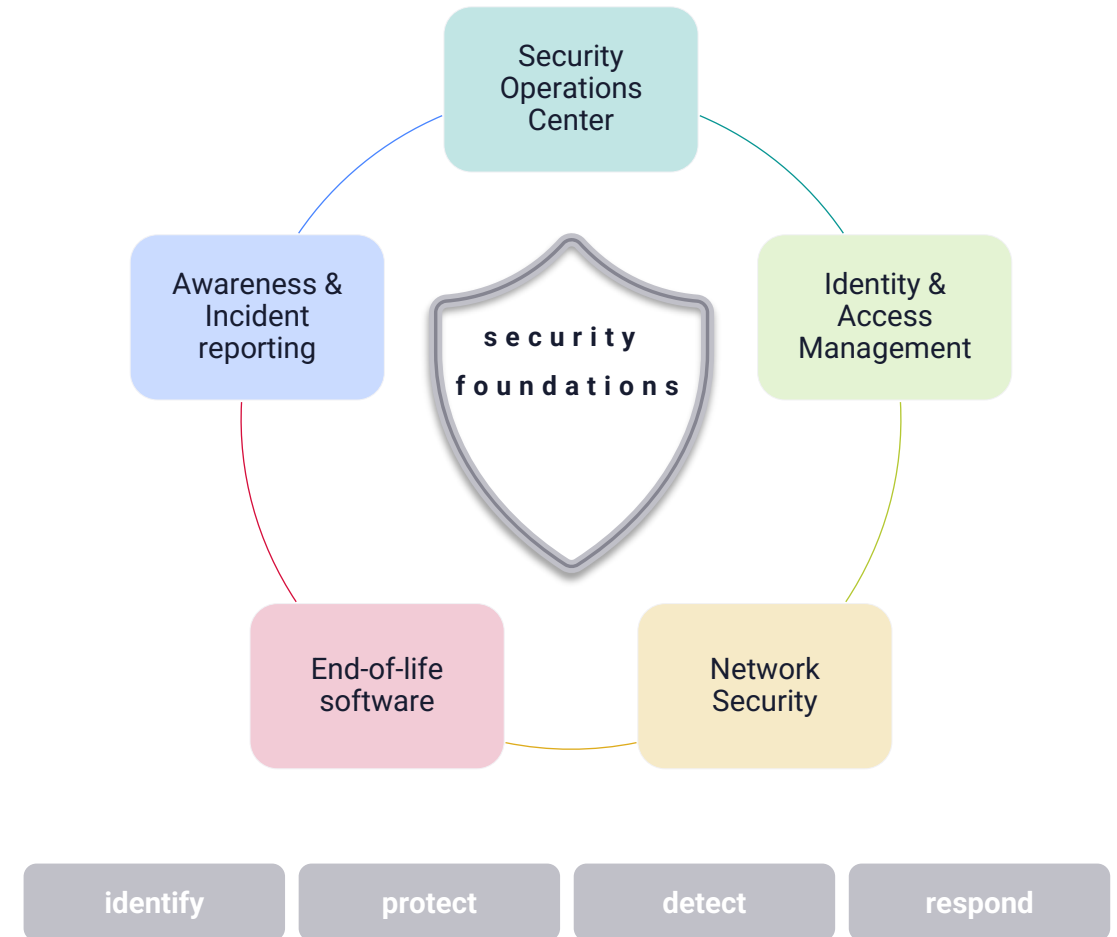
Use AI to fight AI threats, helping to work experts faster

1. Cybersecurity foundations

AI does not replace security fundamentals; it makes execution more urgent.

Key observations

- AI accelerates cyber threats, while traditional security controls remains vital, but they must evolve to counter AI driven attacks.
- As the attack surface grows (identities, apps, third parties), a proactive, organization-wide security approach is key, based on a security culture where people are well informed on the risks and how they can help defending against the risk.
- Weaknesses like outdated software or poor IAM controls become riskier with AI.
- Resilience depends on both tech and vigilance—reporting threats quickly is essential, putting pressure on your monitoring systems and incident response playbooks.



2. Vulnerability Management

Focus is evolving from internet-facing, high-criticality assets to a more holistic model, requiring accelerated and broadened mitigation coverage

Key observations

- Vulnerability management is shifting from high-criticality, internet-facing issues to a [risk-based approach](#).
- AI changes the threat landscape: risks now come from [chaining multiple low-risk weaknesses](#), not just single critical flaws.
- Severity ratings alone aren't enough—we now [address vulnerabilities at all levels](#).
- [Expand coverage](#) from the perimeter to code/libraries, using tools (pen testing, bug bounty, scanning) to mitigate risks at every level.

Internet-facing assets

Cloud exposure

Misconfigurations

Exploitable services

Shadow IT

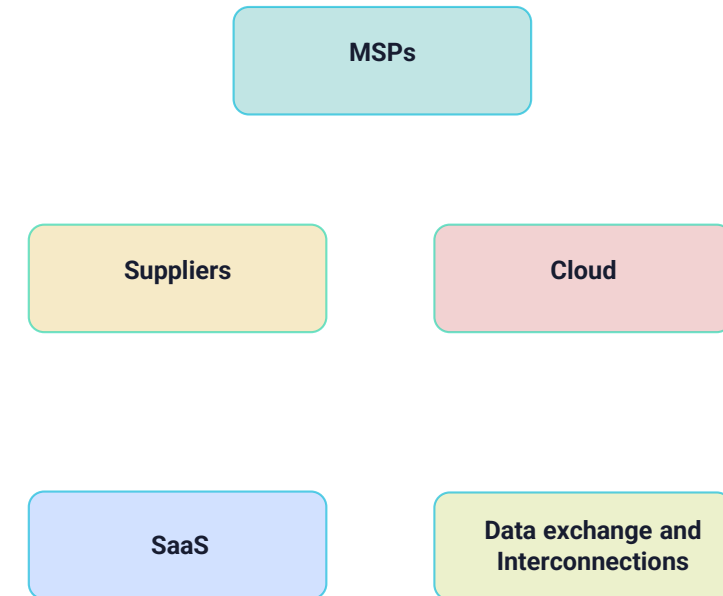
Chaining

3. Third Party Vulnerability Management

Existing third-party risk governance remain robust, but the scope should be broadened to cover all relevant digital interconnections

Key observations

- AI-driven threats **expand our risk scope** beyond traditional suppliers to all connected parties, classified by **interconnection type**.
- **Third-party risk frameworks must include AI cyber risks** and reassess existing providers where needed.
- **Evaluate vulnerability exposure** (attack surface, fourth-party risks) alongside security maturity and incident history.
- Prioritize and mitigate risks across the **extended ecosystem**.



4. Frontier AI Vulnerability testing

Vulnerability testing evolves towards a frontier-AI-ready model: AI-augmented, context-aware, and always-on rather than static and periodic

Key observations

- AI lowers the attack barrier, enabling fast, large-scale exploitation of zero-day and N-day vulnerabilities.
- Traditional Static Application Security Testing (SAST) falls short: lacks context, misses complex flaw chains, and creates false positives requiring manual review.
- The shift to AI-powered, context-aware scanning, treating remediation as an automated supply-chain problem to speed up patching.
- Move to continuous scanning, replacing periodic checks with AI-augmented Dynamic Application Security Testing (DAST).

Model & prompt security

Data leakage

AI supply chain

Abuse monitoring

Tool / agent permissions

Human oversight

