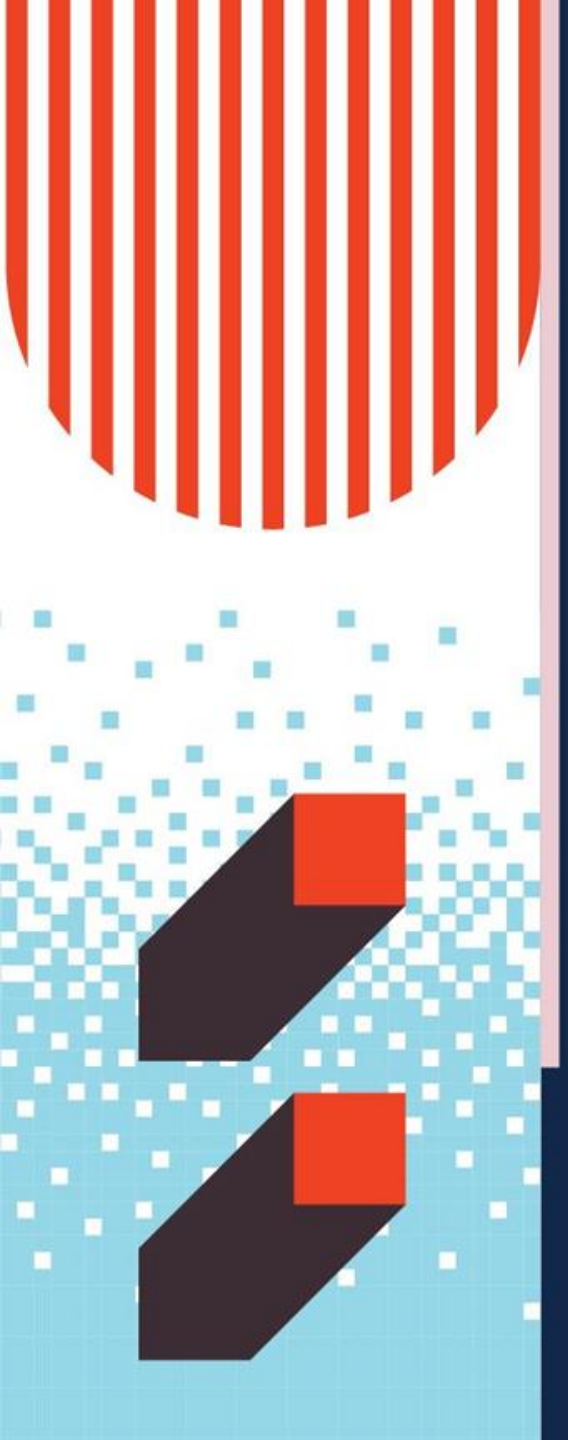


IAPP **AI Governance Global Europe 2026**

Training 1-2 June
Workshop 2 June
Conference 3-4 June
DUBLIN

#IAPPAIGG26

Operationalizing AI Governance Before the Incident

Why organizations need an AI Incident Response Plan before the next AI incident

Welcome and Introductions

Zach Burnett

CEO, RadarFirst

Alex Layng

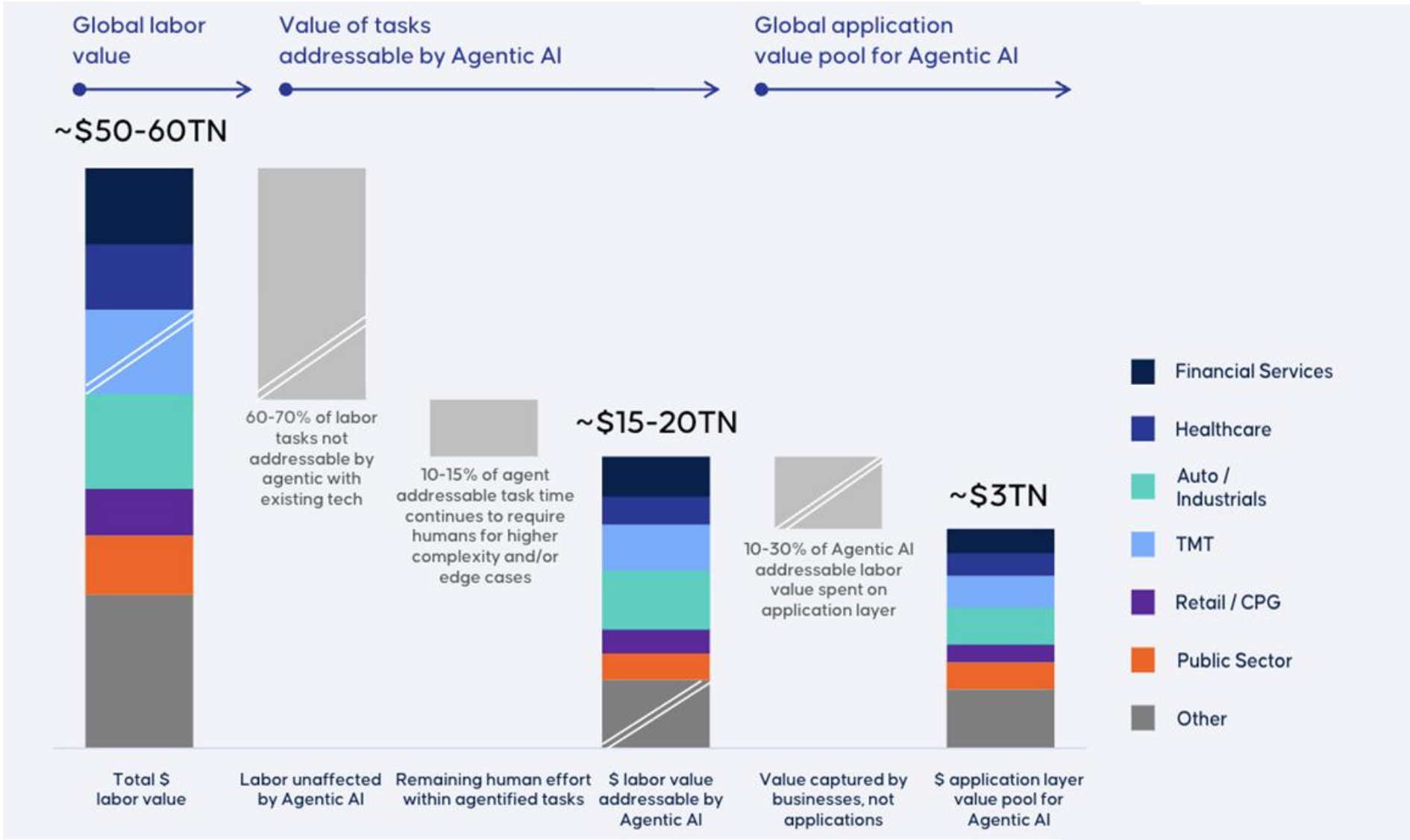
VP of Product, RadarFirst

The stage is set for AI incidents

AI is becoming operational infrastructure faster than incident response models are maturing

Why agentic AI is being embraced by business

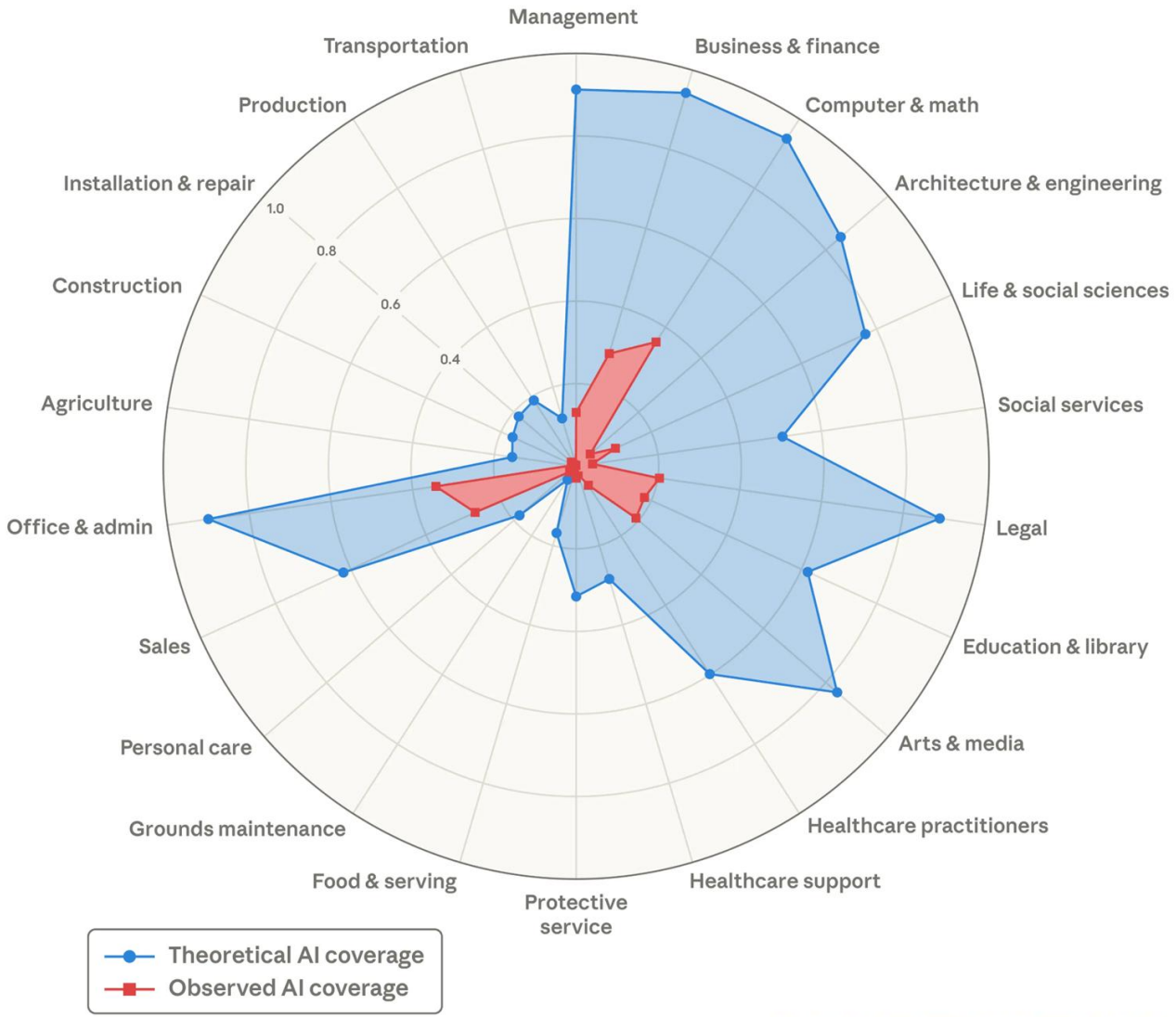
Agentic Enterprise Solutions Could Capture $3TN of the Current Value of Global Human Labor



Source: Google + BCG AI TAM model, as of 03/2026

The constraint is not capability - it is operationalization

Theoretical capability and observed usage by occupational category



Source: 'Labor market impacts of AI: A new measure and early evidence' (2026) Anthropic
https://www.anthropic.com/research/labor-market-impacts

AI incidents are **different**

AI incidents are higher volume, harder to classify, and broader than traditional cyber/privacy events

Incident volume is high - and growing

1 in 6 **data breaches involved AI driven attacks.**

On average, 16% of data breaches involved attackers using AI, most often for AI-generated phishing (37%) and deep fake impersonation attacks (35%).

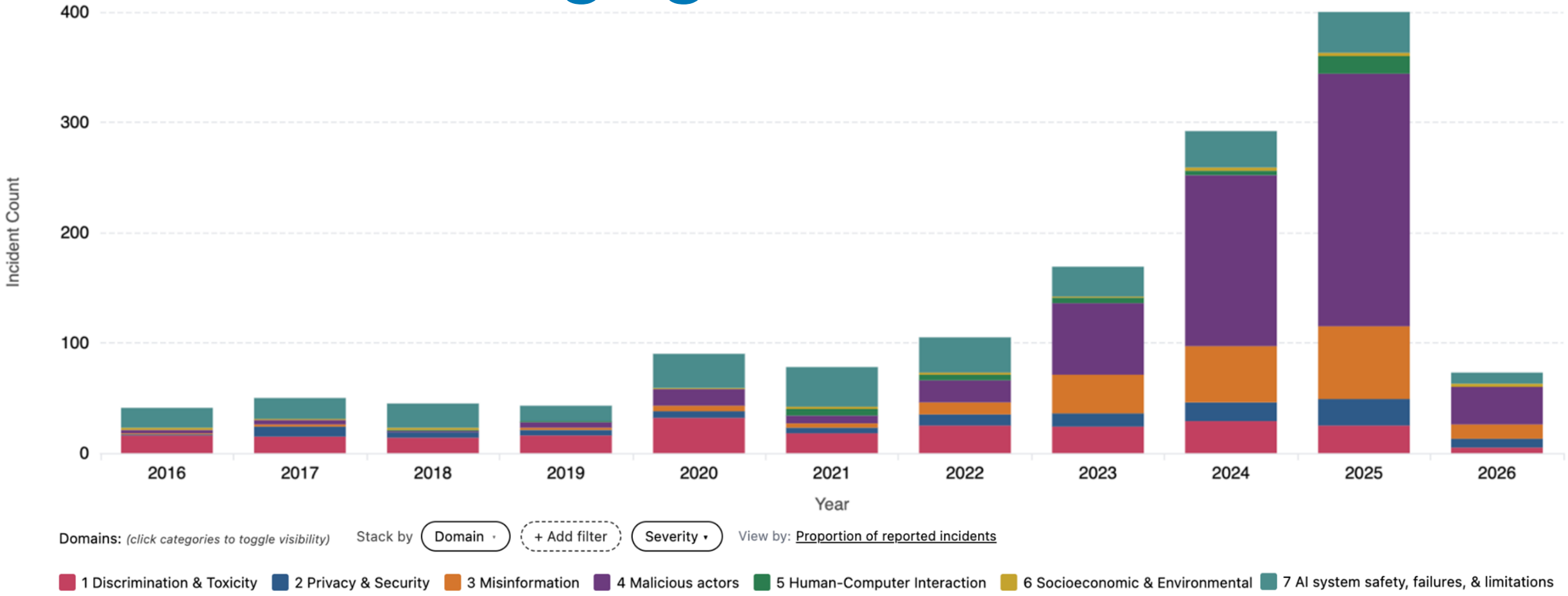
Source: IBM 'Cost of Data Breach Report 2025'

14.9K

AI incidents and hazards listed in the OECD AI Incidents Monitor from public sources (as of May 2026).

Sources: OECD AI Incidents Monitor, accessed May 2026; IBM 'Cost of Data Breach Report 2025'

How are numbers of reported AI Incidents changing over time?



Source: MIT AI Risk Repository, airisk.mit.edu

AI changes the incident equation

Exploit windows are collapsing

Attackers move faster than ever.

771 DAYS (2018) → **<4** HOURS (2024) → **<1** HOUR (BY END OF 2026)

Median time from vulnerability discovery to weaponized exploit

Source: ArmorCode "The Claude Mythos Security Playbook."

AI is transforming businesses

Organizations are moving from pilots to transformation.

34% Using AI to transform the business

30% Redesigning core processes around AI

Source: Deloitte "The State of AI in the Enterprise"

AI risk is inherently ambiguous

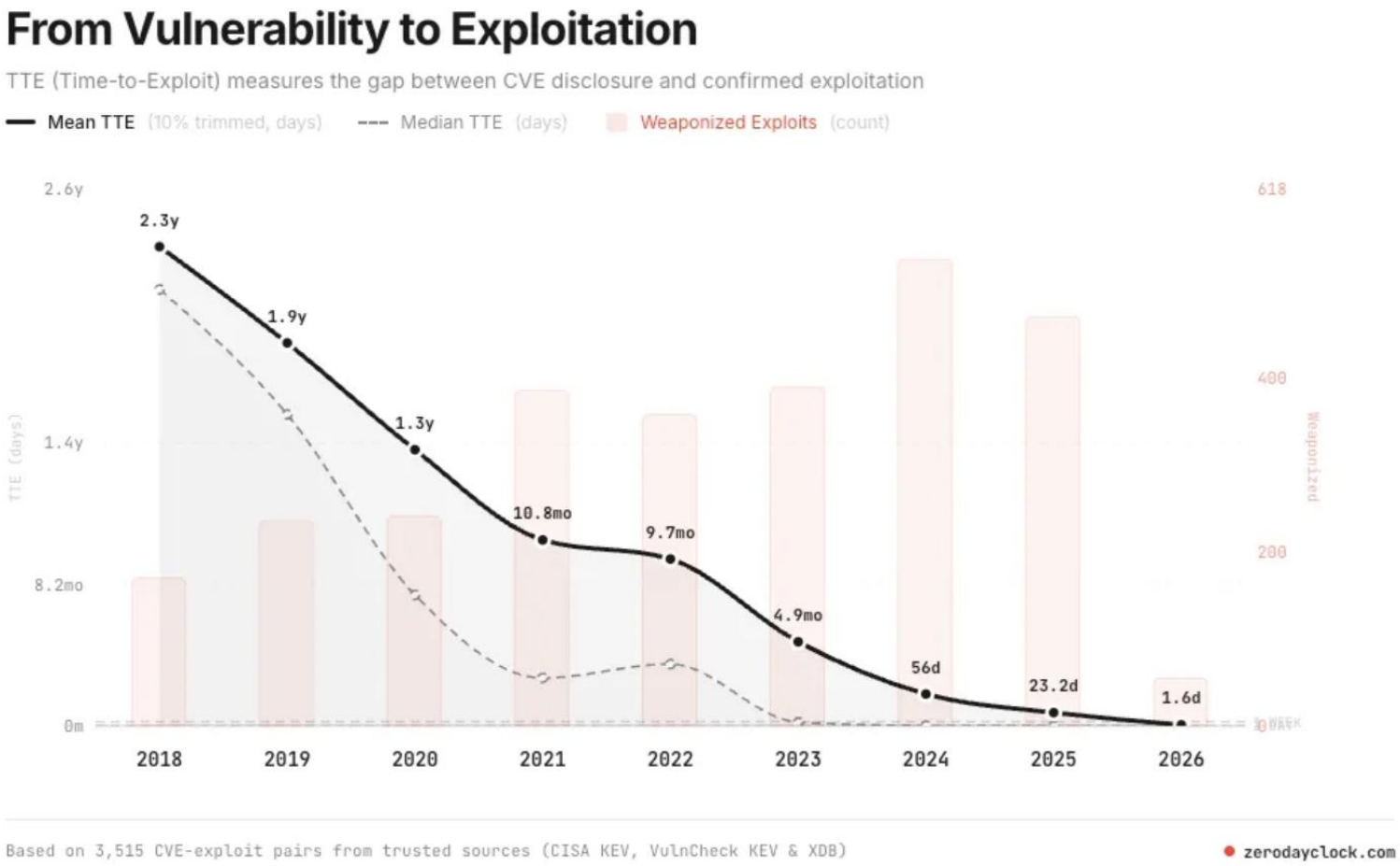
Definitions vary, making response harder and slower.

AI incident databases are emerging to standardize ambiguous AI risk and incident definitions.

(incident database AI)

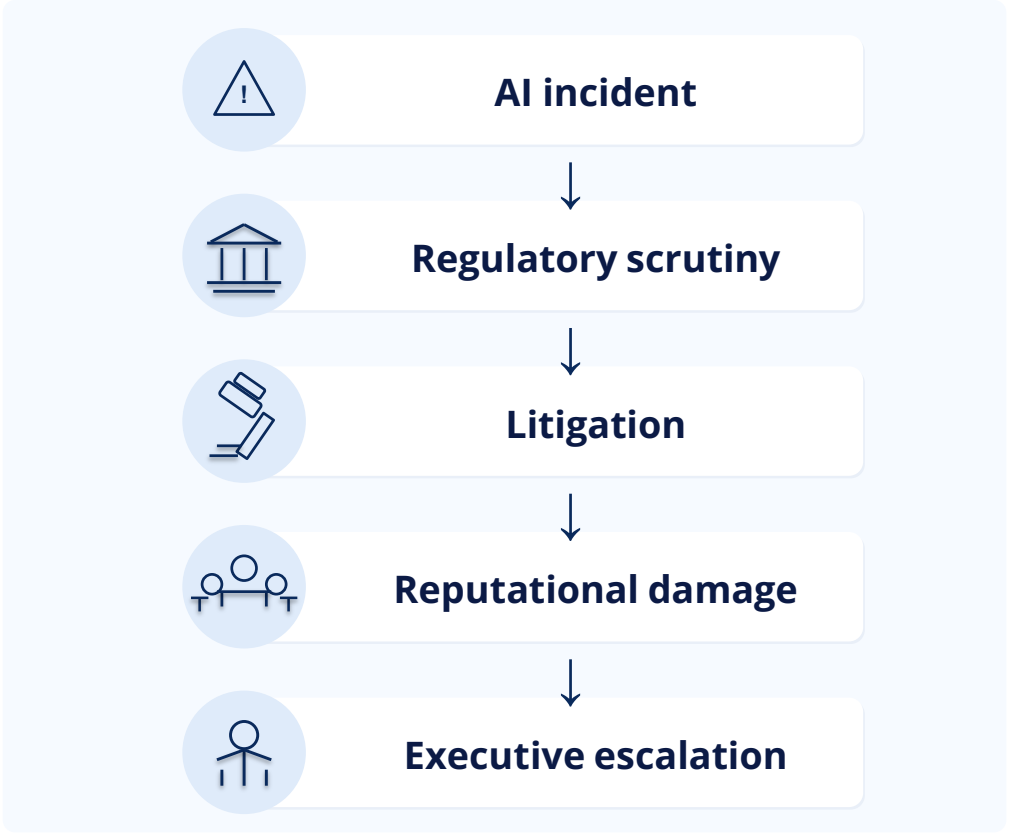
Source: ArmorCode "The Claude Mythos Security Playbook." Deloitte "The State of AI in the Enterprise", AI Incident Database

AI changes the incident equation



Source: Resilient Cyber “The Zero Day Clock Is Ticking: Why the Collapse of Exploitation Timelines Changes Everything”

The First AI Incident Your Org Cannot Explain



Most organizations have:

- AI policies
- governance committees
- fragmented workflows
- disconnected tools

Few organizations have:

- ✓ an AI incident response plan
- ✓ operational decision rights
- ✓ defensible workflows
- ✓ a system of record
- ✓ explainable governance processes

Operational readiness matters before the incident — not during it.

Governance requires **shared language** and **systems**

Are AI incidents defined?

A shared language is emerging for AI incidents

The OECD framework separates potential dangers from actual harms.

AI hazard

A potential danger or condition that could lead to harm if it materializes.

AI incident

An event, circumstance, or series of events where the development, use, or malfunction of one or more AI systems directly or indirectly leads to harm.

Source: OECD, Defining AI incidents and related terms, 2024; OECD AI Incidents Monitor.

A shared language is emerging for AI incidents

MIT AI Risk Initiative

Legislation *vs.* Litigation

Global & U.S. AI Regulation Landscape

Category	Key Developments
International	• EU AI Act (2024) - risk-based AI regulation with phased rollout, pending omnibus changes (2025-2028) • South Korea AI Basic Act - effective Jan 2026, national AI governance law • United Kingdom - principles-based oversight through existing regulators • China - national frameworks and specific technology ordinances
United States - Federal	• No comprehensive federal AI statute • Policy driven by Executive Orders, America's AI Action Plan, agency guidance, and voluntary standards.
United States - State Laws *(not a comprehensive list)*	• New York AI Act (S1169A - proposed) - audits, risk management programs, and human review • Texas (HB 149) - effective Jan 2026, prohibited harms, disclosures, and AG enforcement. • California (SB 53) - effective Jan 2026, frontier-model transparency, safety-framework, and incident-reporting duties
United State - Trend	Nationwide patchwork of AI legislation.

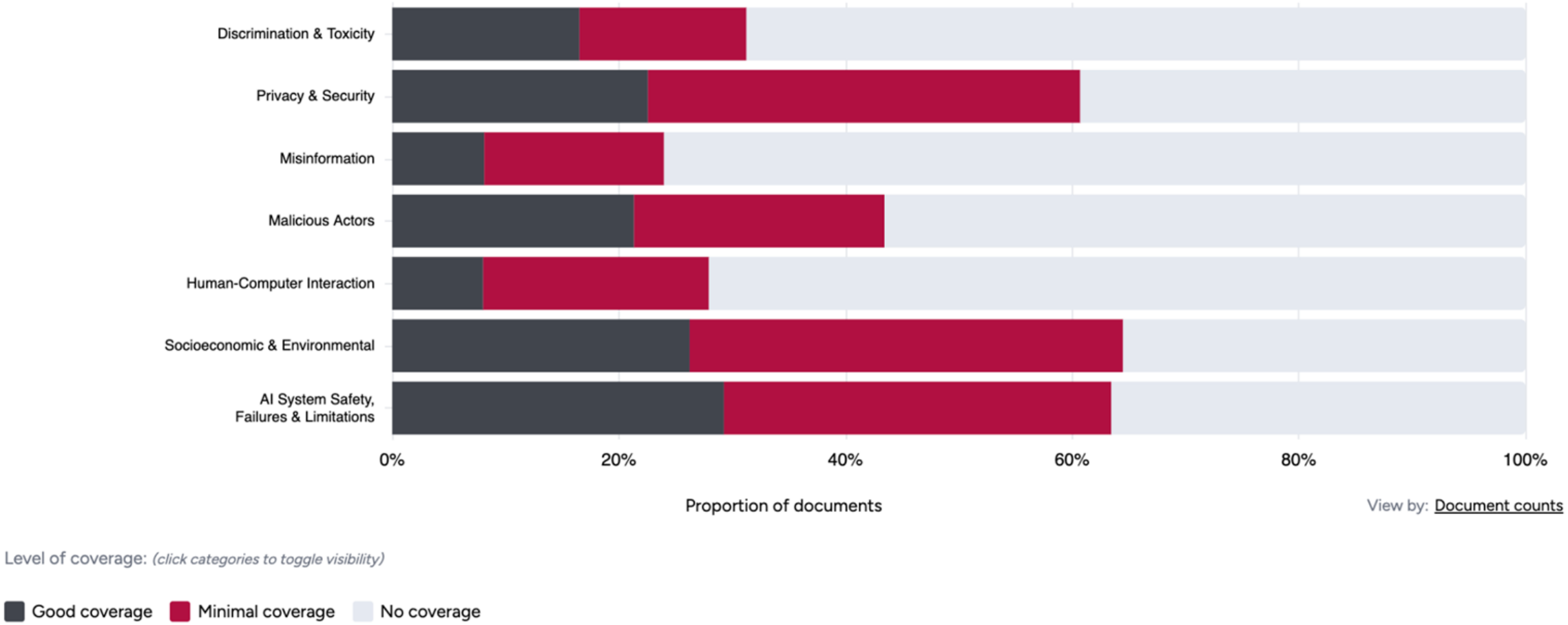
Implication: Organizations are adopting structured AI governance programs (e.g. ISO 42001) to prepare for emerging regulation.

The AI risk universe is broad

MIT maps ***1,700+ risks*** across 74 frameworks into a shared taxonomy.

Source: MIT AI Risk Repository, airisk.mit.edu; 1,700+ risks from 74 frameworks, organized into 7 domains and 24 subdomains.

What AI Risks are being governed today?



Source: MIT AI Governance Map and Mapping the AI Governance Landscape, April 2026.

The AI Incident Response Plan

You build it before the incident, or you improvise during the incident.

Traditional incident response leaves AI-specific gaps

Traditional IR is optimized for:

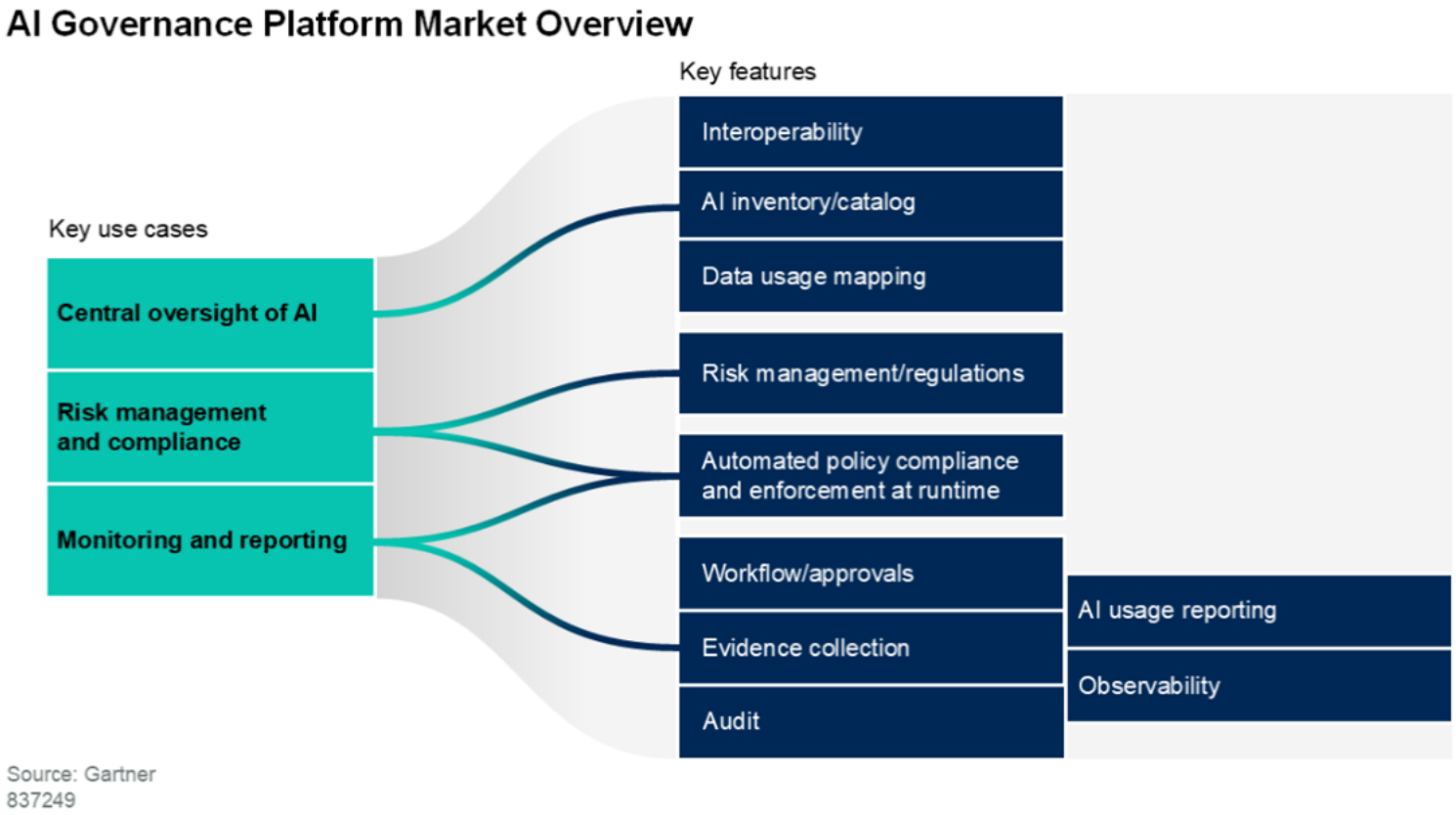
- Data breaches
- Malware & outages
- Unauthorized access
- Forensics & logs

AI IR must also handle:

- Drift, hallucinations & bias
- Training & data lineage
- Third-party AI dependency risk
- Explainability & auditability

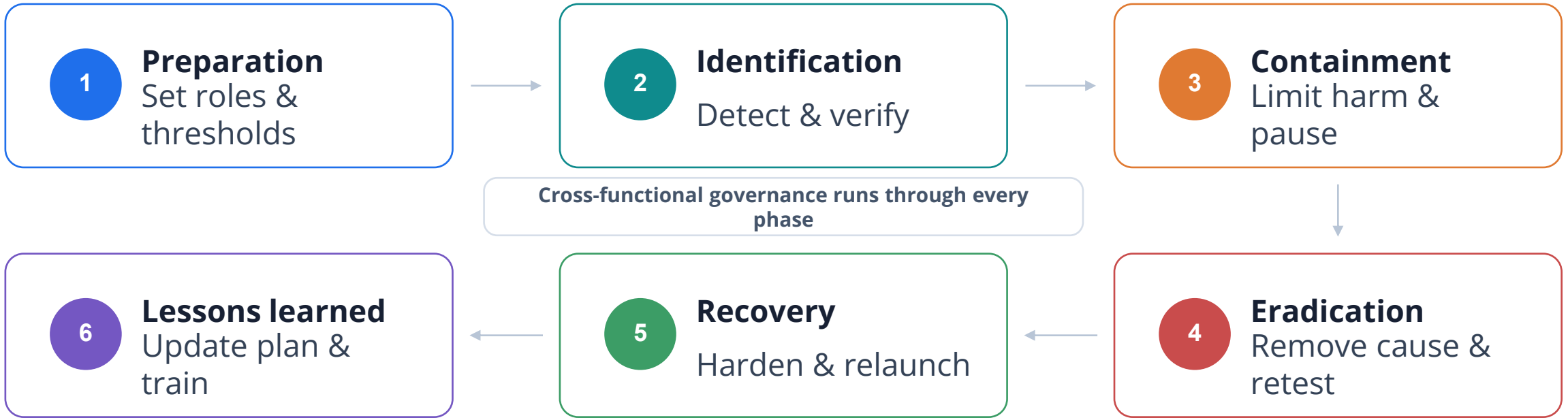
Source: RadarFirst AI-Driven Risk whitepaper; EU AI Act serious incident obligations.

Governance platforms are becoming the control plane



Source: Gartner Market Guide for AI Governance Platforms

IAPP - AI Incident Response Plan



AI-specific triggers Security • unauthorized outcomes • bias • privacy • safety • transparency • model decay • data poisoning • adversarial attacks

Source: IAPP AI Incident Response Plans

CSET - AI Incident Response Plan

WHAT TO CAPTURE

Classify	Characterize	Evidence	Context	Close out
incident vs. near miss	harm + severity	technical record	people + setting	response + ethics

1 Type of Event

Did harm occur?

Classify

- Incident
- Near miss

2 Harm Profile

What types of harm?

Characterize

- Harm type
- Mechanism
- Severity factors

3 Technical Information

Which AI system?

Preserve

- AI system card
- AI model card
- Datasheet

4 Context + People

Who, where, when?

Ground

- Purpose + sector
- Dates + location
- Actors + affected

5 Response + Ethics

What changed?

Close out

- Mitigation / termination
- Ethical impact

TAGS THAT MAKE THE REPORT ANALYZABLE

Harm categories	Physical	Environmental	Economic/financial	Reputational	Public interest	Human rights	Psychological
Severity lens	Remediability	Level	Distribution	Population	Duration	Optionality	Frequency

Source: Center for Security and Emerging Technology, "AI Incidents: Key Components for a Mandatory Reporting Regime," Table 1.

How it works in practice

1

Intake

Eliminate blind spots with structured incident intake.

2

Assessment

Evaluate applicability, risk, and obligations in minutes.

3

Guidance

Apply regulatory logic and decisioning models to reach consistent outcomes.

4

Documentation

Maintain complete, audit-ready records without manual effort.

Every action captured in a single, audit-ready system of record.

Agentic Layer

Enhances intake, triage, and investigation workflows to improve speed, accuracy, and efficiency across the lifecycle.

Thank you for joining us!

www.radarfirst.com | @radarfirst

www.linkedin.com/company/radarfirst

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP AIGG Europe 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!