Cyberweek[25]

Perspectives Cybersécurité 2025-2030

Jeremy D'Hoinne

Gartner®

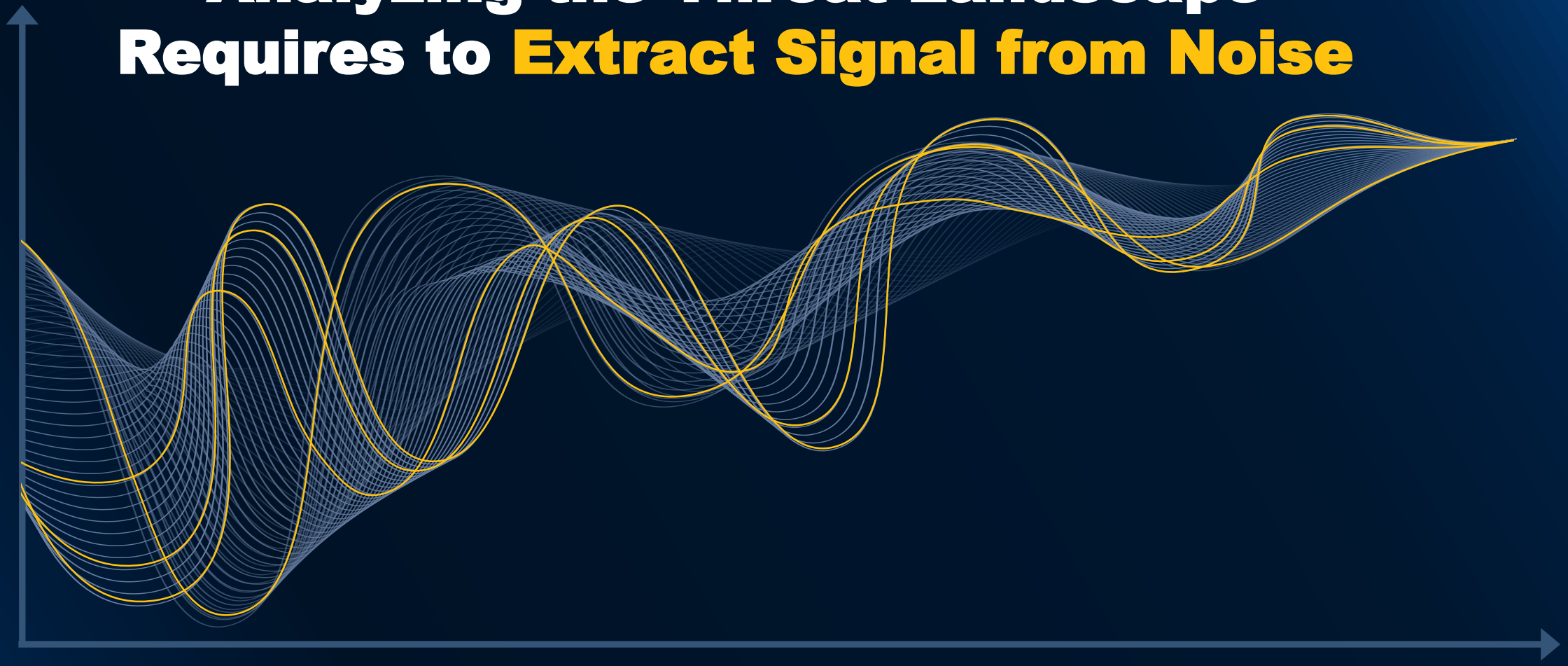
“

Mal nommer les choses, c’est ajouter au malheur du monde.

Albert Camus

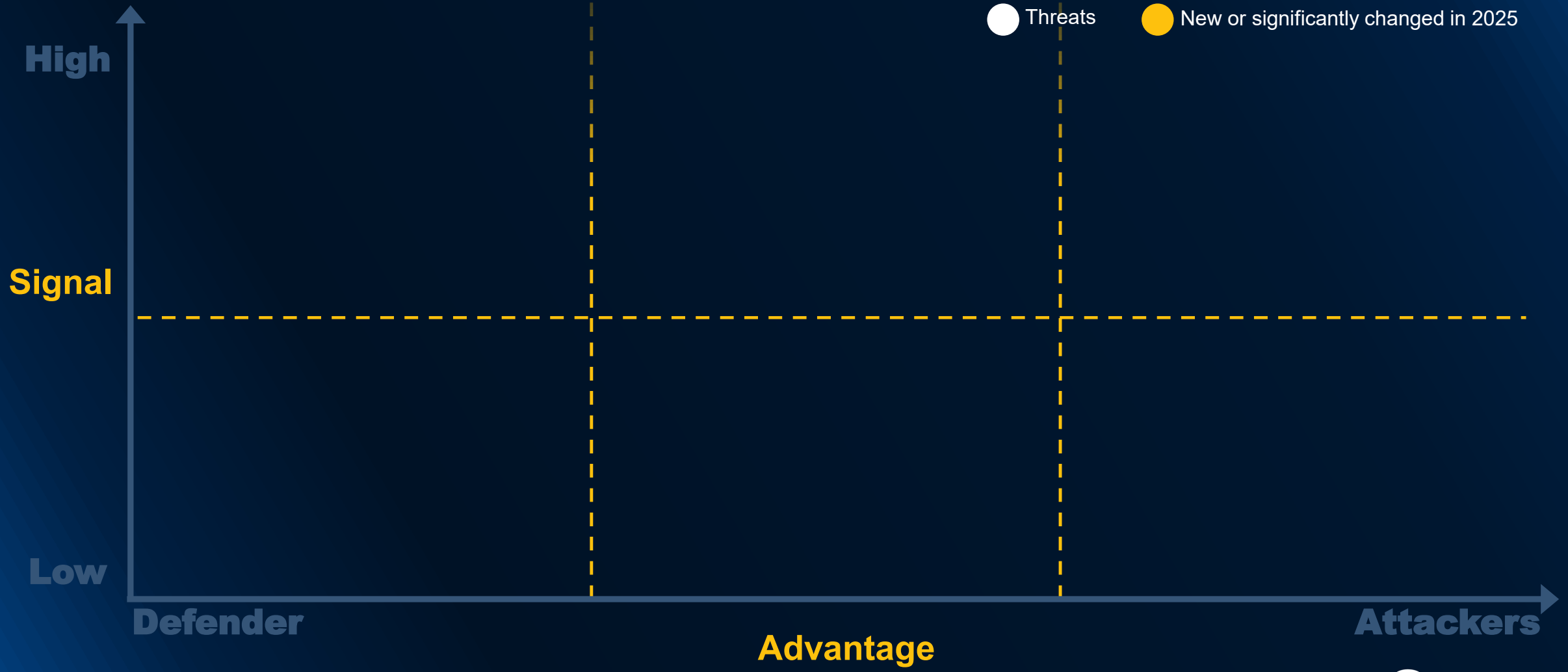
Source: Wikimedia commons

Analyzing the Threat Landscape Requires to Extract Signal from Noise



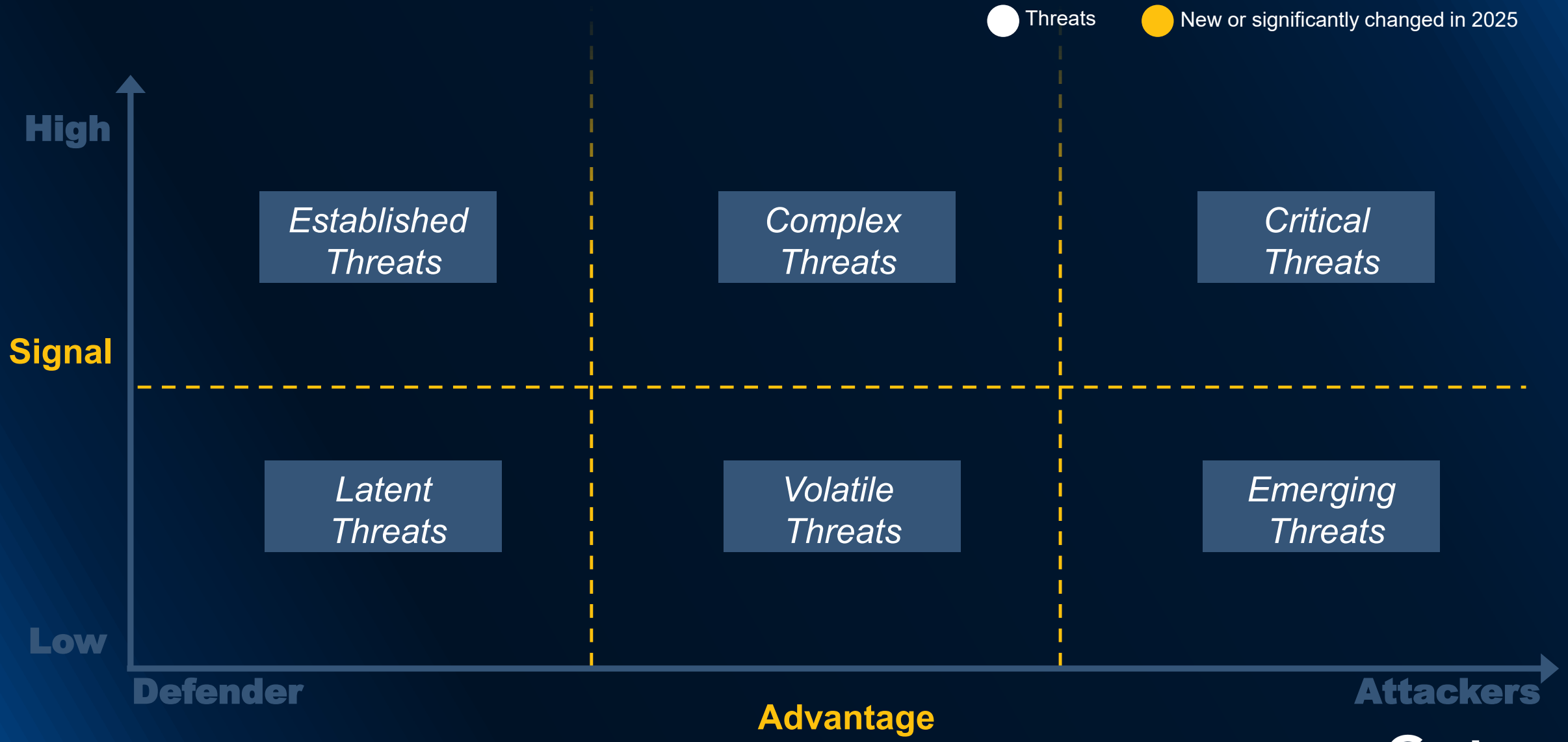
Gartner®

Visualizing Threats to Support Cybersecurity Decisions



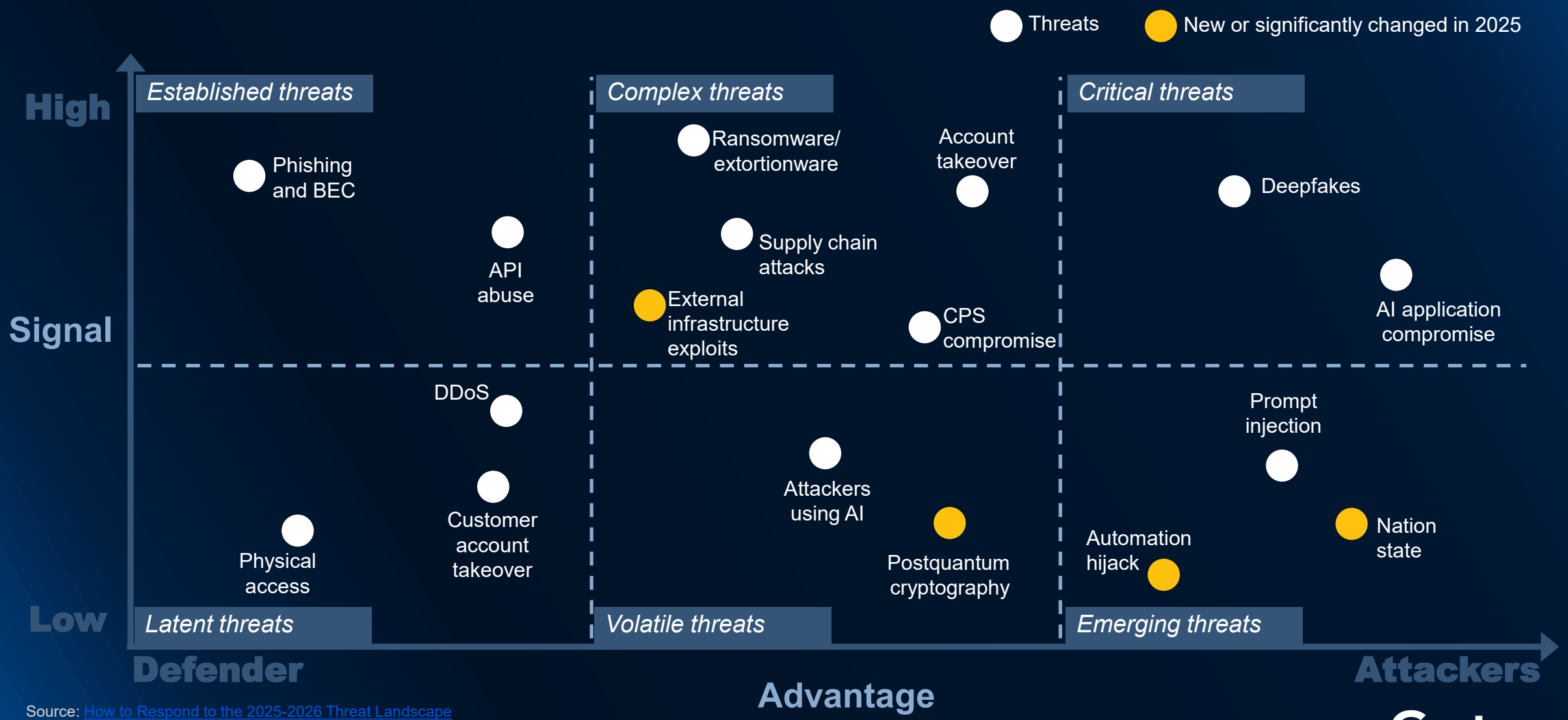
Gartner®

The ThreatScape Categories



Gartner

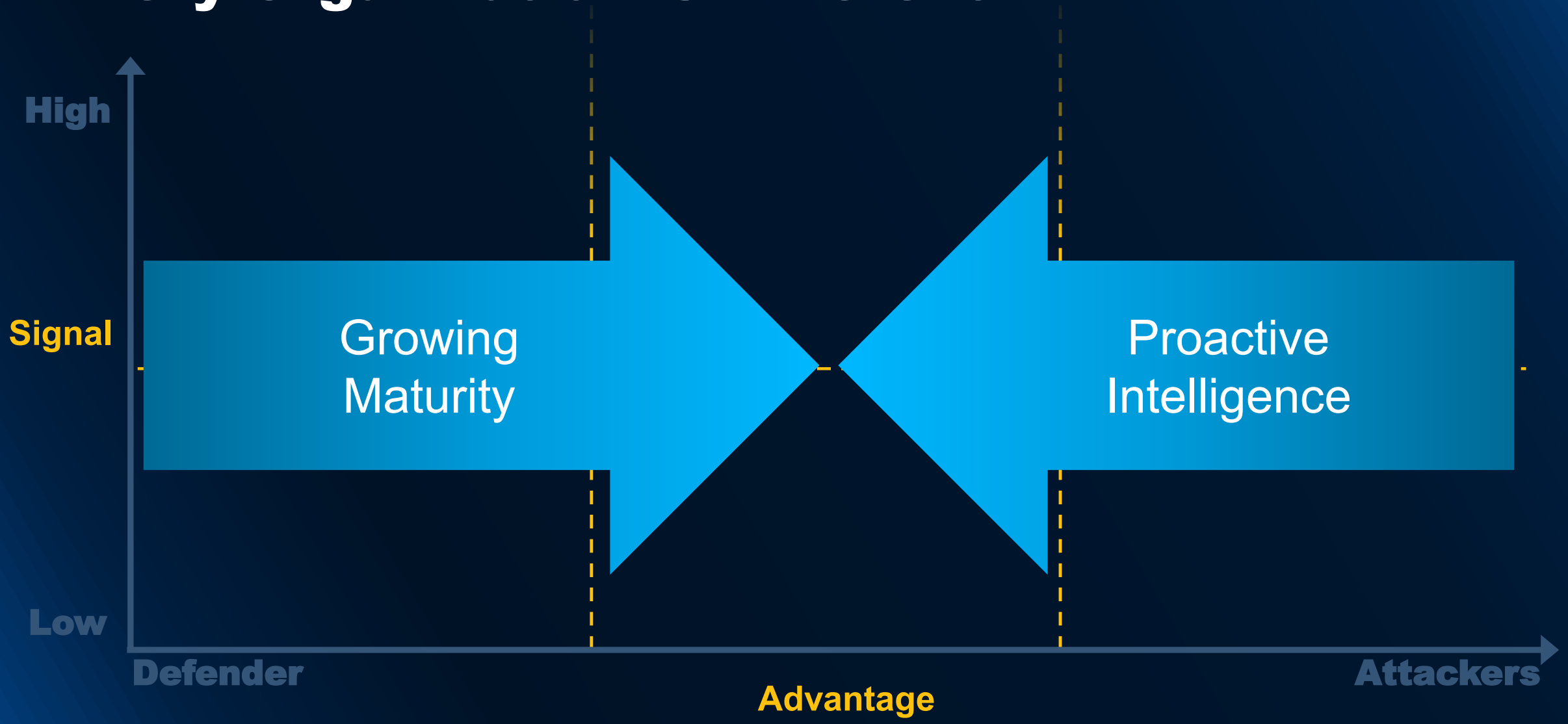
Gartner 2025 ThreatScape



Source: How to Respond to the 2025-2026 Threat Landscape

Gartner

Every Organization is Different



Gartner

Emerging & Critical Threats

Emerging & Critical Threats

1. Automation Hijack
2. Nation-State Sponsored
3. Adversarial Prompting
4. AI Application Compromise
5. Deepfakes

Gartner®

1 Automation Hijack

“Agent = Software”

Everything is an agent
Every workflow is now agentic

Gartner®

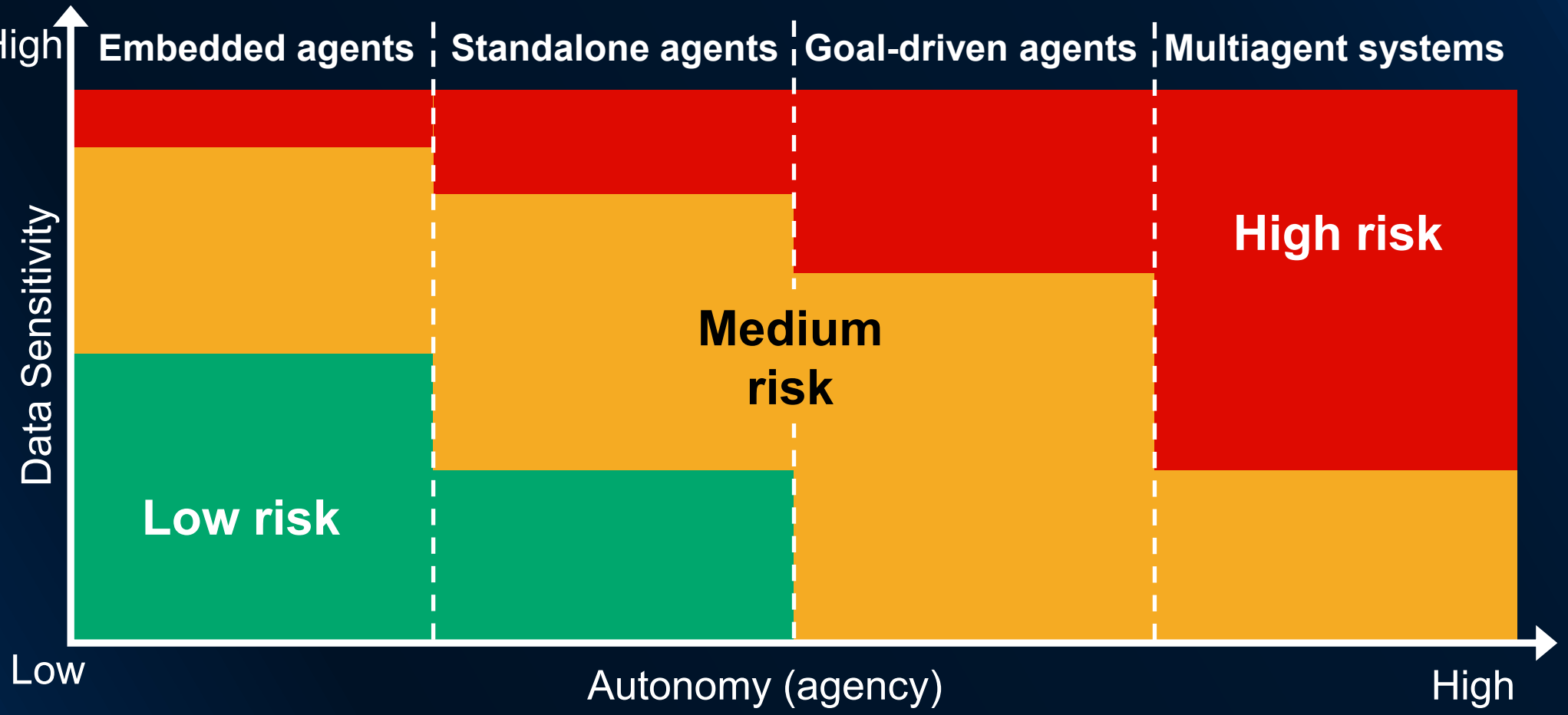
1 Automation Hijack

Agent Risk Categorization

Gartner

1 Automation Hijack

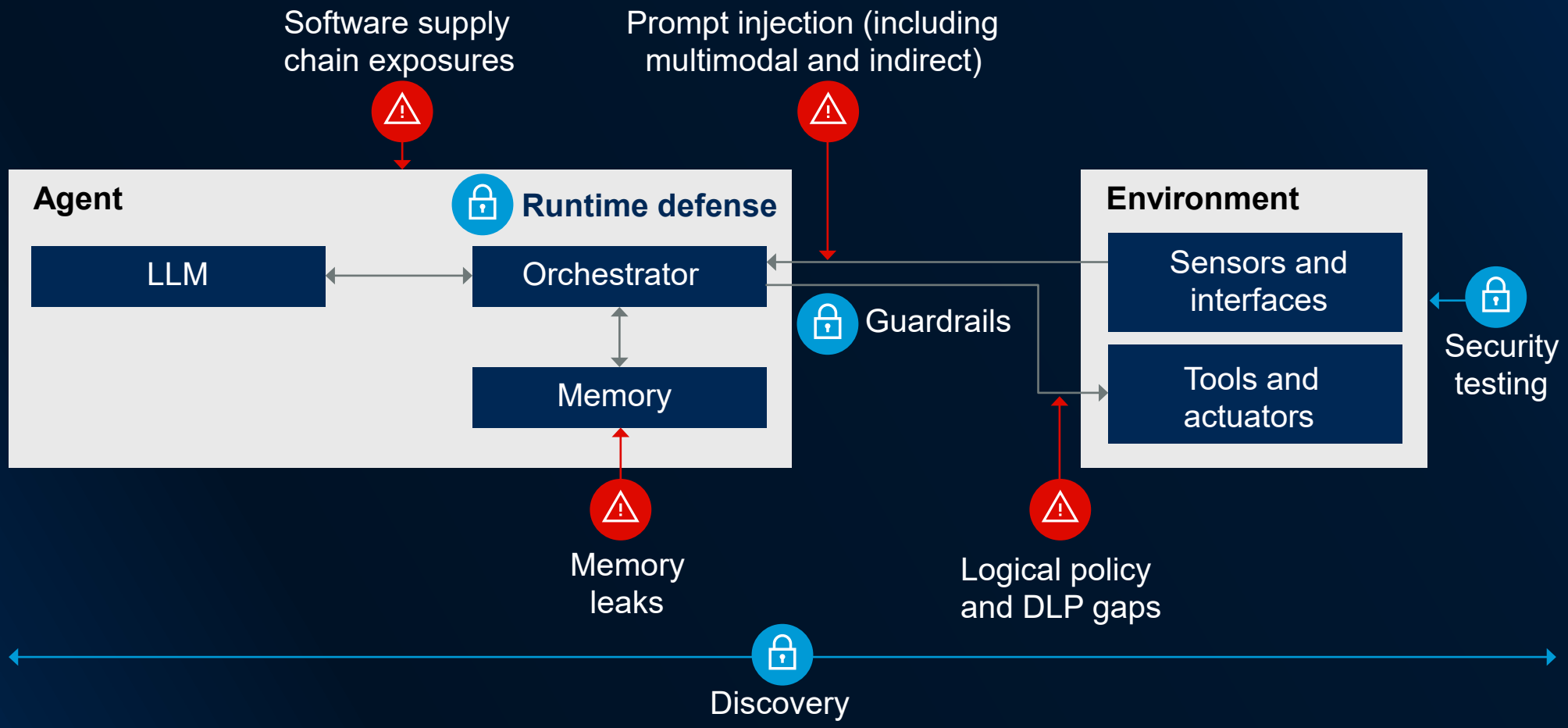
Agent Risk Categorization



Gartner®

1 Automation Hijack

Custom-built AI Agents Threats, Attacks and Security Measures



Source: Gartner
824390_C

Gartner

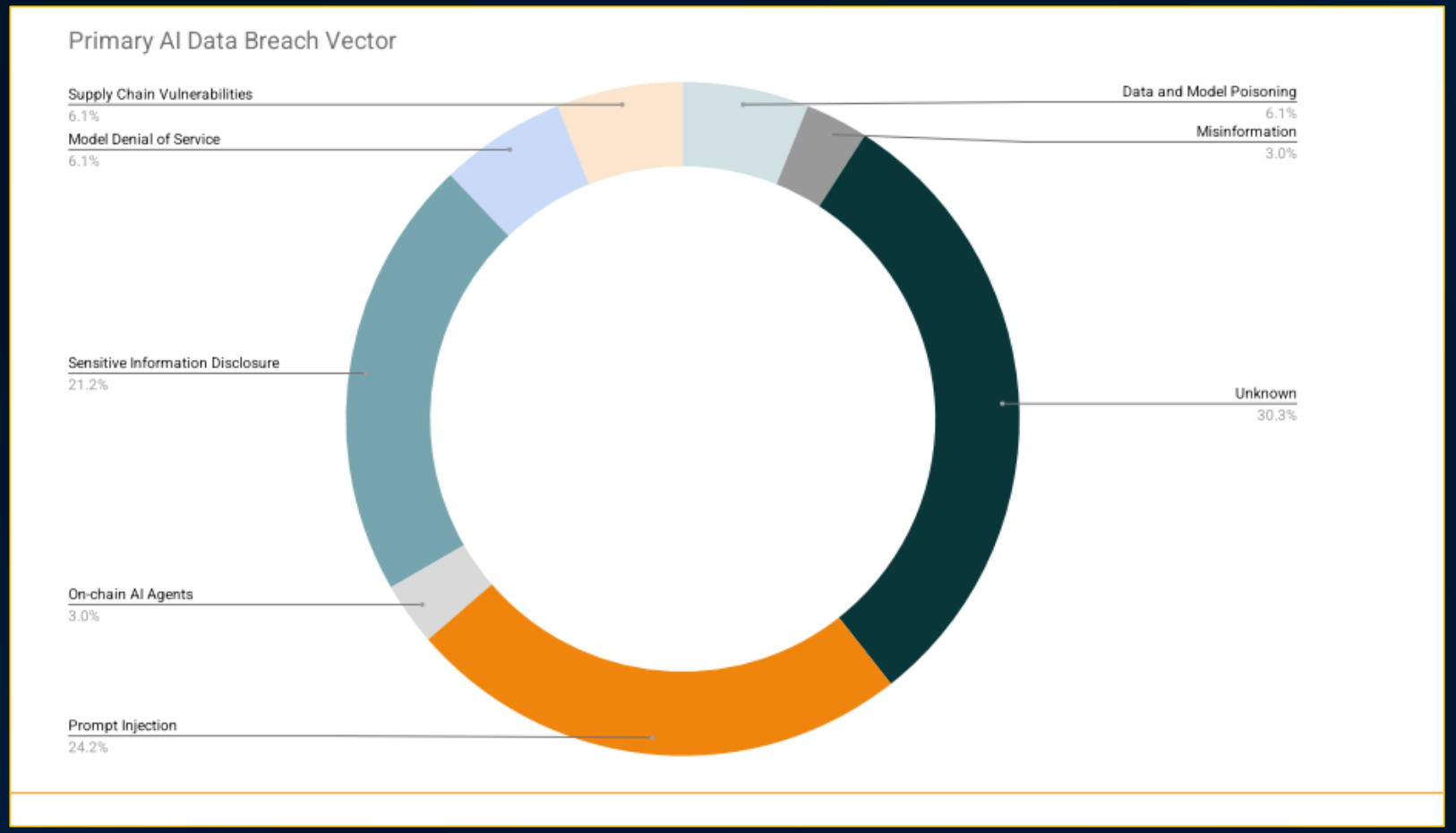
2 Nation-State Sponsored

Threat assessment questions	Considerations
What do we have that is of interest to a nation state attacker?	Contracts with defense entities, intellectual property of interest to a nation state, access to large amounts of compute and storage
Why would a nation state target our organization?	Innovation prowess, critical infrastructure, client base, lucrative data
Where do we do business and where are the assets of interest to a nation state?	Competition against state owned entities (for example, mining or manufacturing), political connections, affiliation with hostile countries
How would a nation state gain access to our environment?	Gaps in security monitoring, unsecured infrastructure, business association connections, novel attack methods
Who are the nation states known to target our industry?	Sophistication of attacks, financing of attacking nations, proxy organizations

Gartner®

3 Adversarial Prompt

Direct and Indirect Prompt Injections

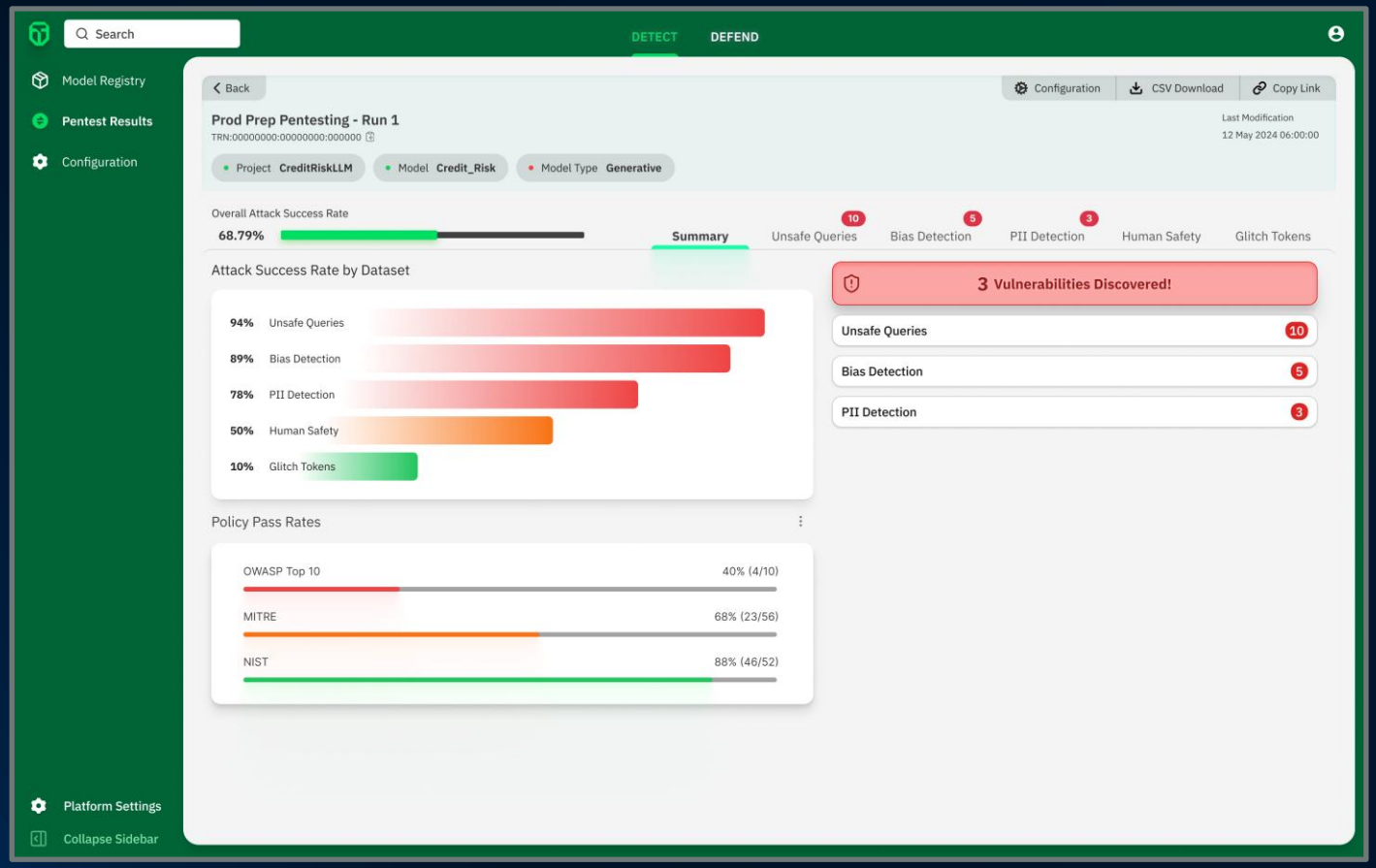


Source: Firetail State of AI and API Security, 2025 , April 2025

Gartner

3 Offensive Security Testing

Include AI Applications in your Red Teaming Efforts



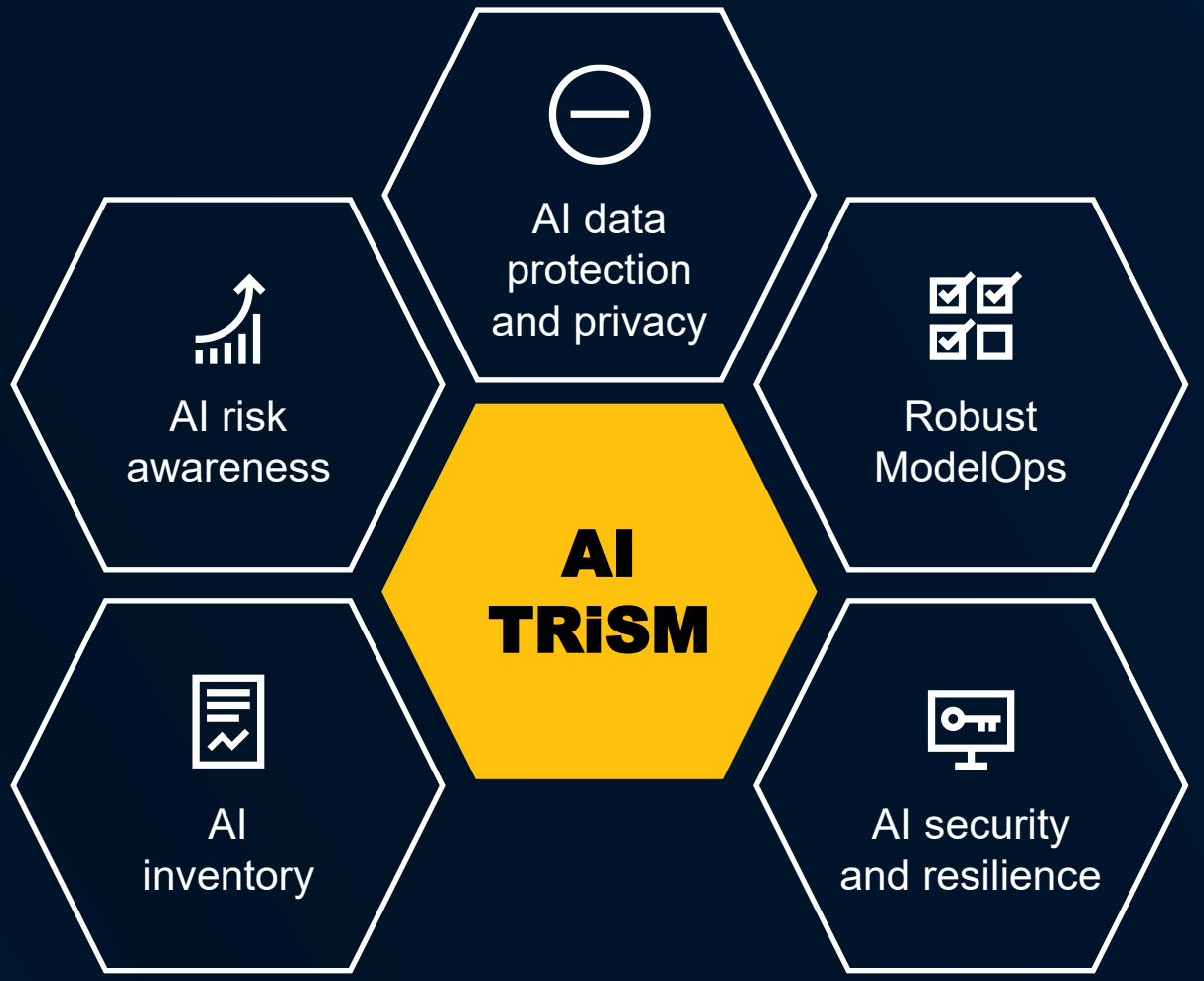
Source: TrojAI Detect

Key elements

- Scope
  - Models (LLMs, multimodal)
  - Application
- Test categories
- Scheduling & retest
- Alerting & reporting

Gartner

4 AI Application Compromise
Prioritize Securing AI Applications

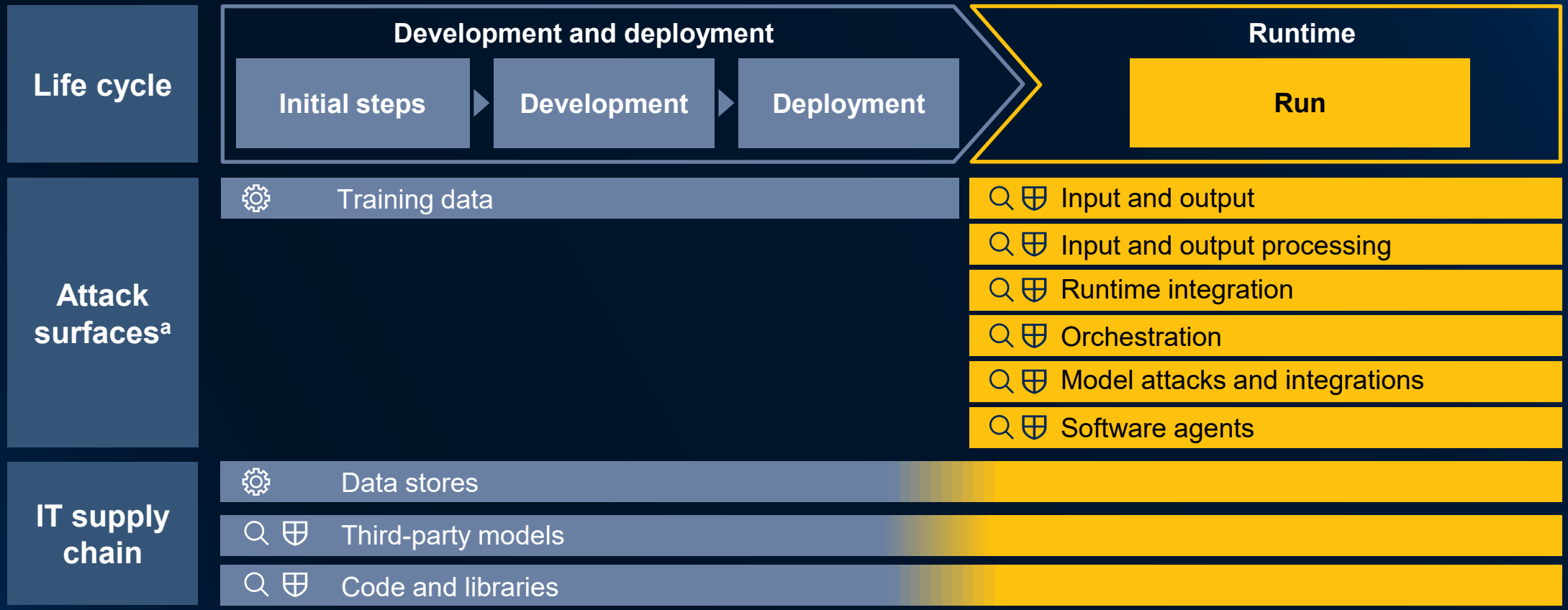


Gartner

4 AI Application Compromise

Attack Surfaces Across the AI Life Cycle

AI TRiSM technology: Content anomaly detection | Data protection | Application security

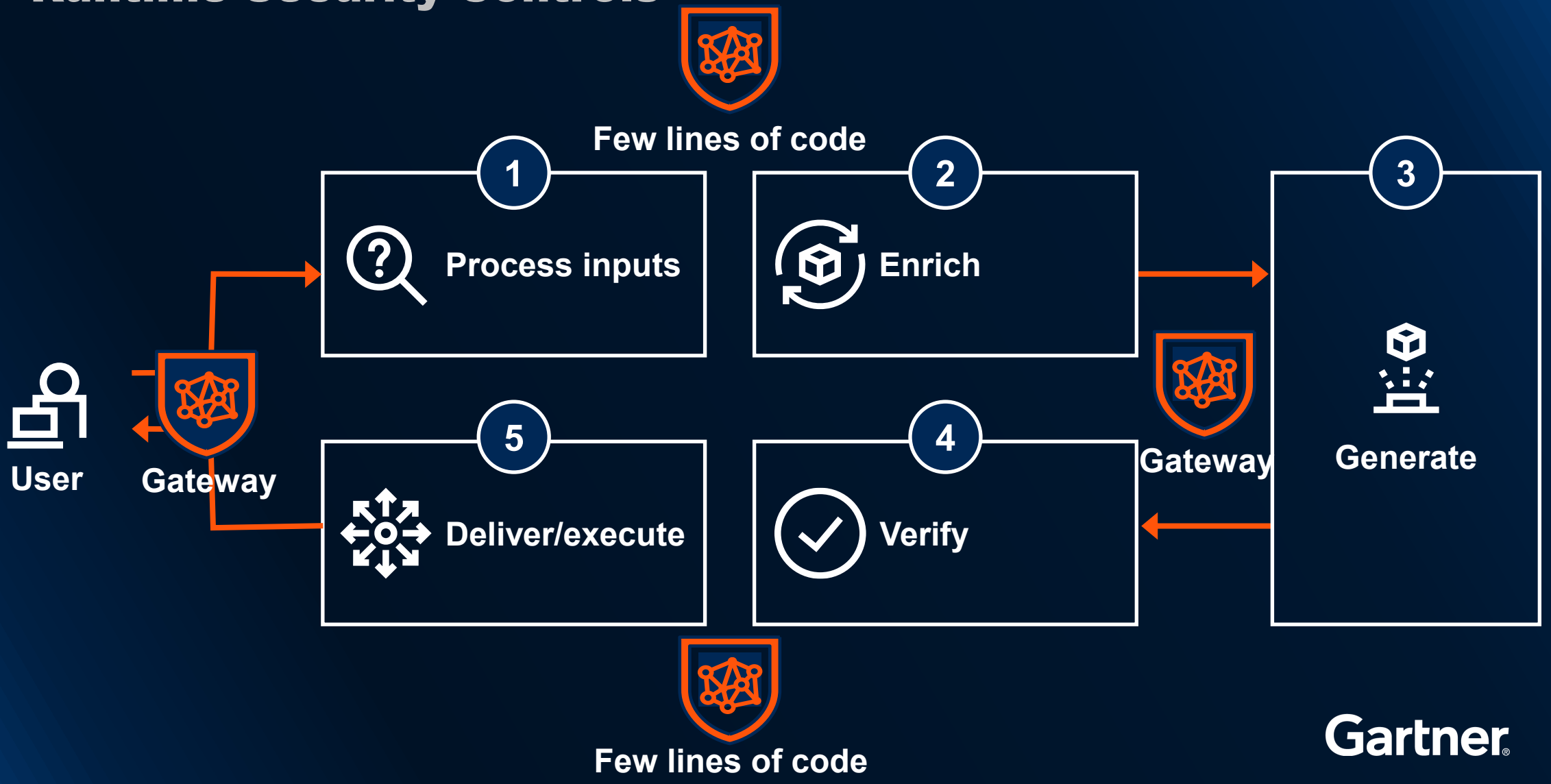


[a] Main sample attack surfaces only; others not shown

Gartner

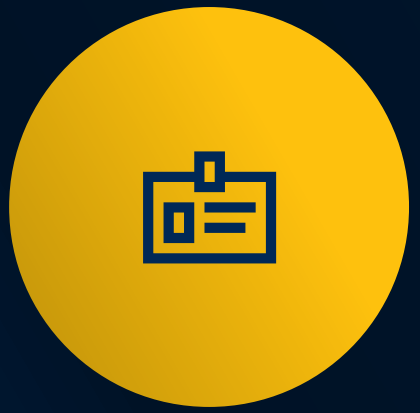
4 AI Application Compromise

Runtime Security Controls



Gartner

5 Identity Impersonation and Deepfakes



Identity verification face biometrics

Voice biometrics

Enterprise internal authority impersonation

Gartner®

5 Identity Impersonation and Deepfakes

62%

We experienced **at least one** minor incident involving audio or video deepfake.

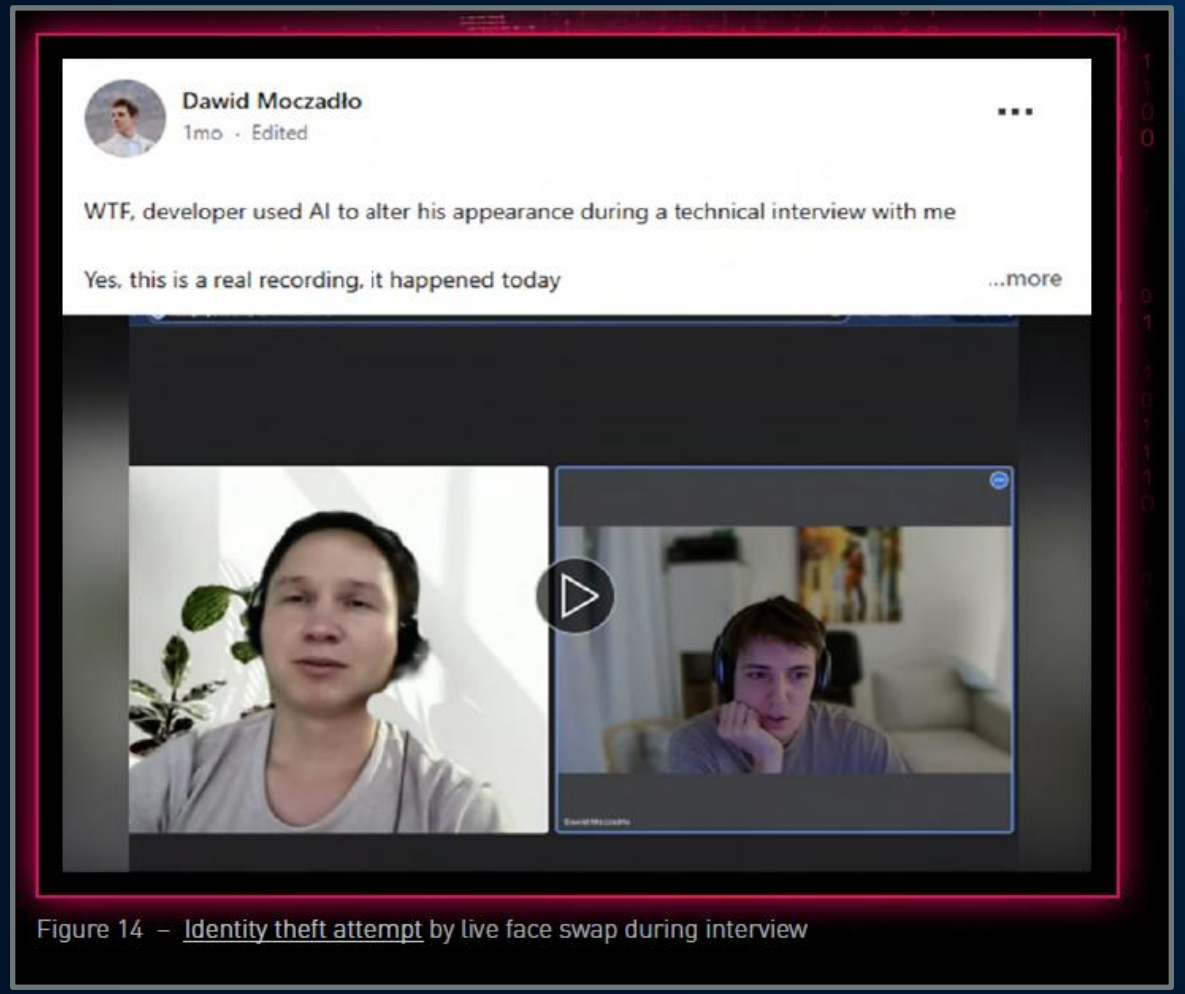


Figure 14 – Identity theft attempt by live face swap during interview

Source: Cyber Security Resource Center, Check Point Software Technologies

n = 293-296, excluding unsure

Q: In the last 12 months, has your organization observed any of the following GenAI-augmented cyberattacks or attacks on GenAI assets?

Source: 2025 Gartner Cybersecurity Innovations in AI Risk Management and Use Survey

Gartner®

5

By 2028, one in four candidate profiles worldwide will be fake.

Mitigate Rising Candidate Fraud Through Identity Verification

Gartner®

5 Deepfake Scenario Planning

Impersonation in business process	Fake voice or fake video used to hijack some less visible but important process: • Requesting a SIM card because you “lost your phone” • Asking HR to update banking details
Supply Chain Deepfake	Impersonating an employee in a conversation with a contractor/partner. IT employee, asking a managed service provider to “open a port”. Procurement employee, asking to change an order…
Deepfake as-a-Service	Criminal organizations like to deliver “attack kits”. How much targeted deepfakes can we get if an attacker can upload a voice/video sample, and a script text, and get back a credible deepfake.
Remote hire	How much of the hiring process for remote employee could be impacted by credible deepfake? What would need to change to ensure that background checks are sufficient? (see also FBI warning on the topic)

Gartner

Build resilience, detection and response to emerging and critical threats

Gartner®

Complex & Volatile Threats

Complex & Volatile Threats

1. PostQuantum Cryptography
2. Attackers Using AI
3. CPS Compromise
4. External Infrastructure Exploit
5. Supply Chain Attacks
6. Account Takeover
7. Randomware/Extortionware

Gartner®

1 Postquantum Cryptography

Gartner

1 Postquantum Cryptography Secure Plan of Action

2025

- Inventory usage
- PQC policy
- Data use timeframe (short, medium, long)
- Plan transition

2026 to 2029

- Purge weak crypto
- Implement transitional policies
- Implement crypto agile applications

Gartner®

1 Postquantum Cryptography Secure Plan of Action

Regulations

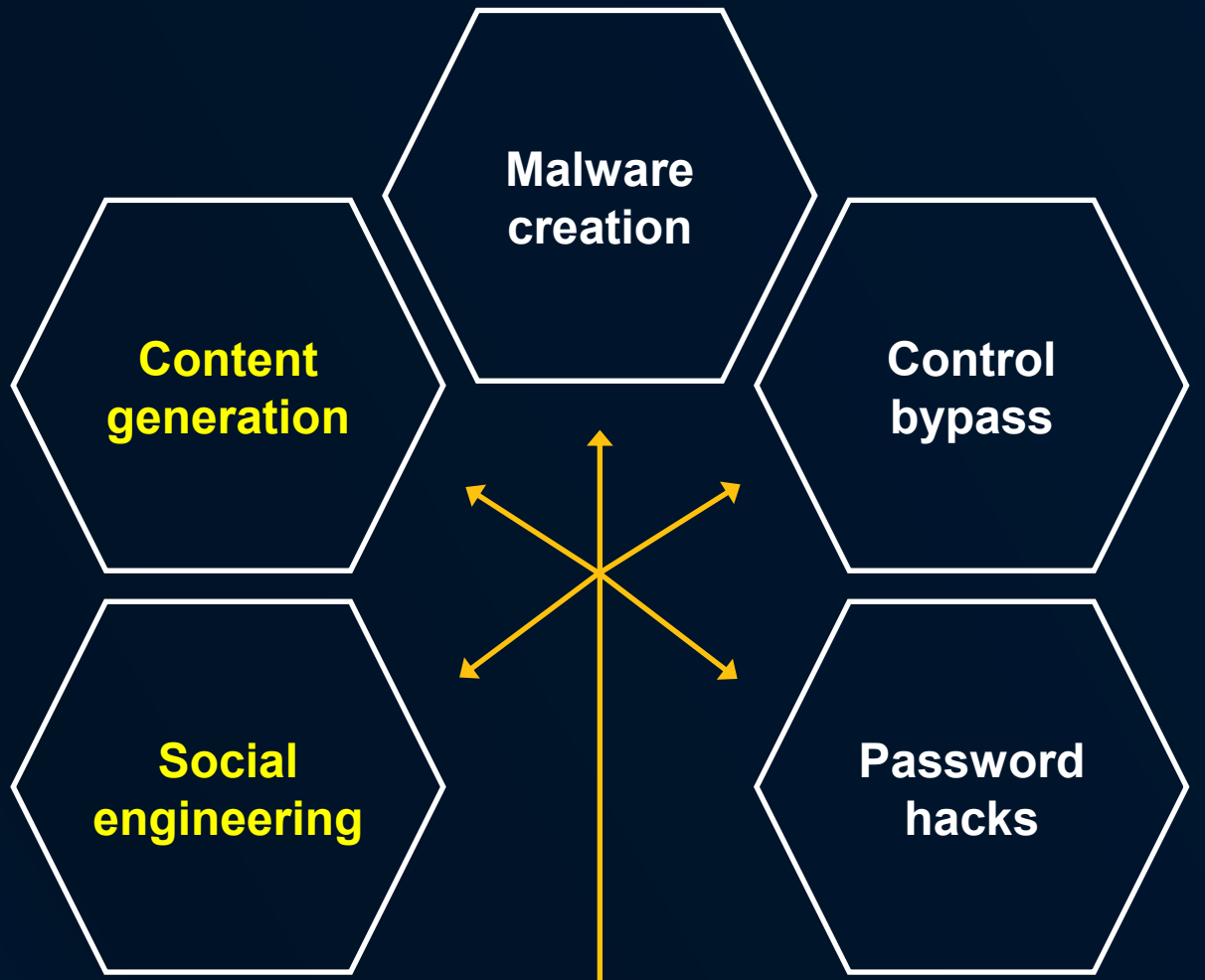
2030

- End-of-life nonagile crypto applications
- Enforce strong crypto policies
- Test new postquantum algorithms

Weak algorithms
such as Diffie-Hellman, Elliptic Curve Diffie-Hellman, Rivest-Shamir-Adleman (RSA), etc.
no longer approved

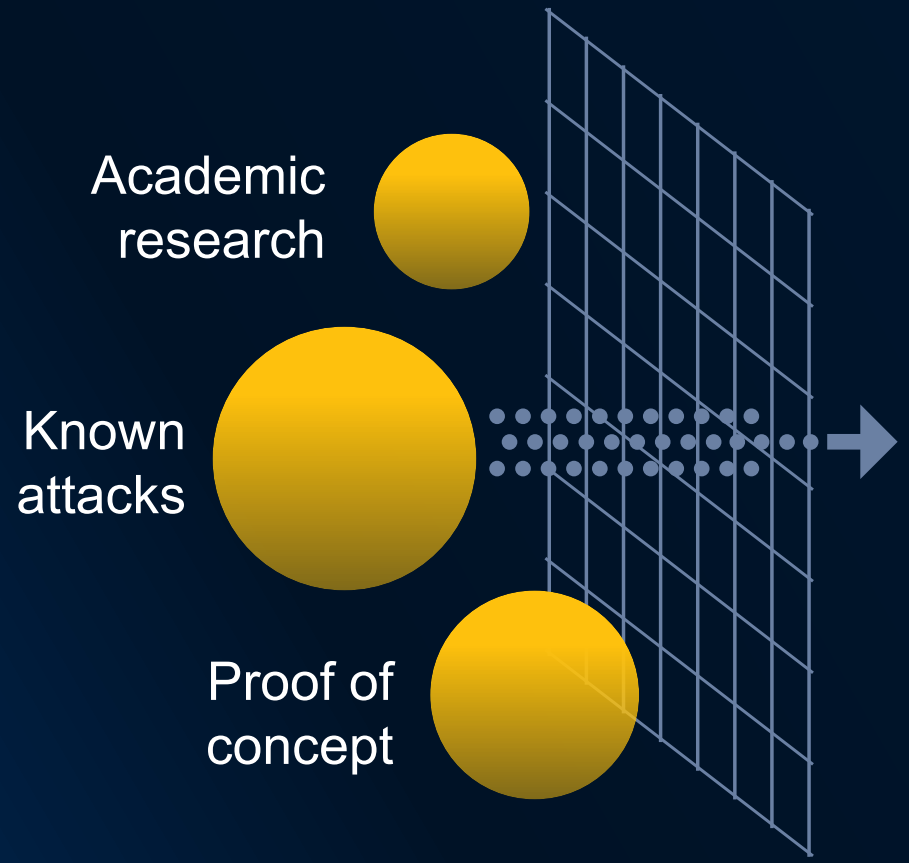
Gartner

2 Attacks Using AI



Gartner

2 Attacks Using AI
Pragmatic Approach to Uncertain AI Attacks



"AI attack" threat intelligence + Threat exposure + Scenario planning

Security team

Tune or upgrade controls

Adapt business workflows

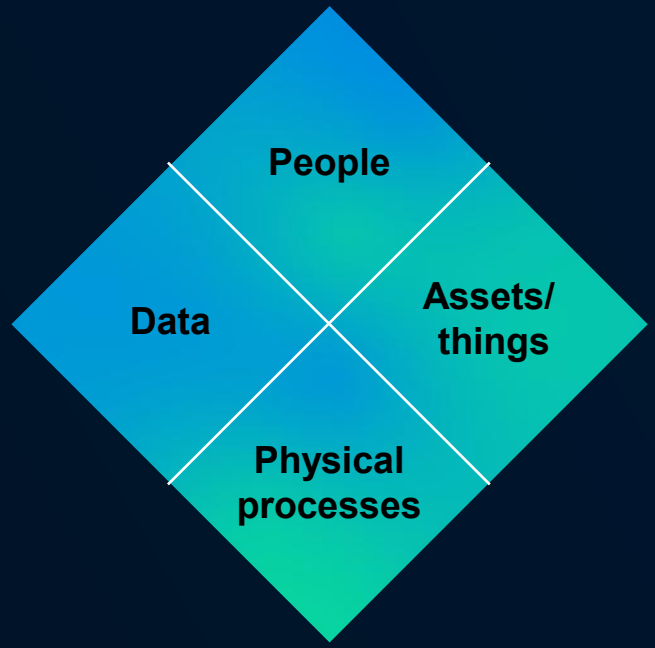
Improve resilience

Gartner®

3 CPS Compromise

Cyber

- Ransomware prompting proactive shutdowns
- Internet-connected assets with default passwords
- Remote operations
- DDoS and lateral movement



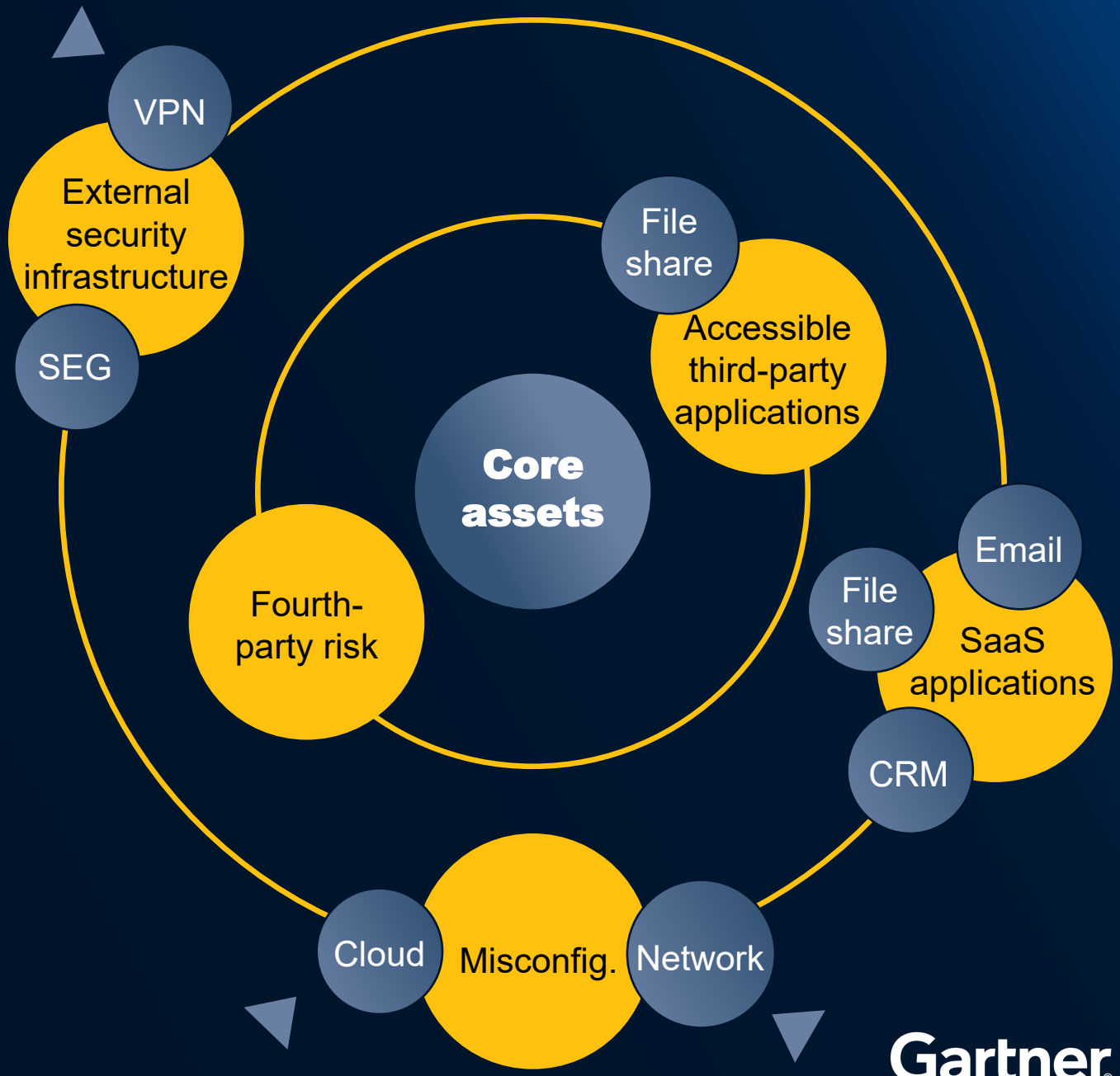
Physical

- Drones eavesdropping, payload delivery
- Sneakernet
- Temperature, humidity, light, time tampering
- GPS jamming/ tampering

Source: Gartner 827923_C

Gartner®

4 External Infrastructure Exploits



Gartner

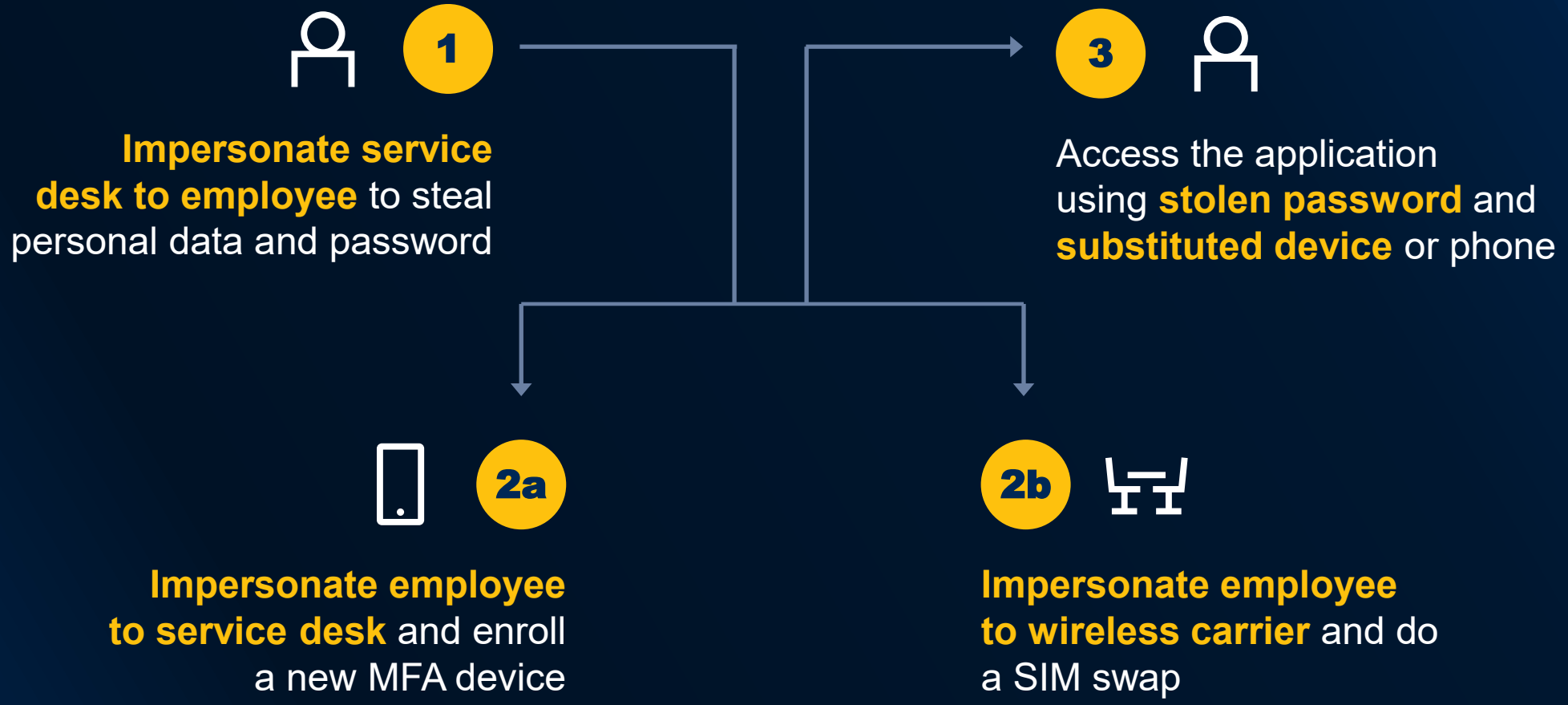
5 Supply Chain Attacks

Source: Open Source Security Foundation

762170_C

Gartner

6 Account Takeover (human & machine)



Gartner

7 Ransomware — Extortionware

Initial access and ransomware delivery

- Ransomware as a service
- Initial access brokers
- Account takeover
- Misconfigurations

Impact and urgency drivers

Data exfiltration

Data encryption

Data corruption

Frequent Government Recommendation: Never pay a ransom

Ransomware payment risks and implications

- Double extortion
- Increased ransoms
- Sanctions violations

Gartner

57%

of Gartner clients report they **do not have advanced network segmentation** — a key control to limit the impact of ransomware.

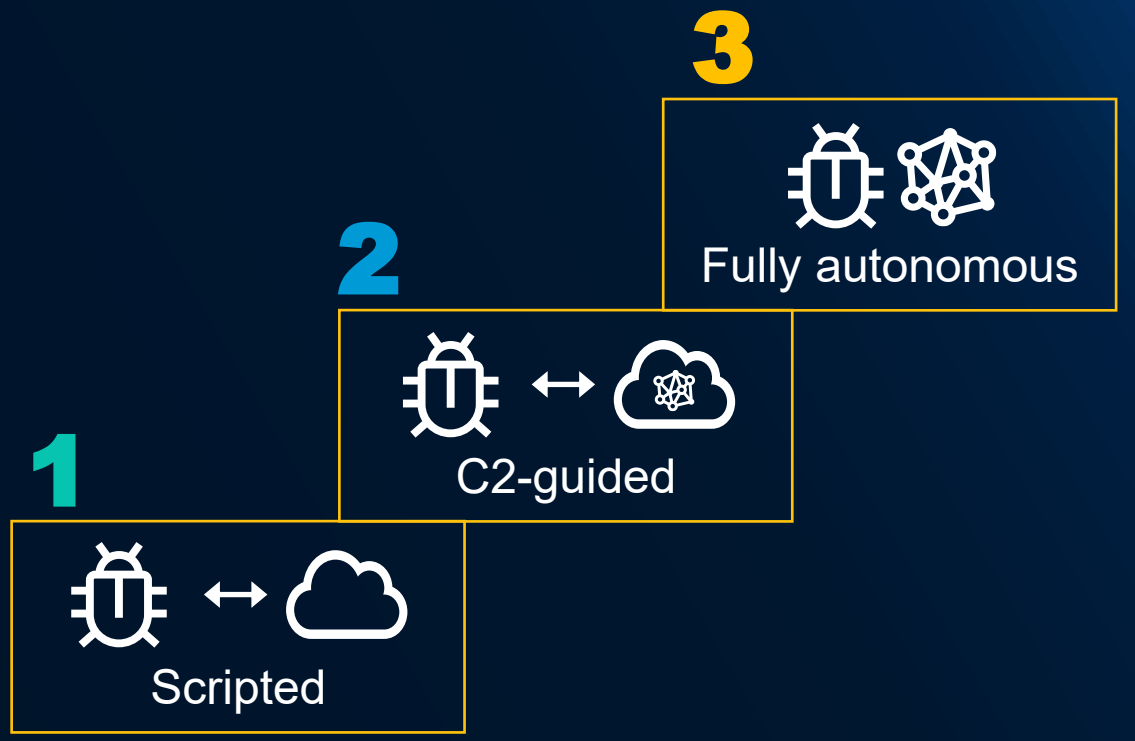
n = 468, all respondents

Source: 2024 Gartner Cybersecurity Control Assessment

Gartner®

7 The Threat of Autonomous Malicious Agent

Workflow



Architecture

Gartner

Established & Latent Threats

1 **API Abuse**

2 **Social Engineering, phishing & BEC**

3 ***Latent Threats***

Established & Latent Threats

Gartner®

Successful API attacks lead to at least

10x

more **breached records** than an average cybersecurity breach.

Source: Various industry estimates

Gartner®

2 Social Engineering, Phishing and BEC

Email

More credible scams

Profiling

LLM content

Gartner

2 Social Engineering, Phishing and BEC

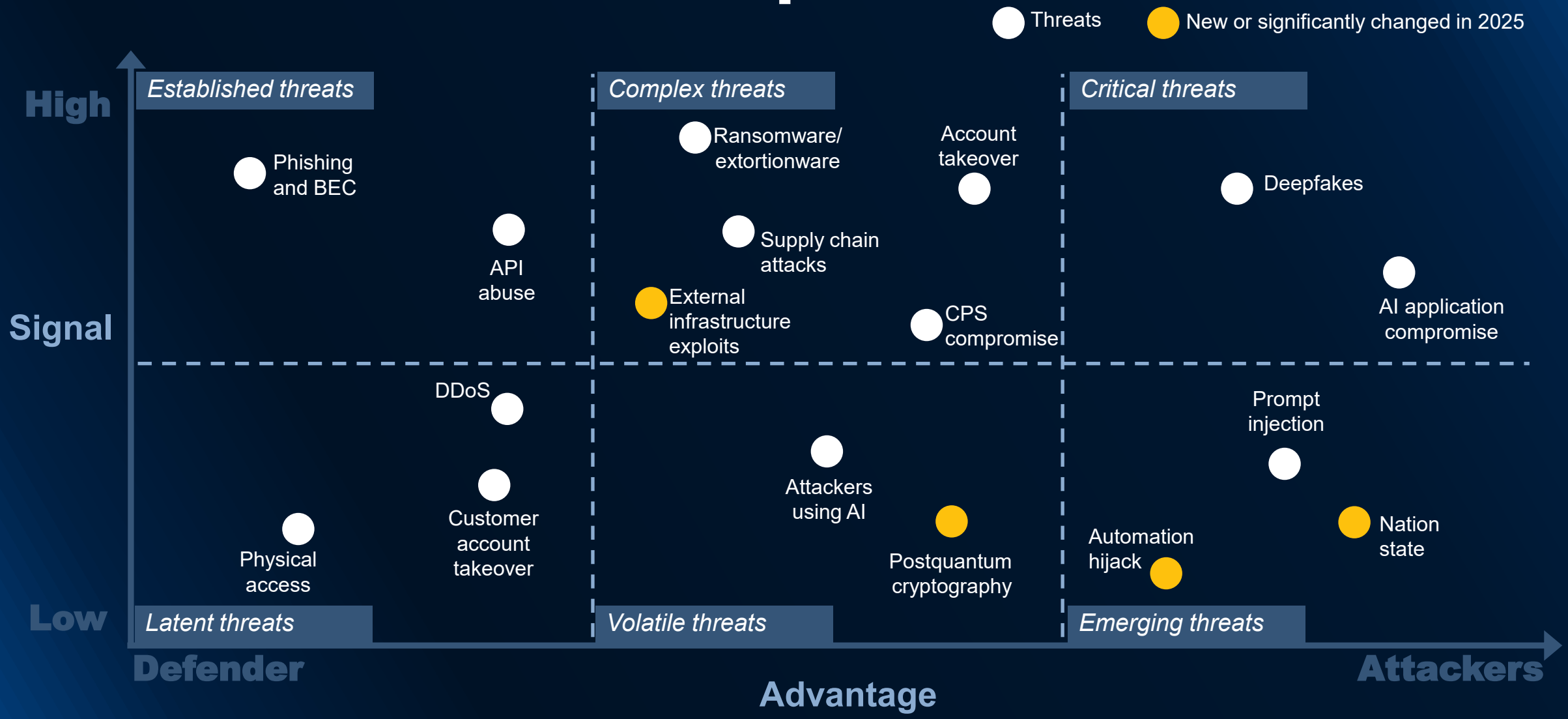
Leveraging profiling to target employees through their personal digital identities

Personal

Business

Gartner®

Gartner 2025 ThreatScape



Source: How to Respond to the 2025-2026 Threat Landscape

Gartner

Responding to the threat landscape is about prioritization

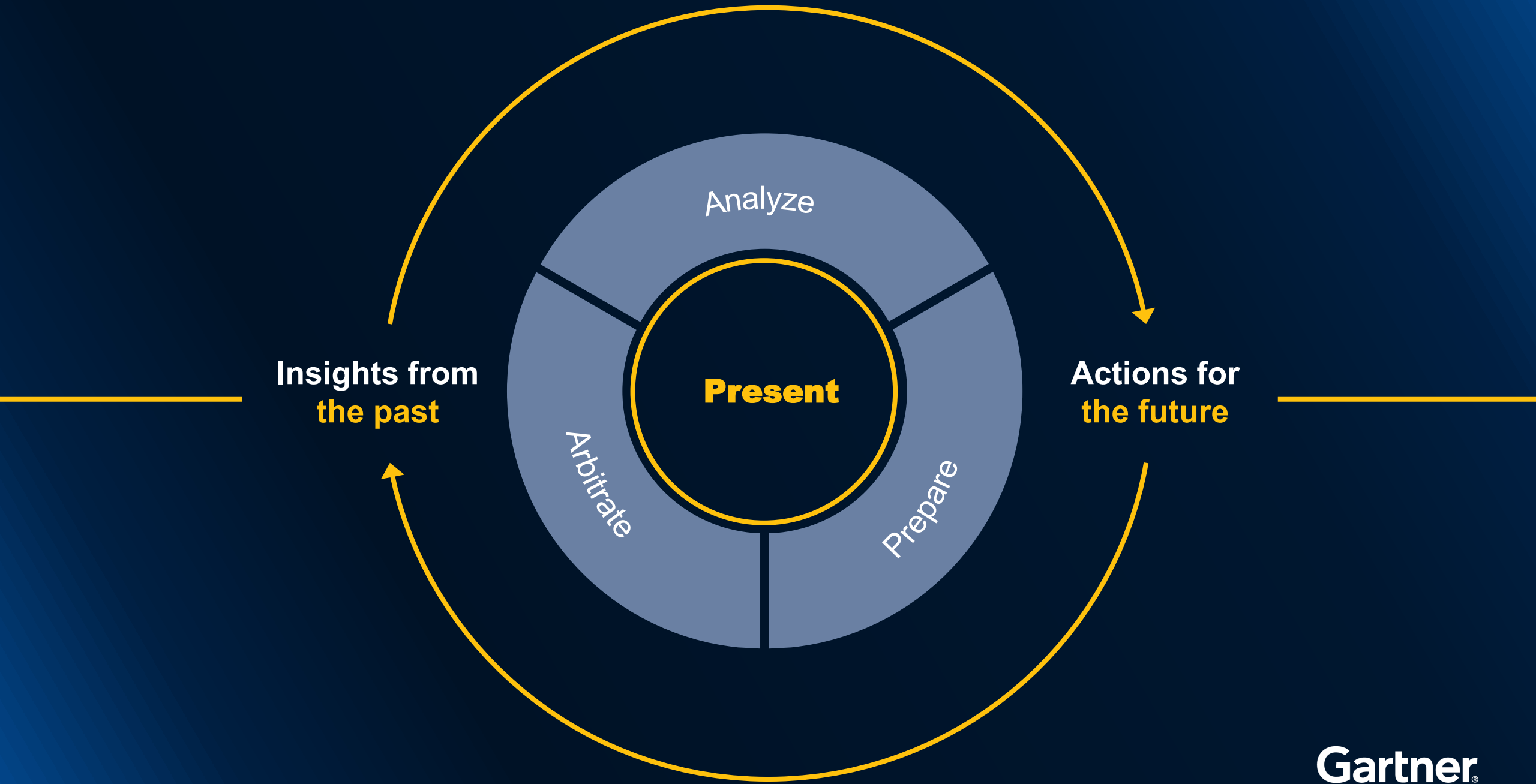
Gartner®

But how do we adapt?

Gartner®

To anticipate future threats

Gartner®


Insights from
the past
Analyze
Present
Arbitrate
Prepare
Actions for
the future

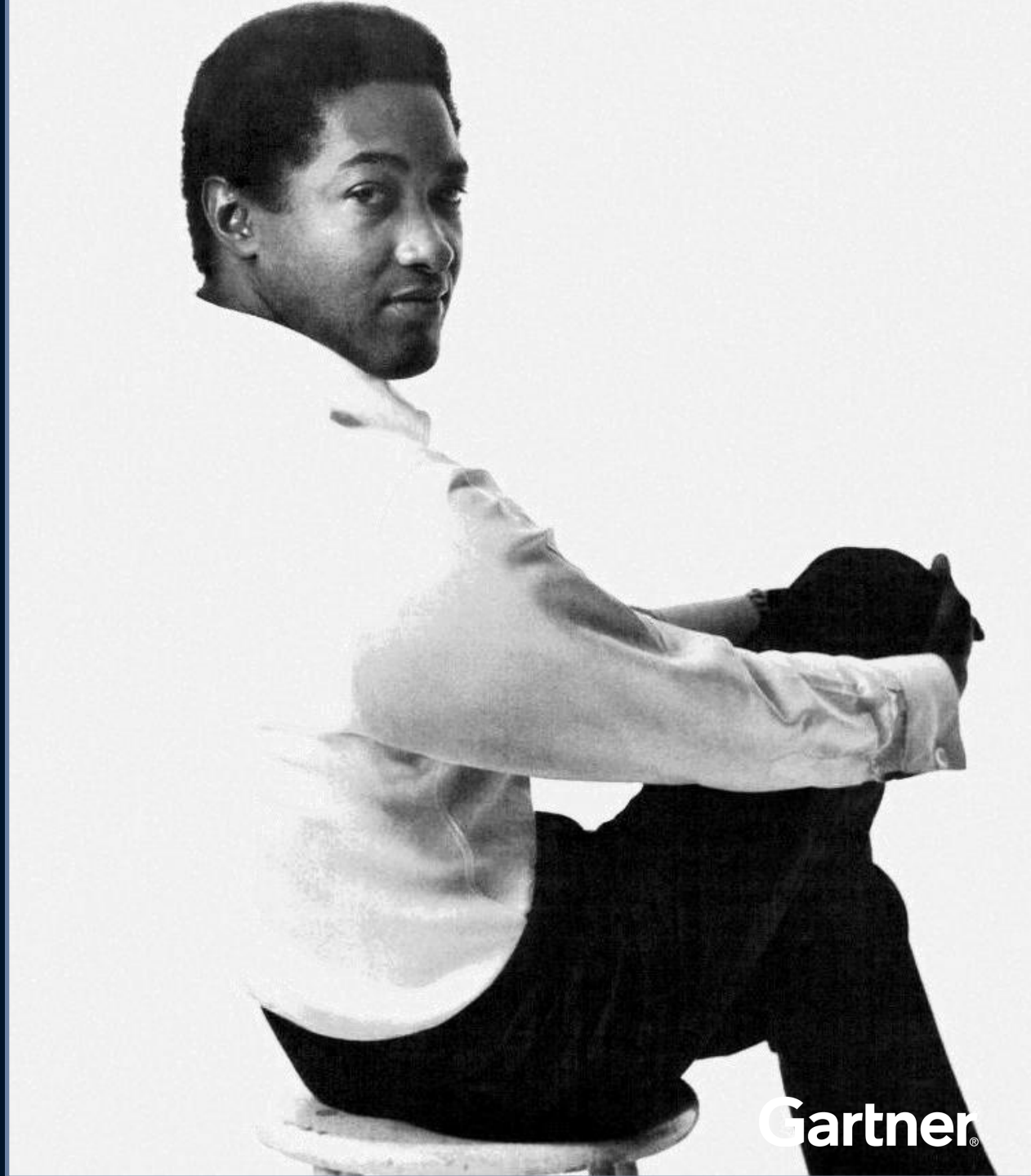
Gartner®

The AI Wave Will Not Recede for You

> There been times
> that I thought
> AI couldn't last for long

Sam Cooke

"A Change Is Gonna Come" — slightly modified



Source: Wikimedia Commons

Gartner®

5 Foundational Elements for the Future of AI

1. AI agents
2. **Composite AI** (e.g., decision intelligence and neurosymbolic)
3. AI engineering
4. AI literacy
5. Responsible AI

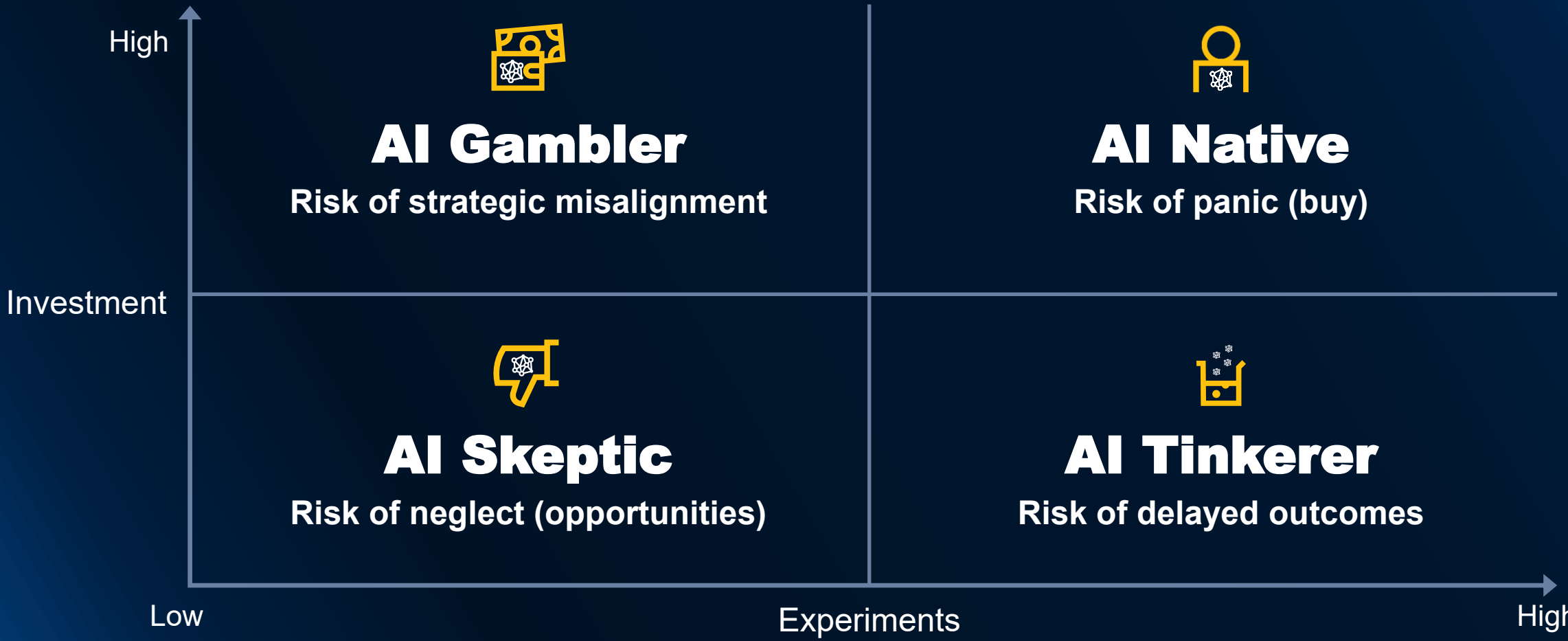
Gartner®

Technology or concept of the year will not solve everything.

Gartner®

The 4 AI Personas Shaping Roadmaps

Embracing AI diversity to enhance our strategic approach



Gartner

AI Tinkerer CISOs Multiply Safer Experiments

Continually experiment and adjust by scaling, extending or pausing based on value

1. AI usage control
2. Automated data classification
3. AI runtime controls
4. AI security testing
5. SOC augmentation
6. SOC replacement
7. Risk prioritization
8. Automated policy analysis

Next 6 months

AI Tinkerer

12-18 months

Gartner

Focus on Solving the Right Problems

Score vulnerabilities	Avoid creating vulnerabilities
Add automation to event triage	Reduce false positive rates
Replace or deskill staff	Augment and upskill team
Reduce cybersecurity cost	Reduce cost of breaches

AI adoption should be guided by identifying the right problems to solve, rather than allowing AI to dictate use-case design and development.

Gartner®

Implement Scenario Planning

1. Start with what is real

Extend possible scenarios from threat and business intelligence.

2. Develop scenario library

Incorporate GenAI impact in the most likely threat vectors.

3. Run AI scenario exercises

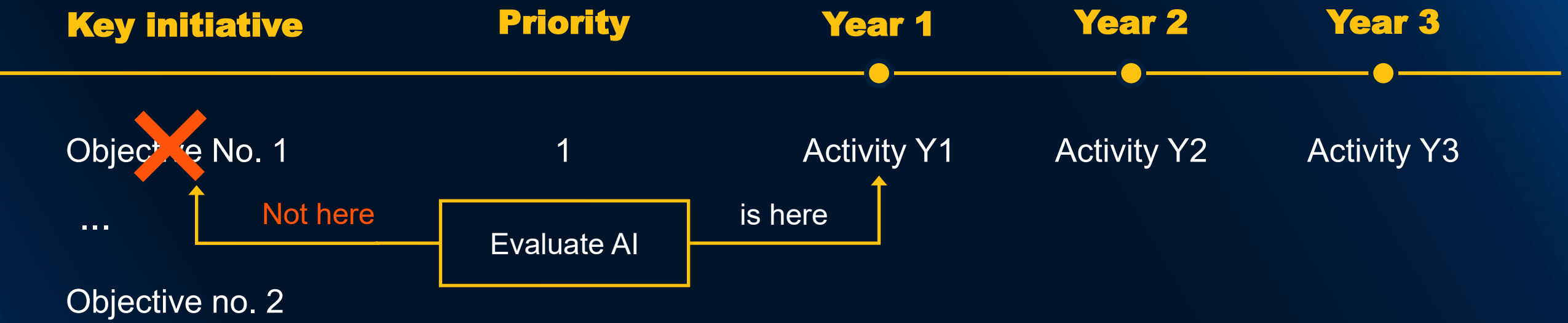
Run simulations and tabletop exercises.

4. Tune roadmap

Strengthen process. Prioritize exposure reduction.

Gartner®

AI Must Improve on Key Cybersecurity Objectives

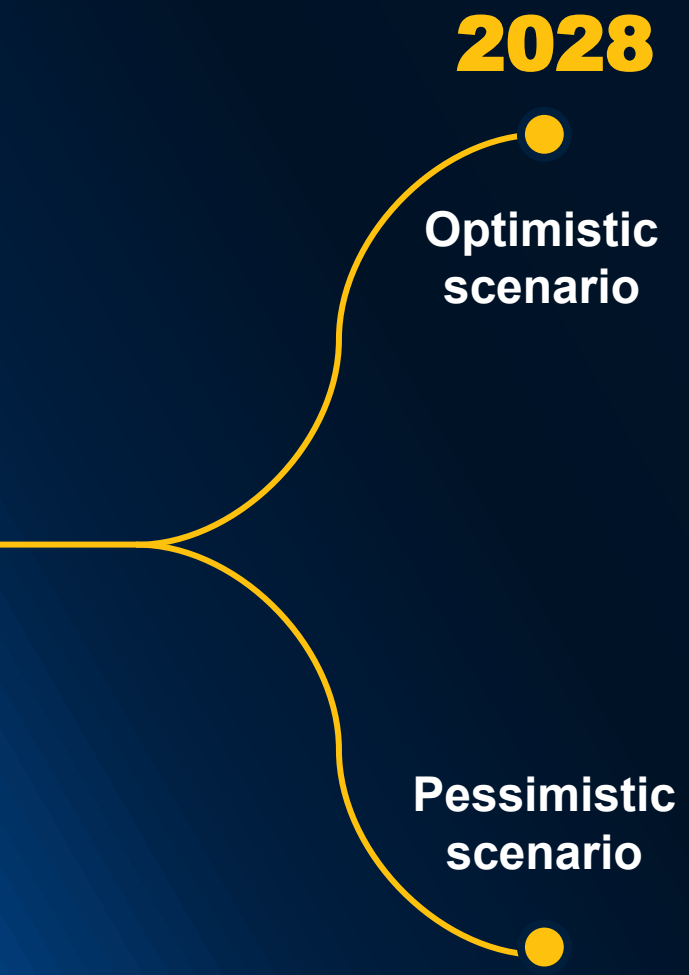


Objective no. 1 — Detail

Current situation	Gap	Target situation	Action plan and timeline
		Security metrics	AI experiments

Gartner

AI Agents Might Help But the Jury Is Still Out



By 2027, 25% of common SOC tasks will become **50% more cost efficient due to automation** enhancements and hyperscaling strategies.

Predict 2025: There Will Never Be an Autonomous SOC

By 2027, 30% of SOC leaders will have been **unsuccessful in their efforts to integrate GenAI** into production processes due to inaccuracies and hallucinations in outputs.

Predict 2025: There Will Never Be an Autonomous SOC

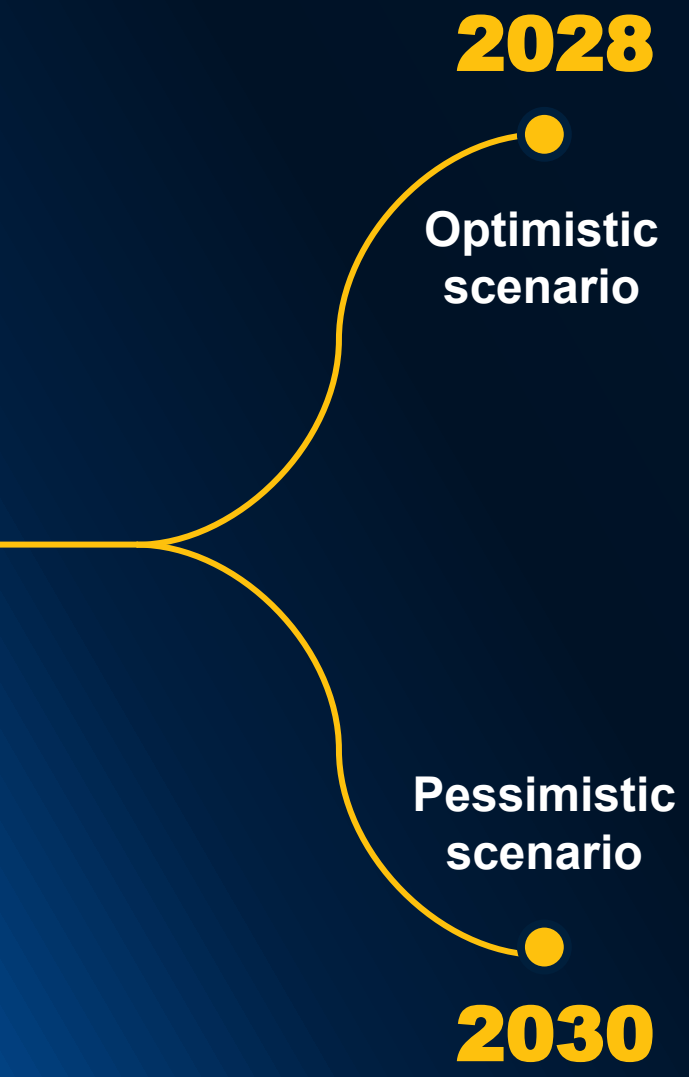
Gartner

“By 2027, **90% of successful AI** implementation in cybersecurity will be **tactical —** task automation and process augmentations — rather than role replacing.
”

Source:Predicts 2025: Navigating Imminent AI Turbulence for Cybersecurity

Gartner®

We need to Upskill for Cybersecurity in 2030



By 2028, **80% of digital workers will use** multimodal interfaces with **generative AI,** significantly improving task efficiency and workplace accessibility.

Predicts 2025: Empowering Workers With Intelligent Applications

By 2030, half of enterprises will **face irreversible skill shortages** in at least two critical job roles due to GenAI accuracy decline, skill erosion and uncompetitive pay.

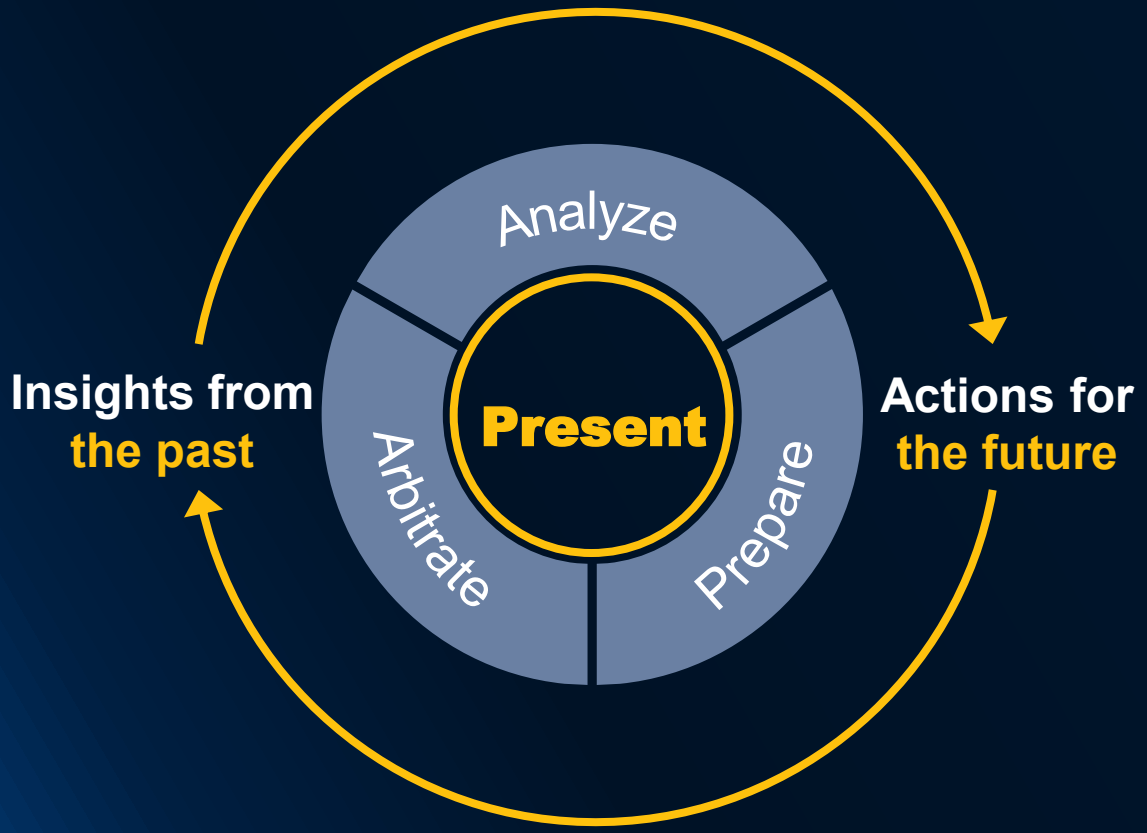
Predicts 2025: AI and the Future of Work

Gartner

“By 2030, the half-life of technical skills will shorten to two to five years from eight to 12 years, resulting in **adaptability and learning velocity** being the primary metric for hiring.”

Source: Predicts 2026: AI’s Impact on the Future of Workforce

Gartner®



- Defend increased investments
- Augment your team, don’t replace
- Adopt tactical AI as a strategic principle
- Work on compressed time horizons
- Select AI by cybersecurity objective
- Measure on outcomes
- Be an AI Tinkerer

Gartner®

“Il semble que la perfection soit atteinte, non quand il n’y a plus rien à ajouter mais quand il n’y a plus rien à retrancher.”

— Antoine de Saint-Exupery,
Écrivain, poète, journaliste et aviateur

Gartner®

Cyberweek[25]

Perspectives Cybersécurité 2025-2030

Jeremy D'Hoinne

Gartner®