Microsoft

Keep Pace

Freddy Dezeure
DCISO for Europe

European digital commitments

1. We will help build a broad AI and cloud ecosystem across Europe.
2. We will uphold Europe's digital resilience even when there is geopolitical volatility.
3. We will continue to protect the privacy of European data.
4. We will always help protect and defend Europe's cybersecurity.
5. We will help strengthen Europe's economic competitiveness, including for open source.

We are committed to Europe

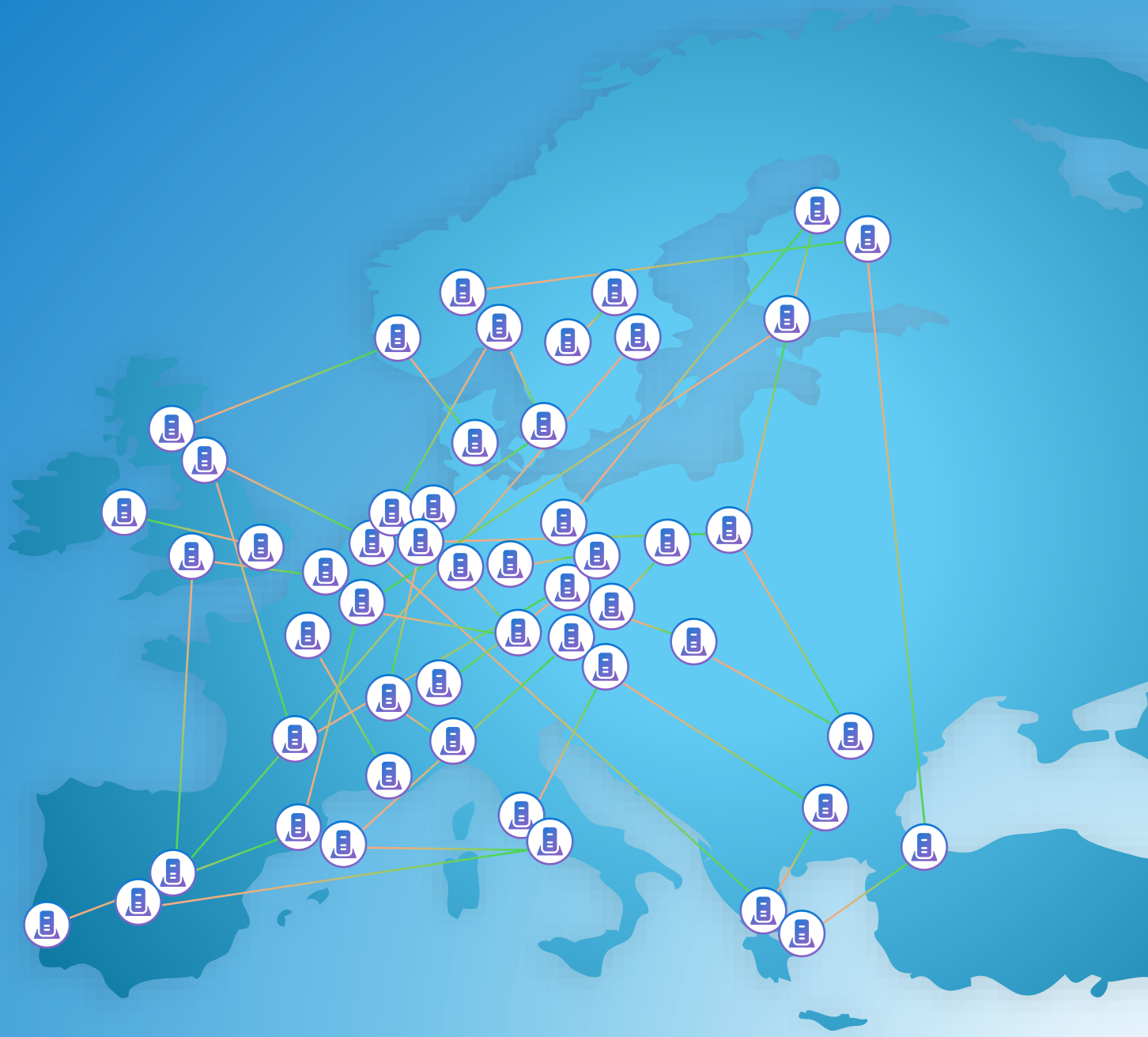
Microsoft Ireland Operations Limited Board

Significant footprint (+20%)

Regionally-specific services

EU data boundary

EU-specific contract terms



COMMITMENT

4

We will always help protect and defend Europe’s cybersecurity.

Deputy CISO for Europe

About my role

A Protect MSFT and its customers

B Comply with European regulations

C Secure by default

Cybersecurity Governance Council

CISO
Igor Tsyganskiy

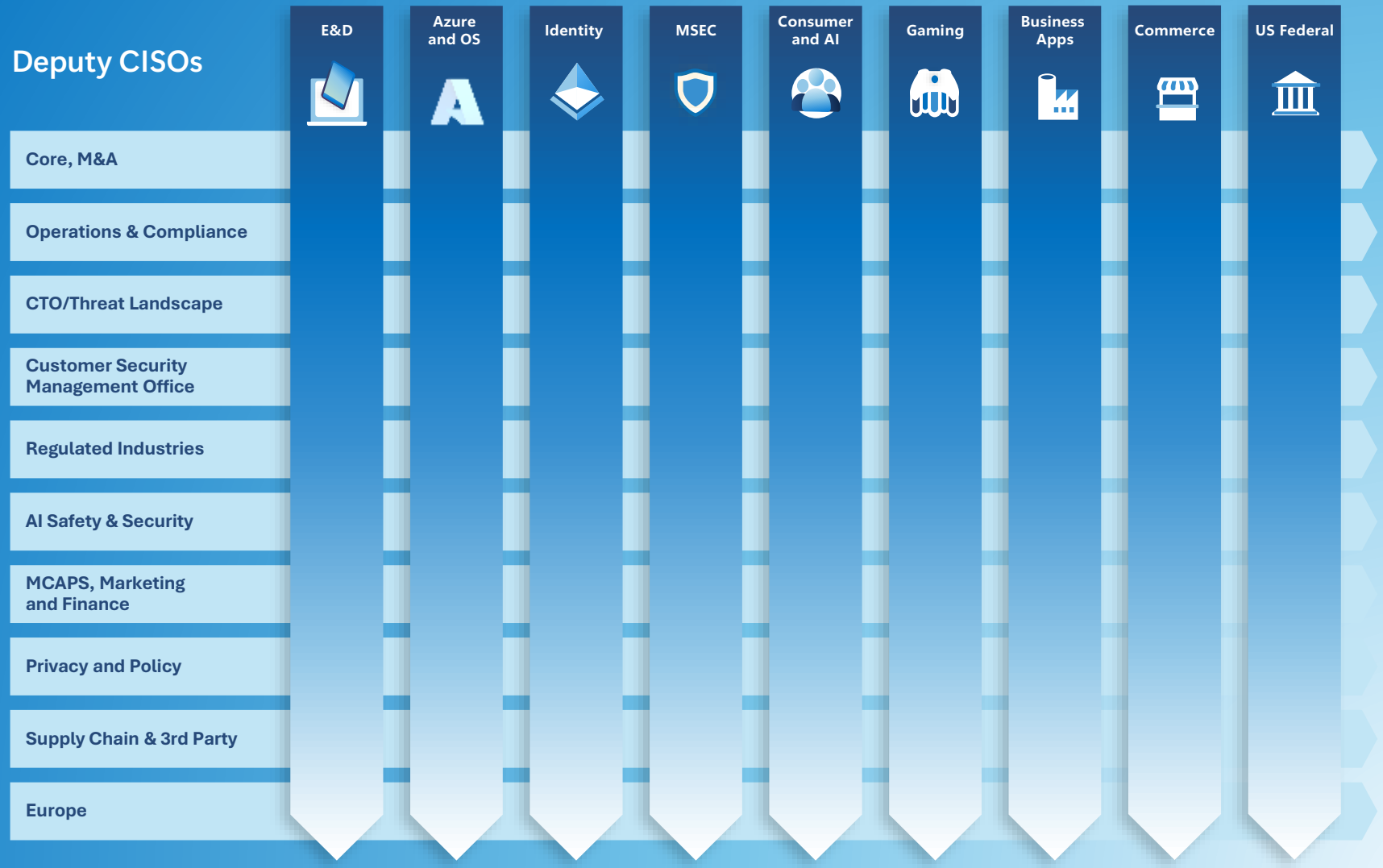
Secretary
Amy Hogan-Burney

CISO

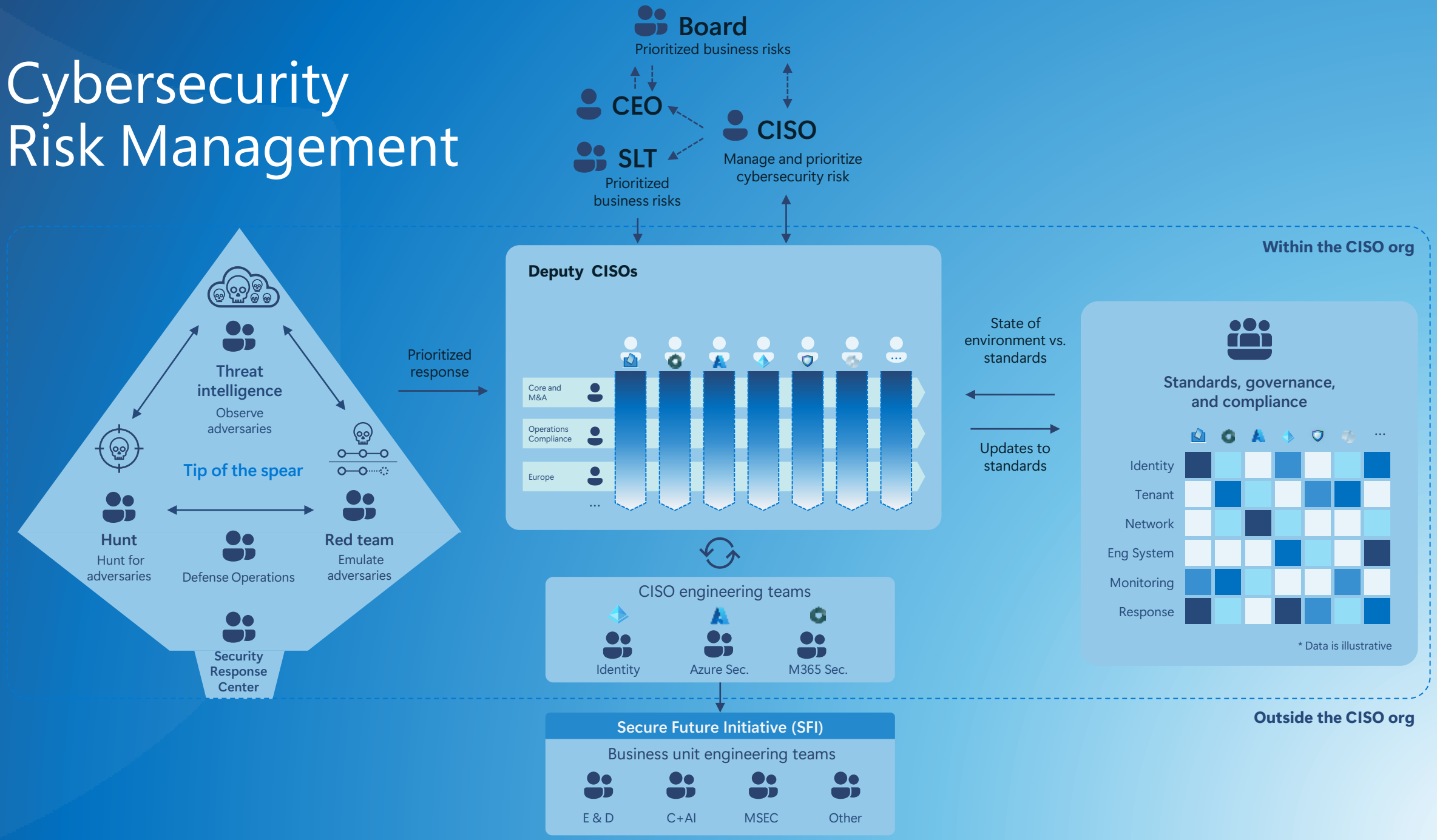
- Accountable to manage & prioritize Microsoft's cybersecurity risk.
- Report cybersecurity posture to SLT and Board of Directors.
- Lead CISO Organization.

Deputy CISO

- Risk ownership and accountability incl. regulatory implementation and compliance within their domains.
- Contribute to design of overall Microsoft security architecture.

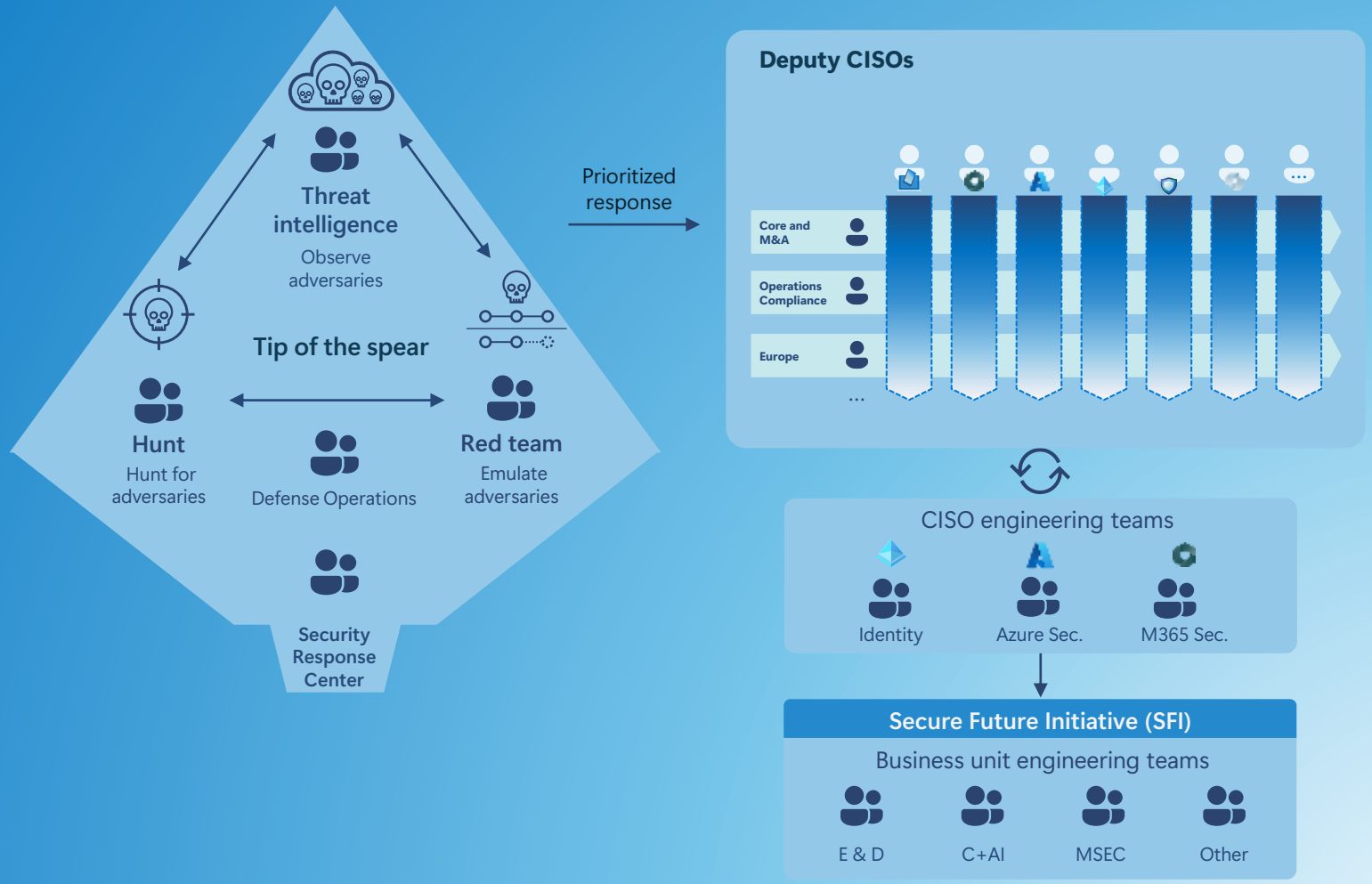


Cybersecurity Risk Management

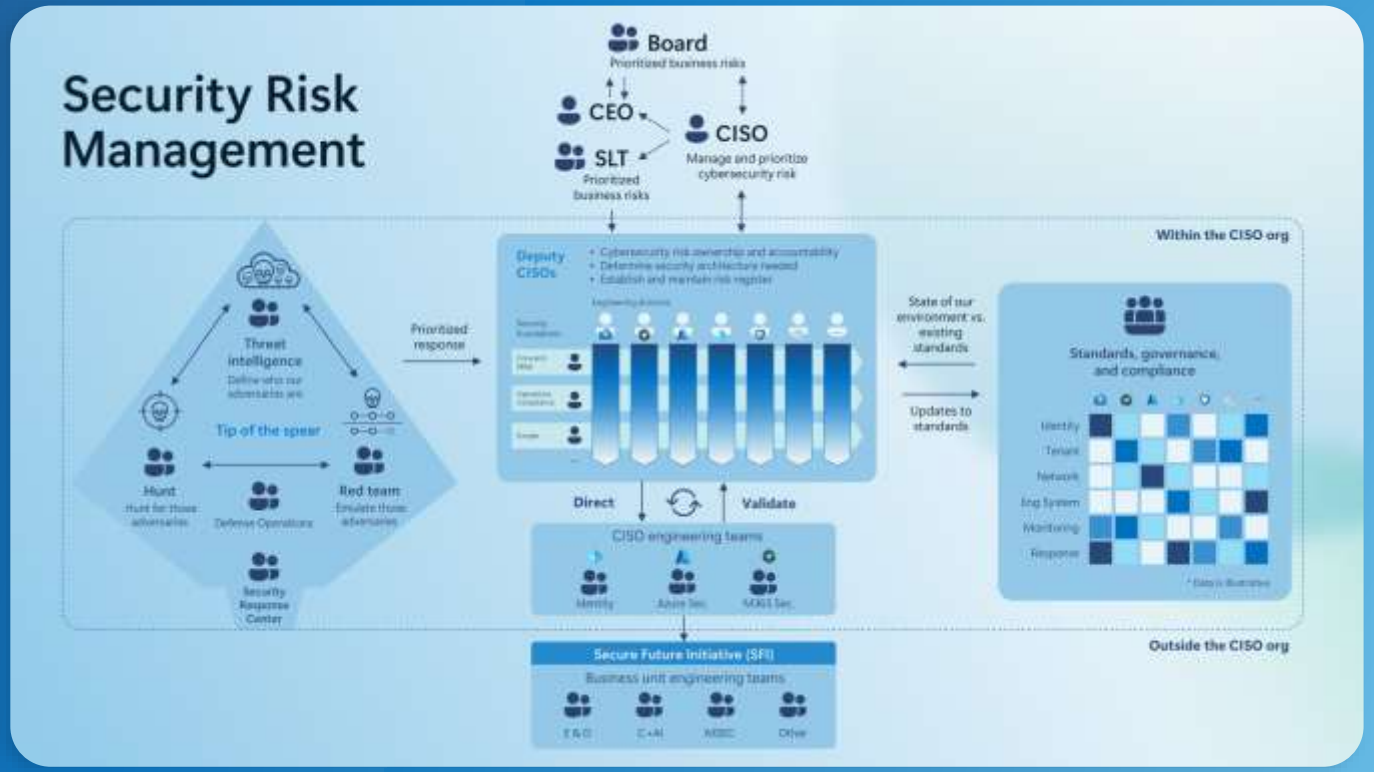


Impactful structure and operation

- Meeting twice a week (or more)
- Cross-function expertise and decision making
- Quasi-real-time threat-informed defense
- Visibility and impact at scale
- Durable improvements in infrastructure and services



Active defense

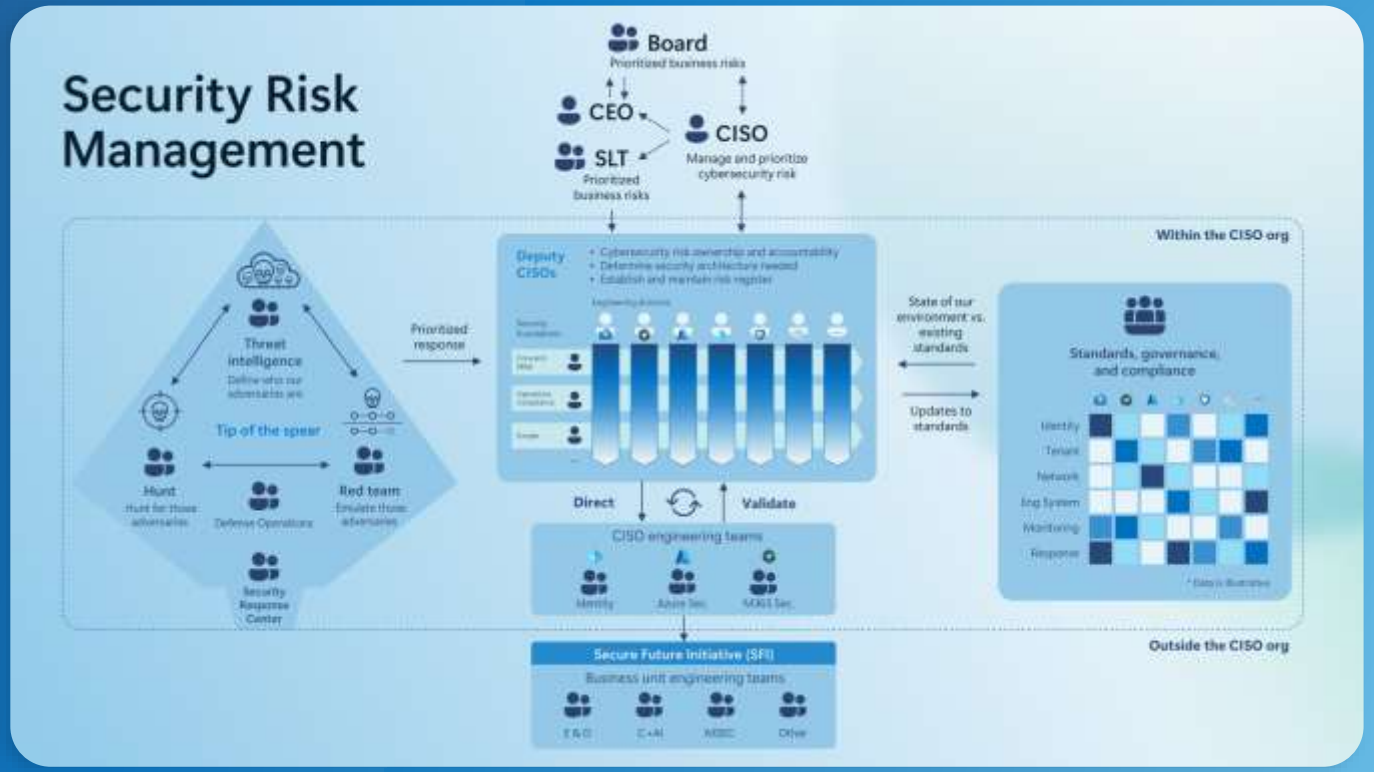


Microsoft tenants

Customer tenants

Microsoft infrastructure and services

Secure by Default



Microsoft tenants

Customer tenants

Microsoft infrastructure and services

Secure Future Initiative (SFI)

Security principles

- Secure by design
- Secure by default
- Secure operations

Security culture and governance

Engineering pillars

- Protect tenants and isolate production systems
- Protect identities and secrets
- Protect networks
- Protect engineering systems
- Monitor and detect threats
- Accelerate response and remediation

Paved path — **Continuous improvement** — Standards

Baseline Security Mode

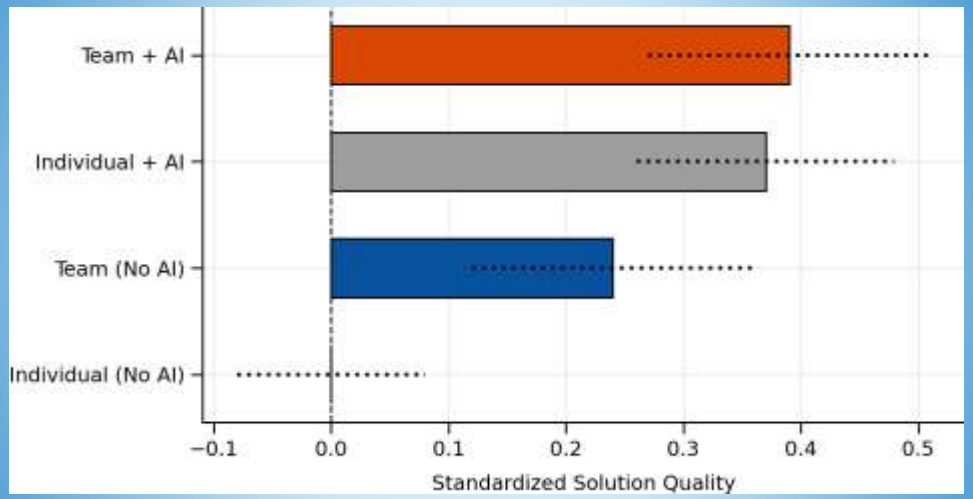
- Turns Secure Future Initiative learnings into protection of tenants against known attack paths.
- Built-in impact analysis, exclusions, and staged rollout enable to adopt protections safely and at scale.
- One entry point in the Microsoft 365 admin center.
- Expansion across Microsoft 365, Entra, Intune, Purview, Dynamics 365, and Azure in fall 2026.
- All new tenants come with BSM controls

- Customers benefit from how Microsoft defends itself.

Baseline security mode settings | Microsoft Learn

AI Impact

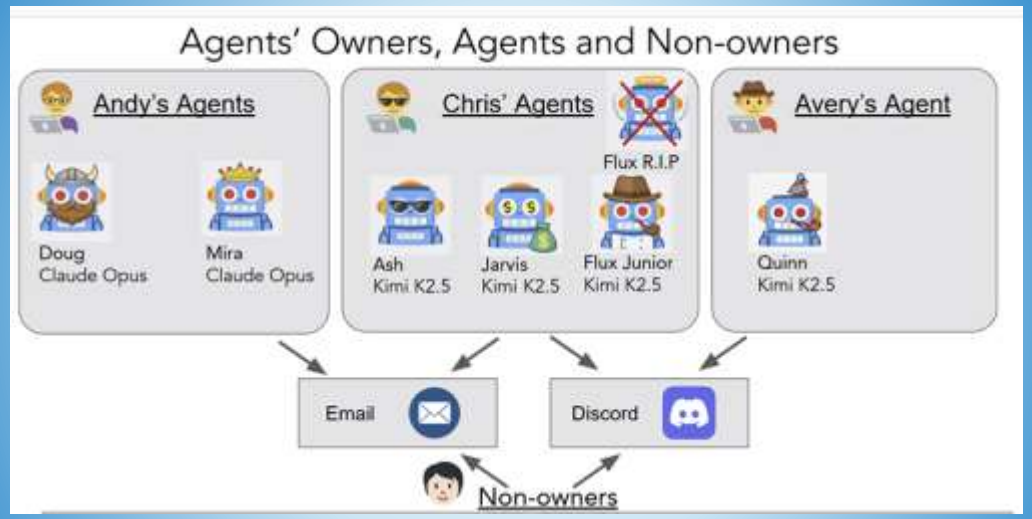
The Cybernetic Teammate



- Harvard Business School field experiment with P&G employees
- Individuals+AI produce better quality than teams
- AI democratizes expertise
- AI reduces bias from dominant individuals in teams
- Individuals are happier, with an AI companion

The Cybernetic Teammate: A Field Experiment on Generative AI Reshaping Teamwork and Expertise

Agents of Chaos



- Exploratory study of AI agent behaviour (OpenClaw)
  - Unauthorized compliance with non-owners
  - Disclosure of sensitive information
  - Execution of destructive system-level actions
  - Identity spoofing vulnerabilities
  - Cross-agent propagation of unsafe practices
  - Partial system takeover
- Issues with accountability, authority, and responsibility

Agents of Chaos

AI Powered Risks

In the Hands of our Adversaries

- Spear phishing efficiency: 54% click rate*
- Automated discovery of vulnerabilities
- Cyber attacks – kill chain
  - Democratization, tailoring
  - Acceleration
  - Increase in scale

* Evaluating-Large-Language-Models-Ability-to-Automate.pdf

In our Hands

- Spear phishing
  - Use AI to detect (97% success rate*)
- Vulnerabilities
  - Discover our own vulnerabilities**
  - Patch at our own pace
- Incident response
  - Identify our most (and least) critical assets
  - Contain without perfect knowledge

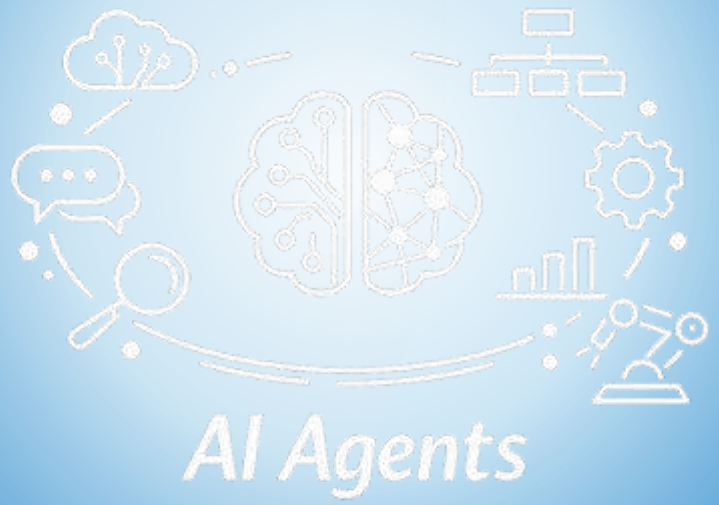
* Evaluating-Large-Language-Models-Ability-to-Automate.pdf

** Project Glasswing

AI Agents at Work

Agentic AI Controls

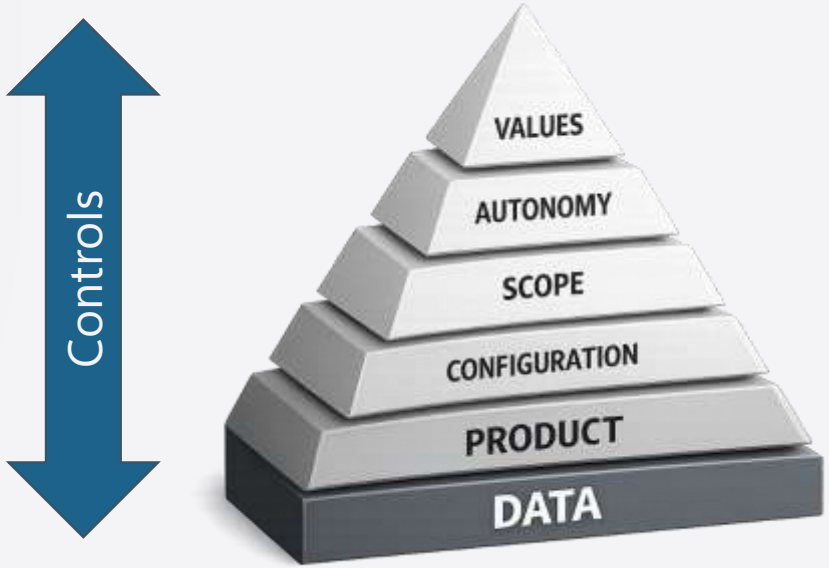
- Product security
  - OWASP AI
  - MITRE ATLAS
  - Secure by design
- Enterprise security
  - NIST CSF, NIST 800-53, ISO 27001
  - MITRE ATT&CK
  - CIS Baselines
  - Secure by default
- Controls update frequency and coverage…



AI Agents – New Hires

- Gaps in our understanding
  - Black boxes
  - Non deterministic
- Pace of technological evolution
- Pace of task execution
- Democratization of development – shadow Agents
- Gaps in our frameworks (HR policies)

Proposed Reference Model

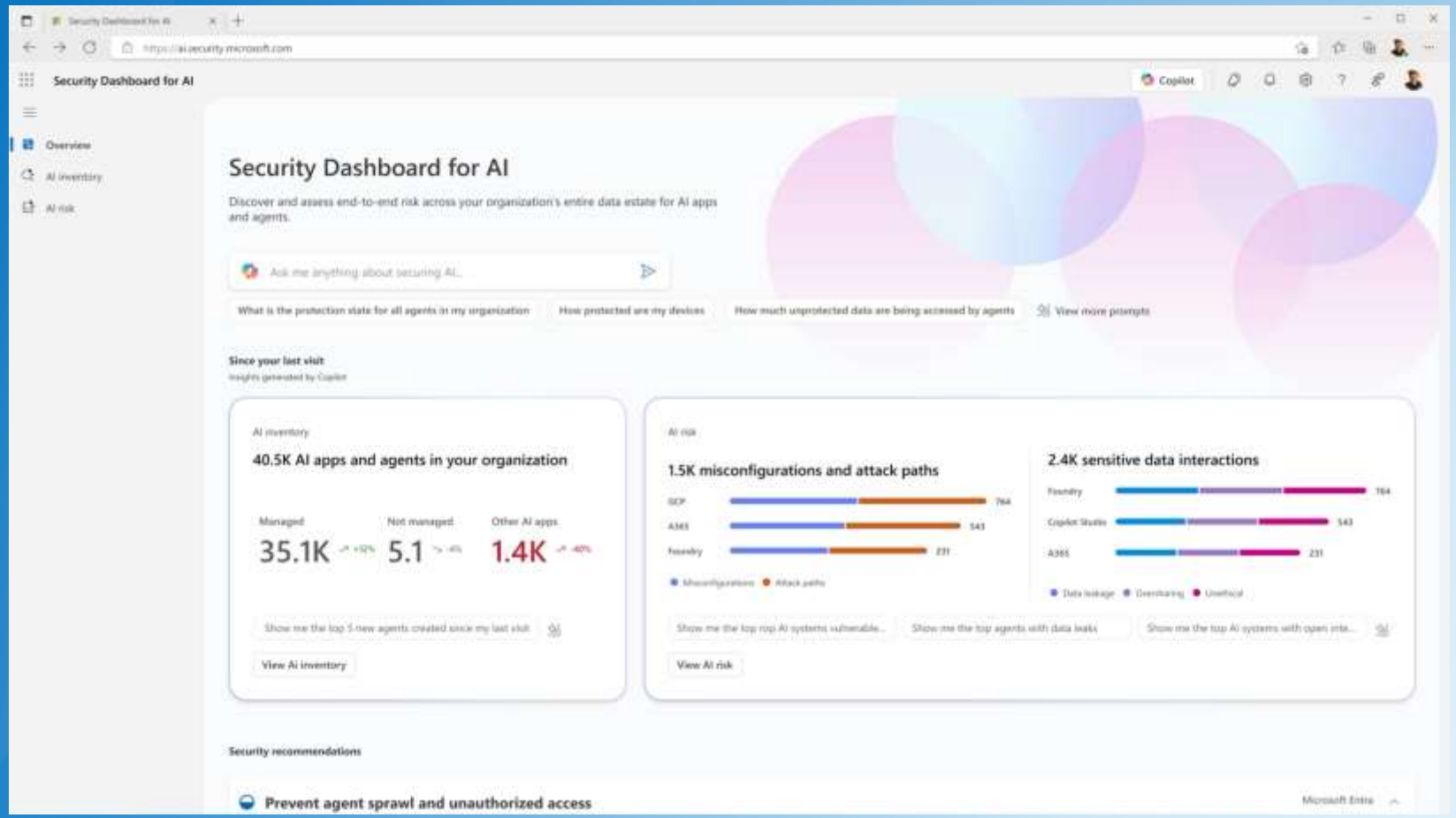


Values	Corporate values the agent must respect
Autonomy	What actions is the agent allowed to take?
Scope	Which access to data, systems, agents?
Configuration	Guardrails, filters, policies at runtime
Product	Model, pipeline, API, SDK security
Data	Provenance, lineage, classification, integrity

Proposed Reference Model

- Values
  - Should AI agents respect the same corporate values as humans?
- Autonomy:
  - Can AI agents modify, delete data?
  - Can they carry out financial transactions and to which threshold?
  - Are they allowed to take initiative?
  - Can they launch physical action?
  - Is a human-in-the-loop required for critical actions?
  - Do we need a “kill switch”?
  - Can we roll back their actions?
- Scope:
  - To what data, services, systems has the agent access?
  - Do AI agents have access to the internet and to other agents?
  - What are their primary role and success factors?
- Data layer is the foundation
  - Provenance, lineage, classification, integrity
- How do we train and contain the AI agents?

Security Dashboard for AI



Microsoft Security Dashboard for AI

Wrapping up

- Use AI to defend
- Respond to incidents with incomplete knowledge
- Treat AI agents as employees
- Train and contain your AI agents
- Deploy AI controls at pace - by default

- Call to action: Update our control frameworks

Microsoft

Thank you!

Freddy Dezeure
DCISO for Europe