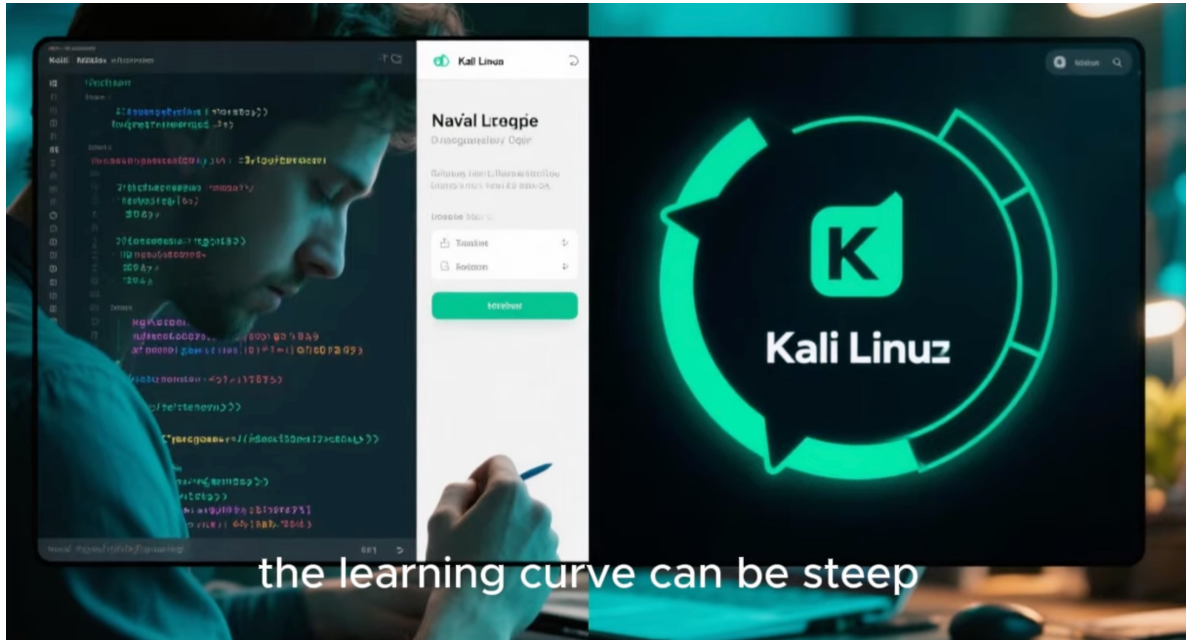
AI Driven Cyber Threats: How Prepared are we Really?

Lightning Talk

Nabil Benamar (SSAC)

ICANN’85

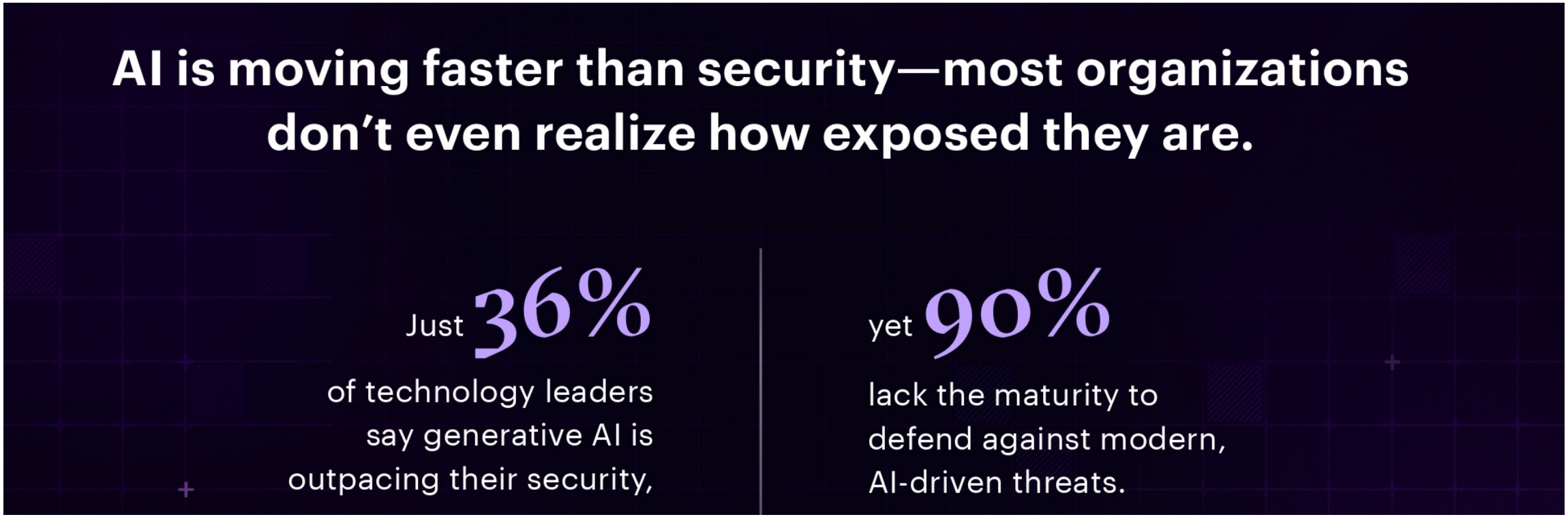
Kali Linux Integrates Claude AI



CROWDSTRIKE 2026 GLOBAL THREAT REPORT

Some threat actors have executed operations using agentic AI via Anthropic's Claude Code Model Context Protocol (MCP) tools, which require minimal human oversight.

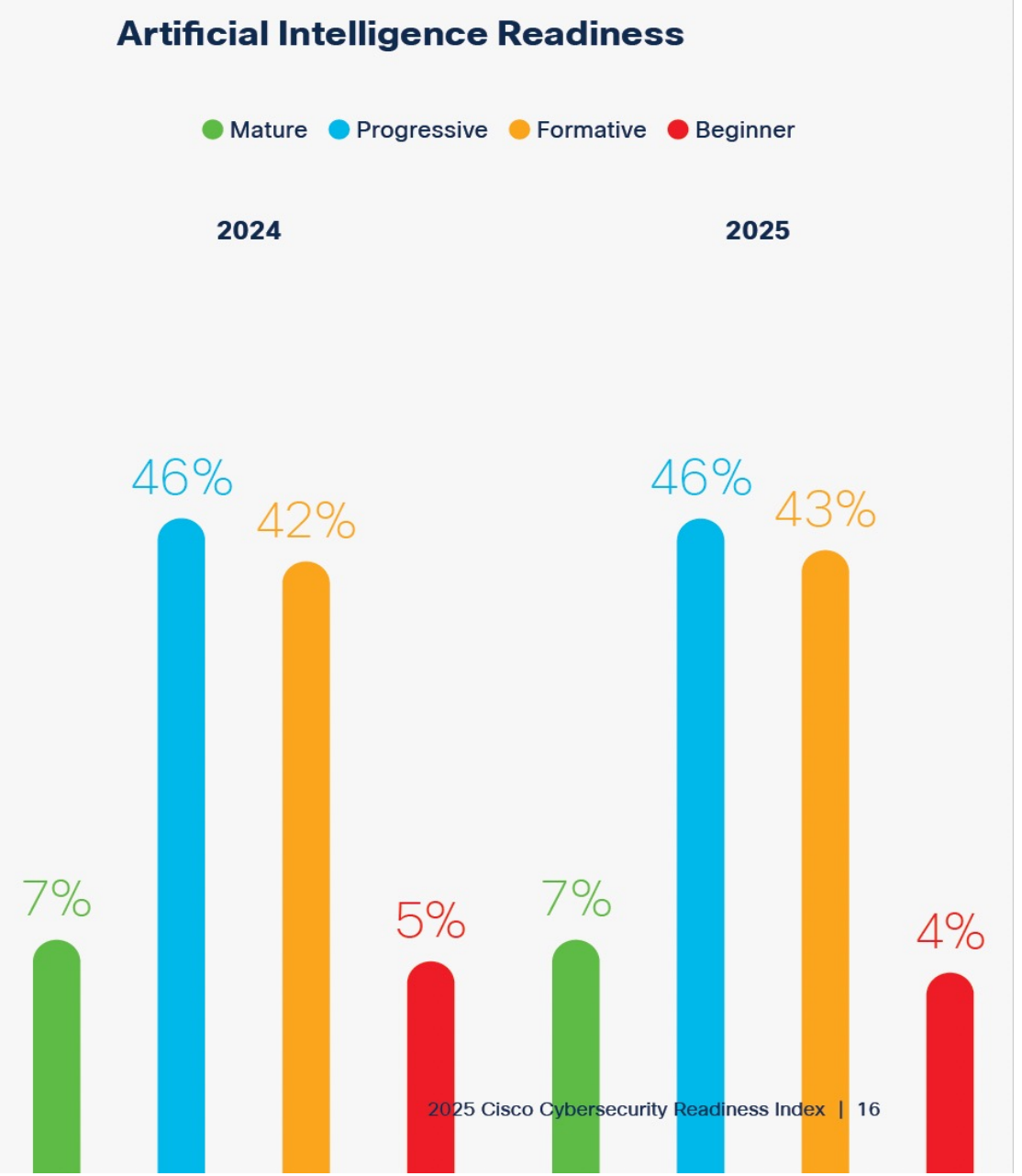
From Accenture



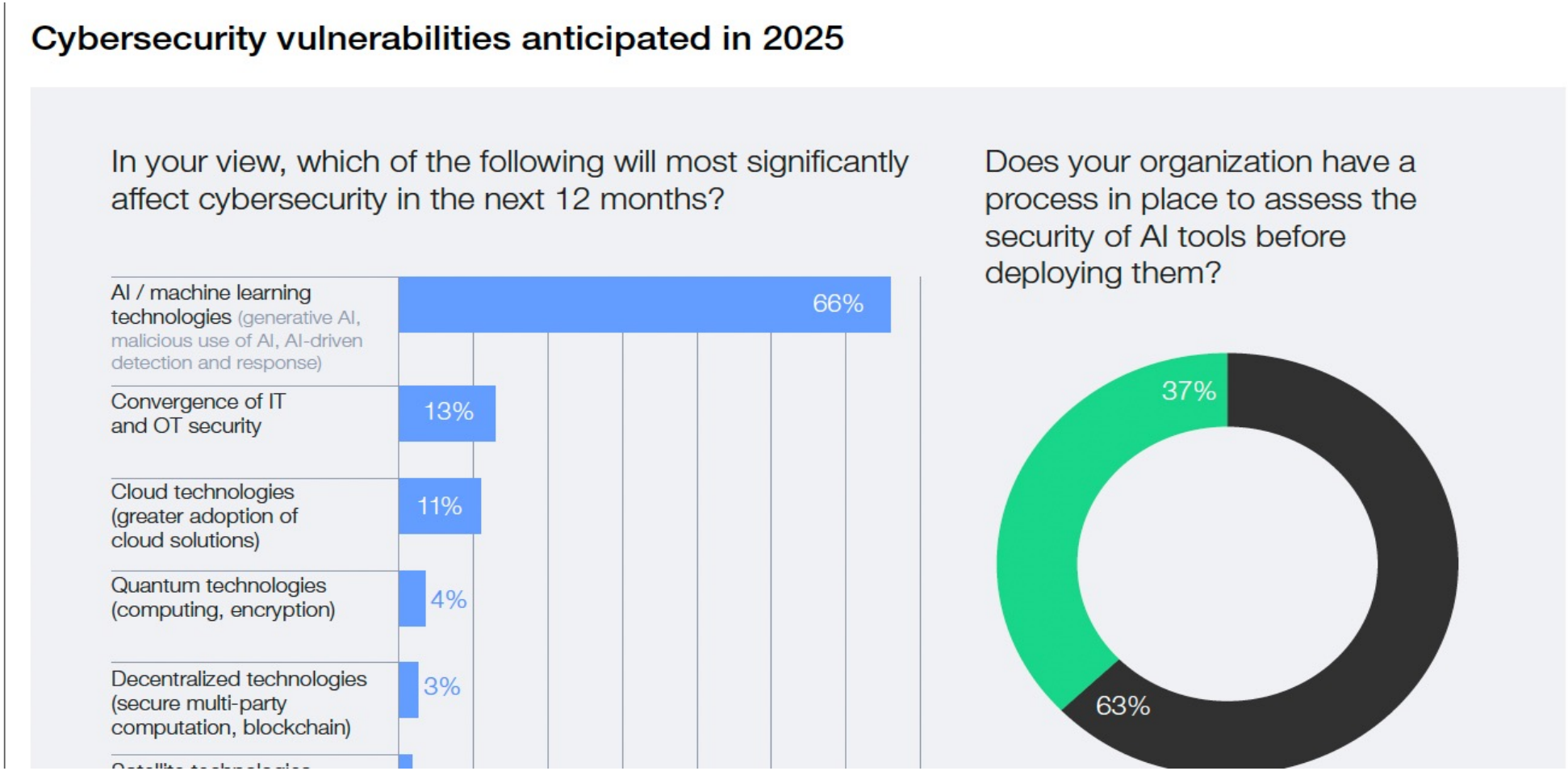
Only **34%**

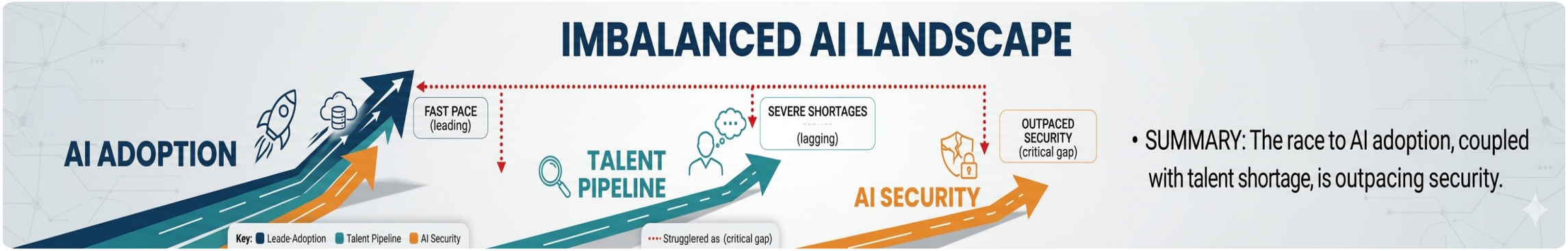
of organizations have a mature cyber strategy. Fewer still—just 13%—possess the advanced cyber capabilities needed to defend against modern, AI-driven threats.

A report from Cisco



Rapid AI Adoption is Creating a Security Gap



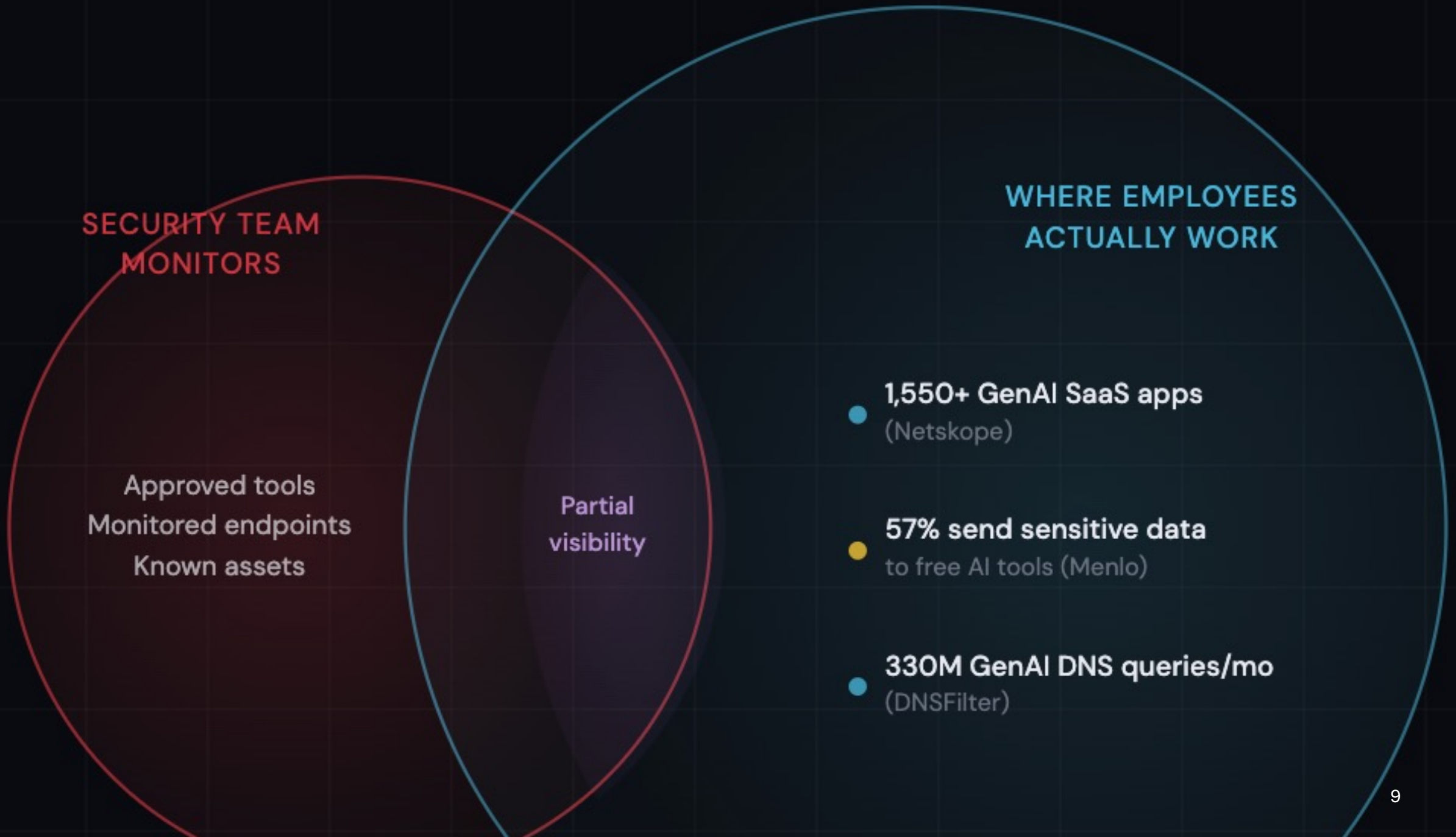


Cybersecurity talent shortage

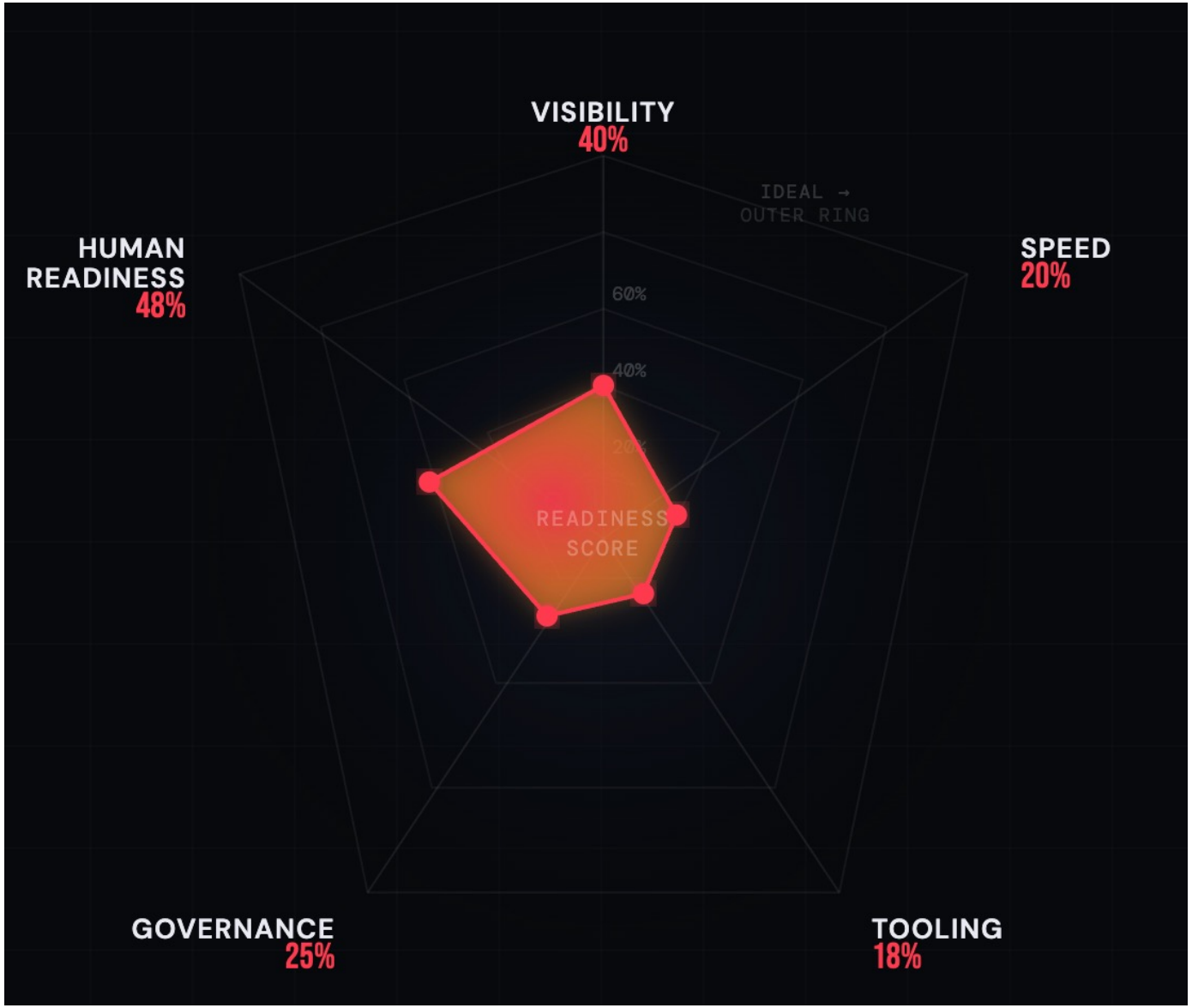
- This challenge is further compounded by a critical cybersecurity talent shortage, with 83% of executives identifying it as a major obstacle to achieving a strong security posture

Shadow AI

- *"60% of organizations cannot see what prompts their employees are sending to GenAI tools." (Cisco 2025)*


SECURITY TEAM MONITORS
Approved tools
Monitored endpoints
Known assets
Partial visibility
WHERE EMPLOYEES ACTUALLY WORK
1,550+ GenAI SaaS apps (Netskope)
57% send sensitive data to free AI tools (Menlo)
330M GenAI DNS queries/mo (DNSFilter)

The Five Dimensions of Unpreparedness



What Organizations can Do Today?

01 · VISIBILITY

Know Every AI Tool Your Employees Use

02 · DETECTION

Retool for Malware-Free Attacks

03 · SPEED

Shrink Your Response Window

Train Staff on AI-Specific Threats