TÜRKİYE AI SECURITY CISO SURVEY 2026

CISO CONNECT

An Exclusive CISO Platform

Methodology & How to use

Survey Scope & Participants

- The survey was conducted with **63 CISOs** from **CISO Connect**, an exclusive CISO platform built by **CISOs from Türkiye's largest enterprises**.
- Participants represent a broad and strategically critical cross-section of the Turkish economy, including **automotive, aviation, banking, energy, finance, fintech, FMCG, health, holding groups, insurance, logistics, online trade/e-commerce, retail, service providers, telecom and textile/apparel** sectors.

Survey Format

- Based on a **structured questionnaire** covering:
  - AI adoption & readiness
  - AI-related risks & threat landscape
  - Benefits and use cases of AI in security
  - Barriers, compliance challenges, and workforce impact
  - Strategic expectations for AI-augmented Security

Why This Survey Matters

- Provides the **most up-to-date view of AI adoption and AI risk perception** among Türkiye's largest enterprises
- Reflects the cybersecurity priorities of organizations representing **a major part of the country's enterprise-scale digital footprint**
- Highlights how Türkiye's largest companies are preparing for **AI-driven threats, compliance pressures, and SOC modernization**

How to Use These Insights

- Benchmark your organization's progress against the **largest CISO sample in the country**
- Guide **AI strategy, investment decisions, and risk management planning** for 2025–2026
- Inform board-level conversations on **AI governance, SOC transformation, and workforce readiness**

For Participating to the Survey

- If you are a CISO and would like to participate in the survey, please contact me at gokhan@cybridge.tech

A Personal Thank You Note to Participating CISOs

A heartfelt thank you to all CISOs who generously contributed to this survey. Your contributions are invaluable — your insights and experiences form the foundation of this report, reflect the collective intelligence of Türkiye’s leading CISOs and not only help us understand the current AI security landscape, but also shape the roadmap for our entire community.

CISO Connect is built by all of you, and this survey is yet another example of the strength of our collaboration.

I am truly grateful for your time, expertise, and ongoing support.

Gökhan Say
CEO
Cybridge Ventures

Current Landscape of AI Adoption and Risks

C-SUITE PRIORITY

ADOPTION & BARRIERS

KEY RISKS & THREATS

BENEFITS IN SECURITY

AI as a C-Suite Priority

AI has transitioned from a **novelty** to a critical component of enterprise strategy.

86%

How much of a C-Suite priority is generative AI in your organization?

GenAI Has Become a True Board-Level Priority

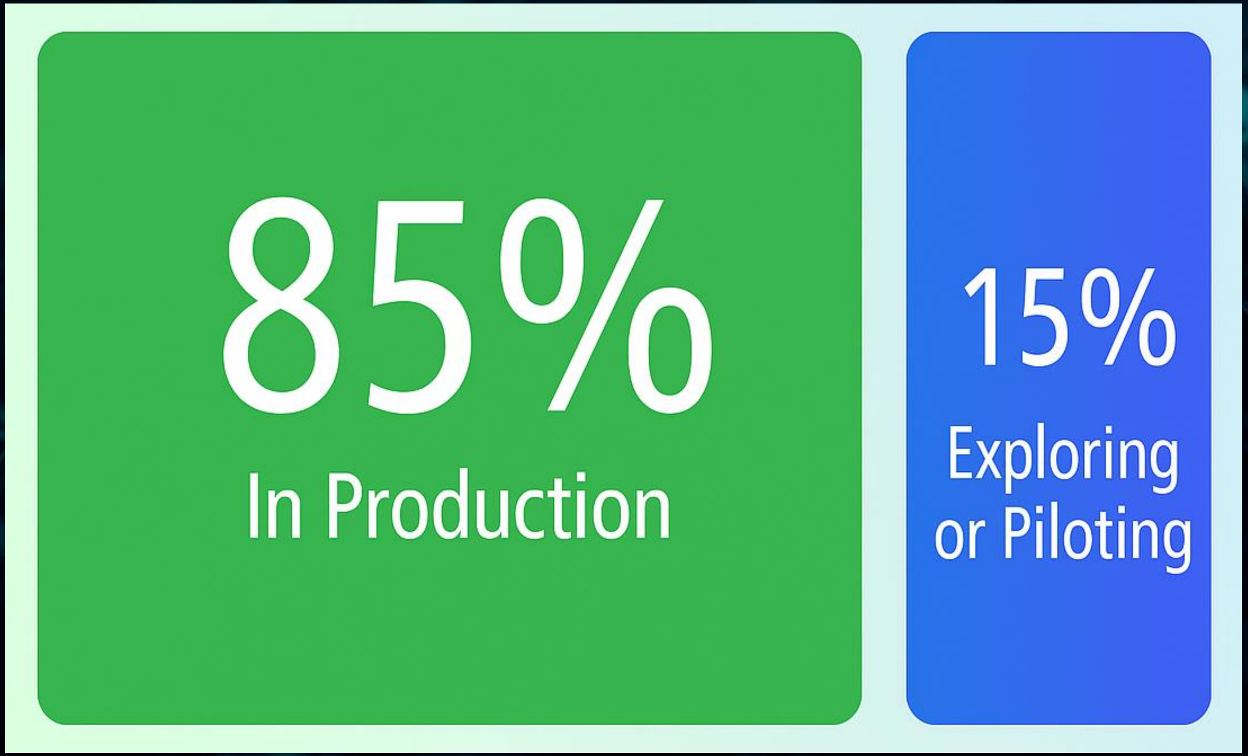
- For almost everyone in the survey, GenAI is no longer an experiment or side project; it’s on the formal C-suite agenda.
- That means CISOs and security leaders are expected *not* to block it, but to show *how* to adopt it safely and responsibly.
- ***“The debate is not if we use GenAI, but how we use it while controlling the risk.”***

Stage of AI Adoption

AI Adoption Has Moved From Pilots to Production

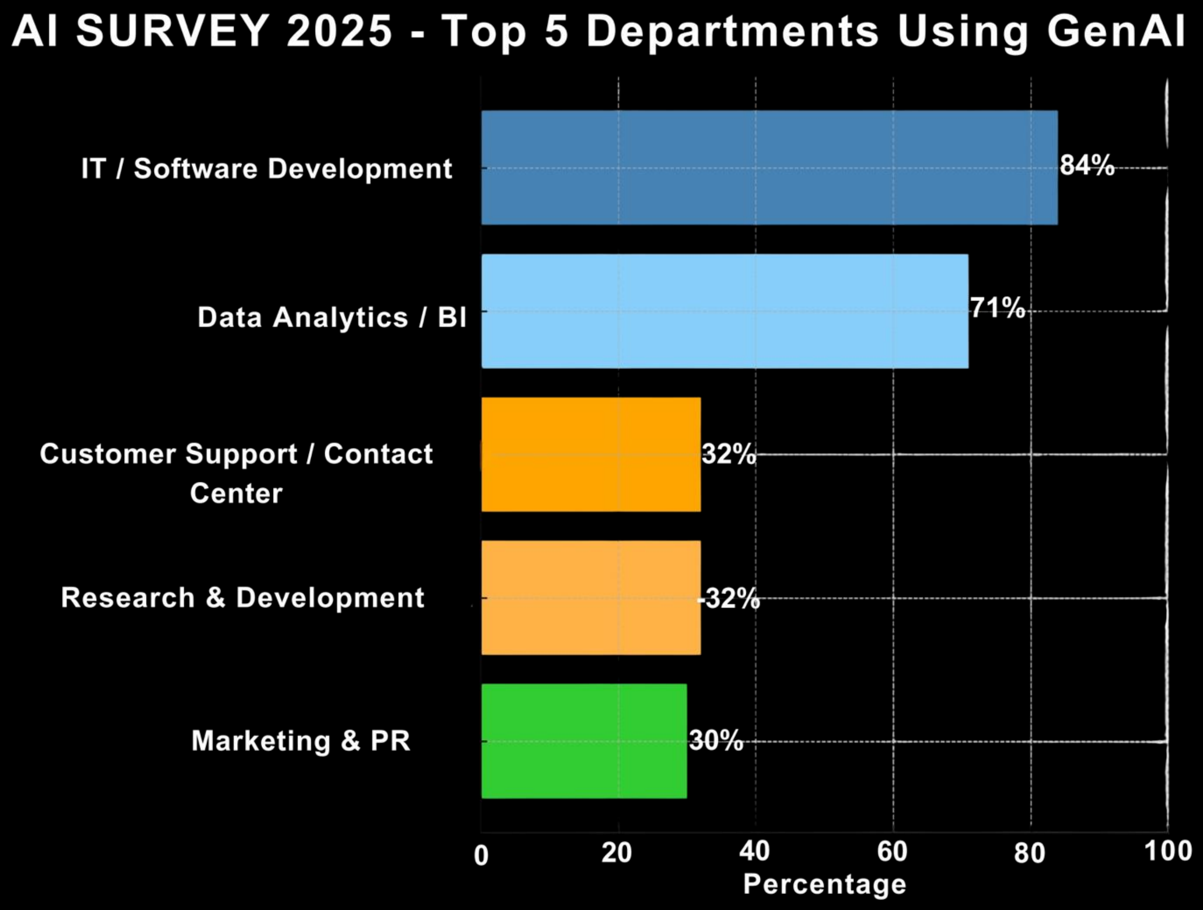
- ✓ The majority of organizations in the survey already have AI systems in production, not just in labs or PoCs.

What stage of AI Adoption is your company currently in?



Yet AI is Mainly a Tech & Data Story, Not Yet Fully Business-Wide

- Top adopters are **IT/Dev** and **Data Analytics/BI.**
- Business-facing functions like **Customer Support, R&D, Marketing/Comms** are in the 30–32% band.
- **Cross-functional AI councils or steering groups** involving engineering, data, security, compliance and business owners will be critical for true enterprise-wide adoption.

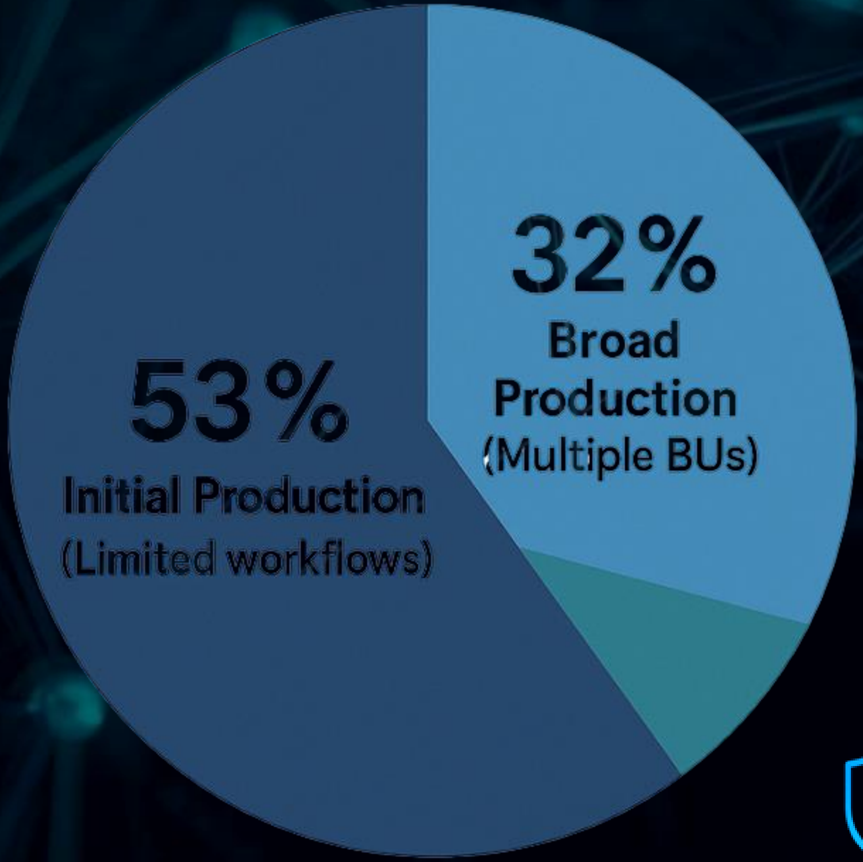


There will soon be a "Big Race" for AI adoption.

- ✓ Of the 85% of organizatons that have AI in production, only 32% have reached broad production.
- ✓ 68% of the total organizations are either in initial production or still in the exploration and piloting stage.
- ✓ Discussions have shifted from *"Shall we try AI?"* to *"How do we scale, govern and secure?"*
- ✓ As a result, security and compliance operations are now working to catch up with decisions that have already been made.

What stage of AI Adoption is your company currently in?

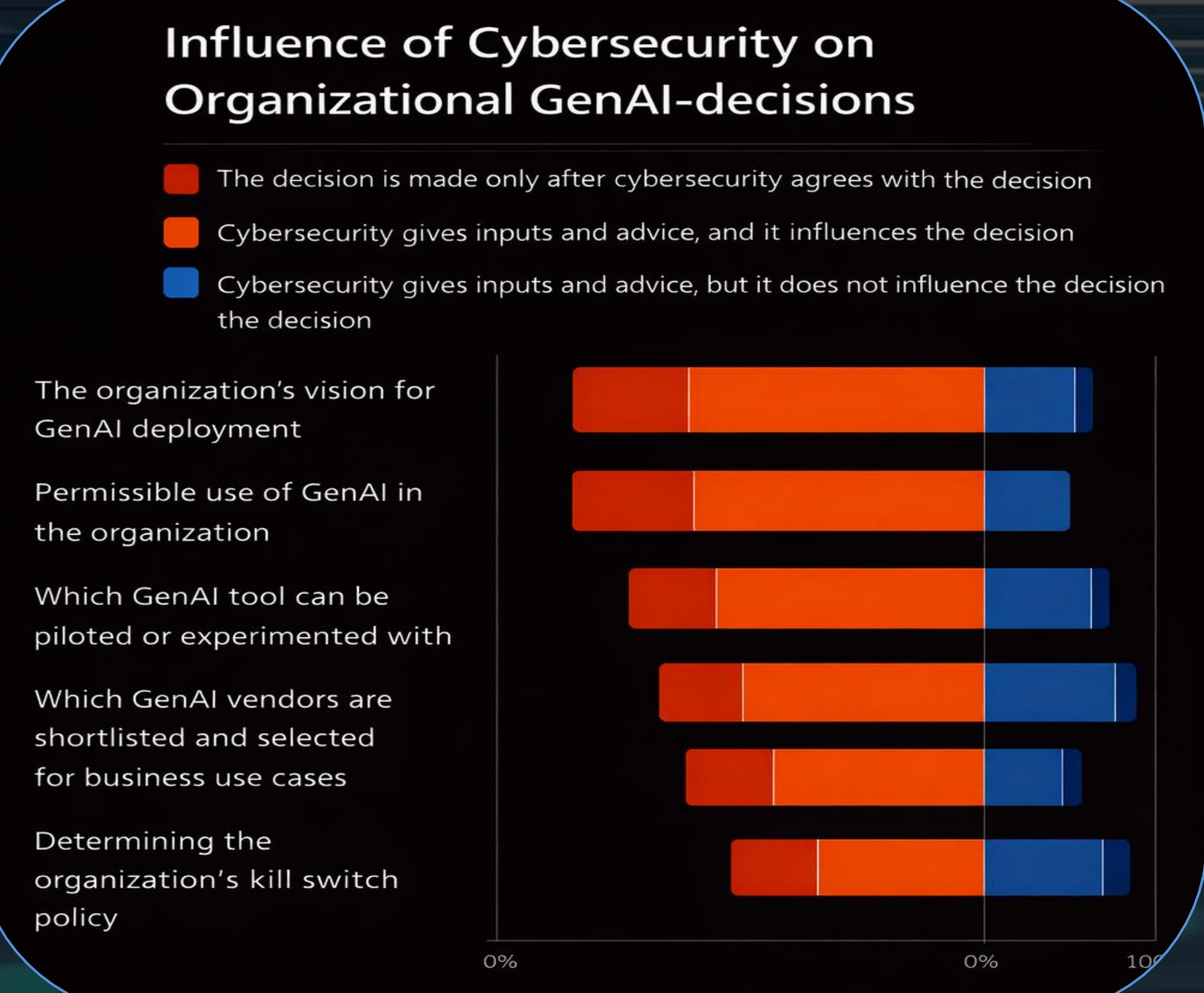
85% in Production



CISO CONNECT

Influence of Cybersecurity on Organizational AI Decisions

CISO CONNECT
An Exclusive CISO Platform



In nearly all GenAI-related decision areas, security teams provide input that influences outcomes.

- ✓ However, most decisions are still led by business and innovation teams — meaning security is consulted, but often reacts to decisions rather than shaping them proactively, and typically becomes involved later in the process than ideal.
- ✓ This dynamic introduces significant organizational risks and reinforces the need for earlier and closer collaboration between innovation, business, and security teams to ensure successful and safe GenAI initiatives.

CISO CONNECT
An Exclusive CISO Platform

Evolving Role of CISOs

CISOs now focus on enabling secure AI environments. They facilitate collaboration between security and innovation.

Despite the barriers, businesses are highly eager to accelerate company-wide AI adoption — at times underestimating the magnitude of the risks involved.

In this environment, it is impossible for CISOs to act as road blockers; they must operate as strategic enablers.

This requires managing regulatory compliance risks, addressing emerging AI-driven threats, and helping their organizations scale AI implementations rapidly and safely.

Gatekeeper → Enabler

BARRIERS TO AI ADOPTION

CISO CONNECT
An Exclusive CISO Platform

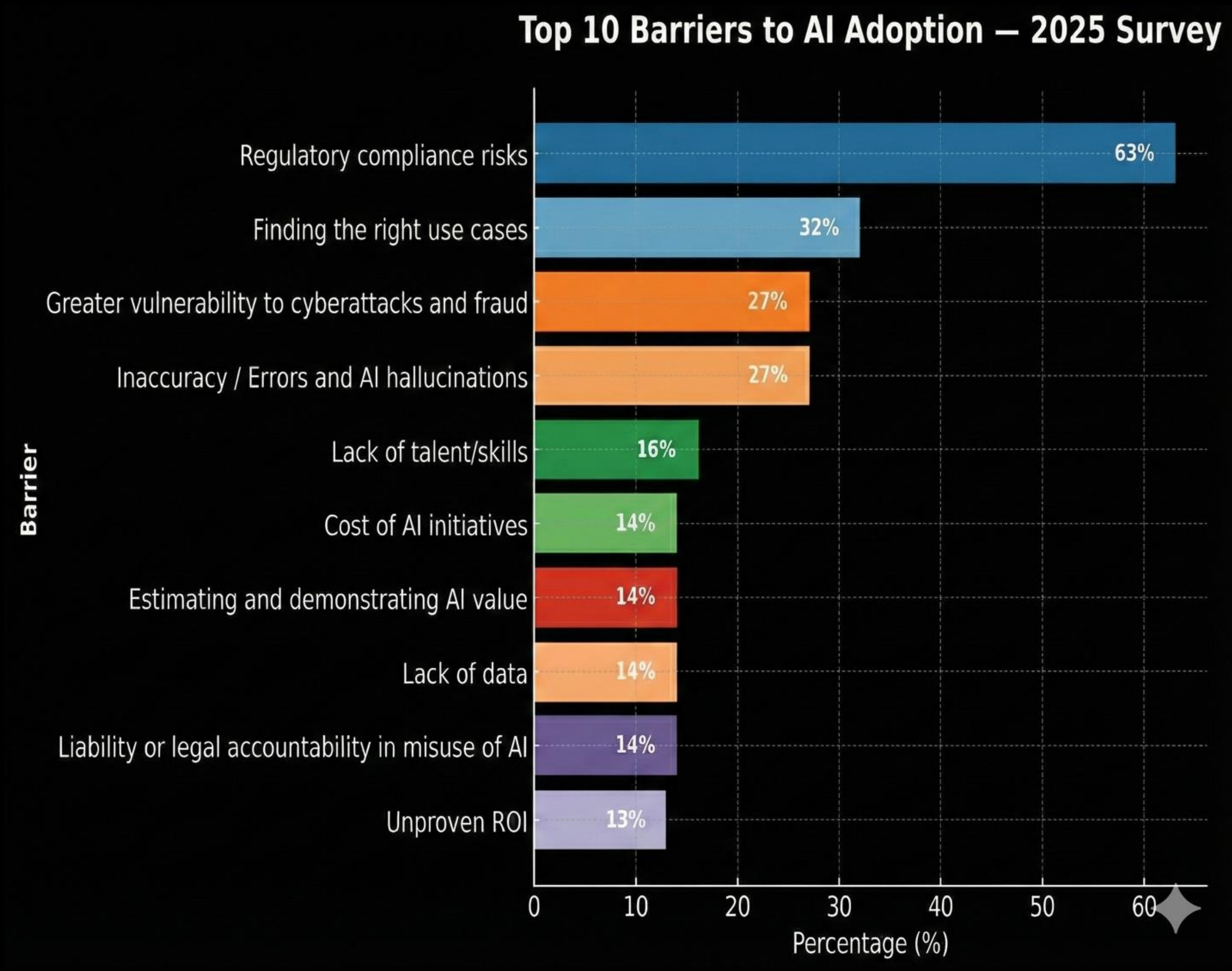
But still there are barriers to AI Adoption Race more from more from organizational and especially regulatory constraints.

As AI moves from experimentation into real-world deployment, uncertainty around compliance, governance, and accountability is creating caution across many enterprises— slowing rollout even where business appetite for AI is high.

REGULATORY COMPLIANCE is the #1 Brake on AI

- **Regulatory compliance risks** are the top barrier to adoption, well ahead of all others.
- This isn't only about laws; it's also about uncertainty: evolving AI regulations, sector-specific rules, data residency, and auditability.
- **Security and compliance teams must become design partners** for AI, not just auditors at the very end.

CISO CONNECT



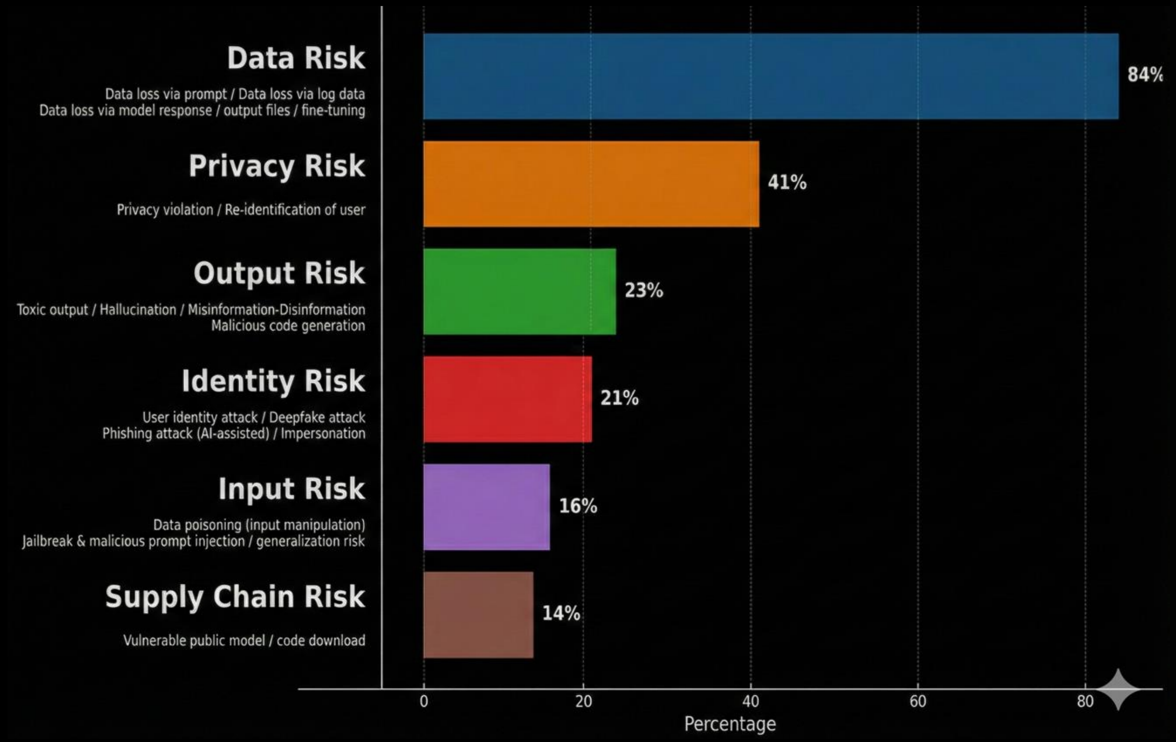
AI RISKS &THREATS

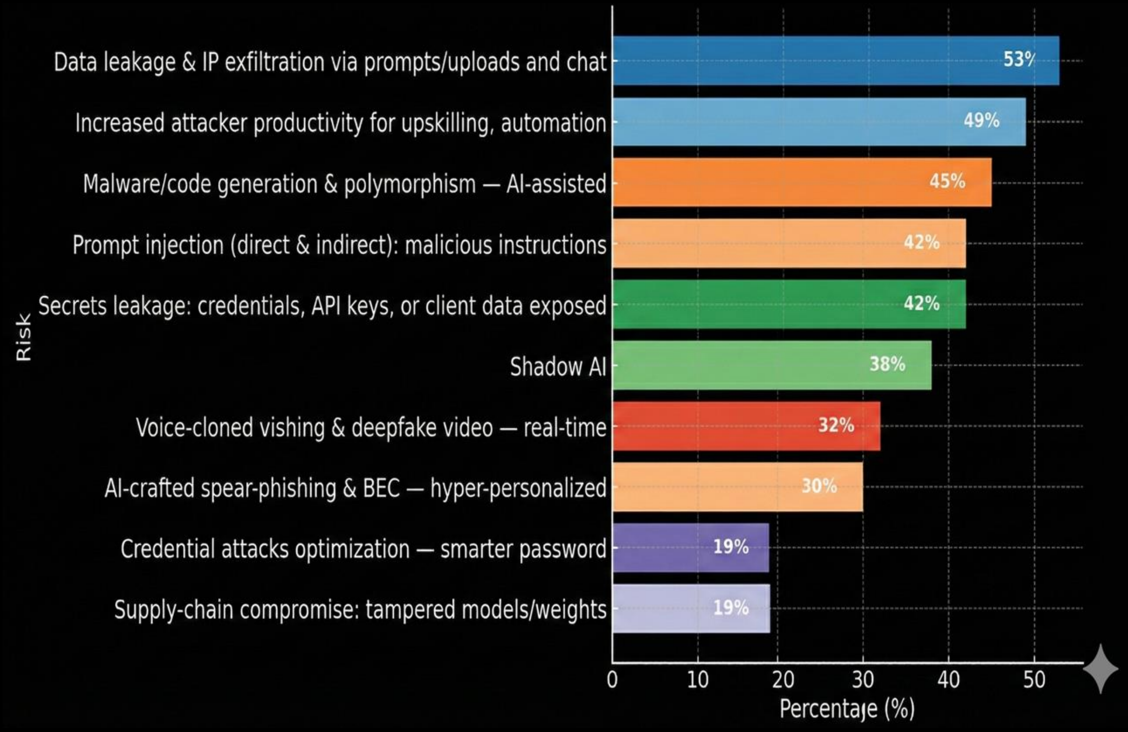
CISO CONNECT
An Exclusive CISO Platform

According to the Survey, AI-specific threat concerns are coming right behind regulatory risks with increased vulnerability to cyberattacks and fraud (27%), plus errors and hallucinations (27%)

- ✓ AI risks and threats are scaling faster than most organizations' ability to respond. The danger is less about a single catastrophic event and more about a **continuous stream** of smarter, cheaper, harder-to-detect attacks that exploit every gap in controls, policies, and human awareness.
- ✓ In this environment, the fastest path to adoption is pairing innovation with controls by design: clear policy + risk assessment, strong data protection, model/output guardrails, and continuous monitoring—so teams can move fast without stepping into regulatory or threat landmines.
- ✓ **Close collaboration between business and security** is critical — security must be embedded early into AI initiatives so organizations can innovate quickly while staying resilient against fast-emerging risks.

What are the most critical Gen AI based Risks by Group?





Data Risks the Dominant Anxiety Around GenAI

- “When we group risks, one theme towers above the others: DATA.
- CISOs are especially worried about sensitive data leaking through prompts, logs, outputs and about privacy and re-identification.
- Privacy, re-identification, and confidential data exposure are seen as far more dangerous than model quality issues.
- This supports the importance of AI data governance, classification, and AI-aware DLP as the foundation for any GenAI program.

CISO CONNECT

Navigating Emerging Risks & Threats in AI

DATA LEAKAGE THROUGH AI

Data leakage through AI occurs when sensitive information is unintentionally exposed via prompts, model outputs, logs, or integrations—often resulting from misconfigured settings or ungoverned usage—creating serious privacy, compliance, and confidentiality risks for organizations.

AI-AUGMENTED ATTACKS

AI-augmented attacks utilize advanced algorithms to create **more sophisticated** threats, making it easier for malicious actors to exploit vulnerabilities and execute large-scale cyber operations.

SHADOW AI

Unauthorized AI tools used within organizations potentially expose sensitive data and escalating security risks, highlighting the need for comprehensive governance and oversight.

DEEPFAKE

Deepfake threats involve the use of AI-generated audio, video, or images to impersonate trusted individuals, enabling highly convincing social-engineering attacks, financial fraud, and unauthorized access attempts that bypass traditional verification methods.

THIRD-PARTY AI RISKS

Third-party AI risks arise from reliance on external models, APIs, and open-source components, where vulnerabilities, misconfigurations, or compromised dependencies can expose organizations to data leakage, model tampering, and supply-chain attacks beyond their direct control.

Understanding AI Data Risks

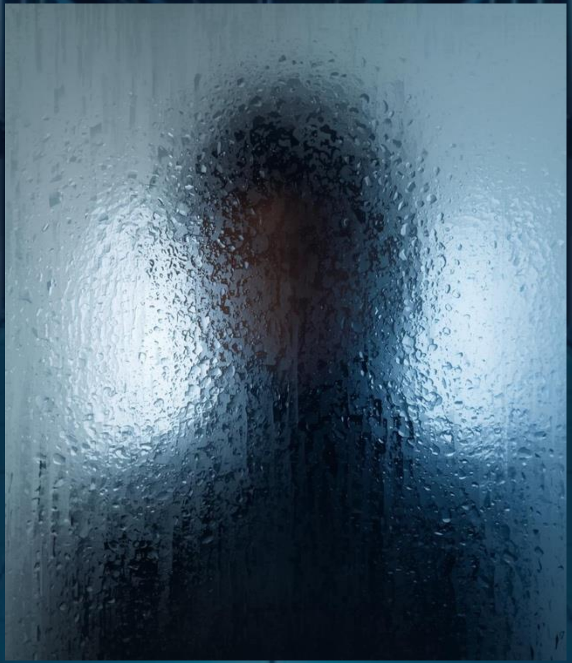
CISO CONNECT

Leakage

Exposure of sensitive data to unauthorized parties

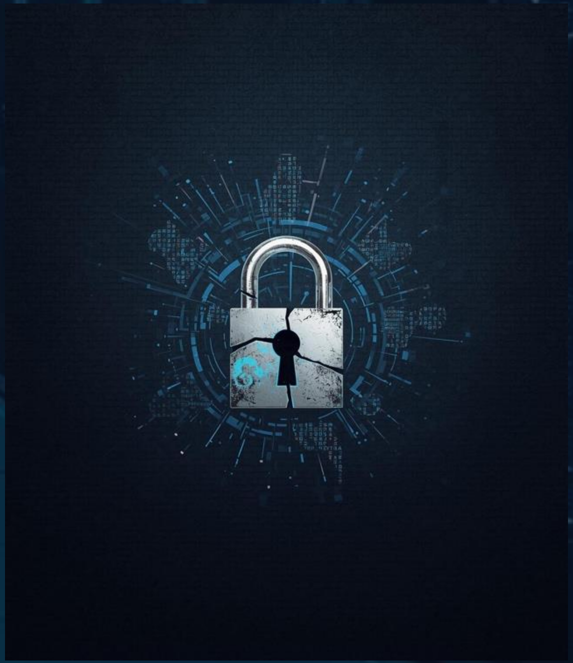
Privacy

Breach of personal information leading to misuse



Vulnerability

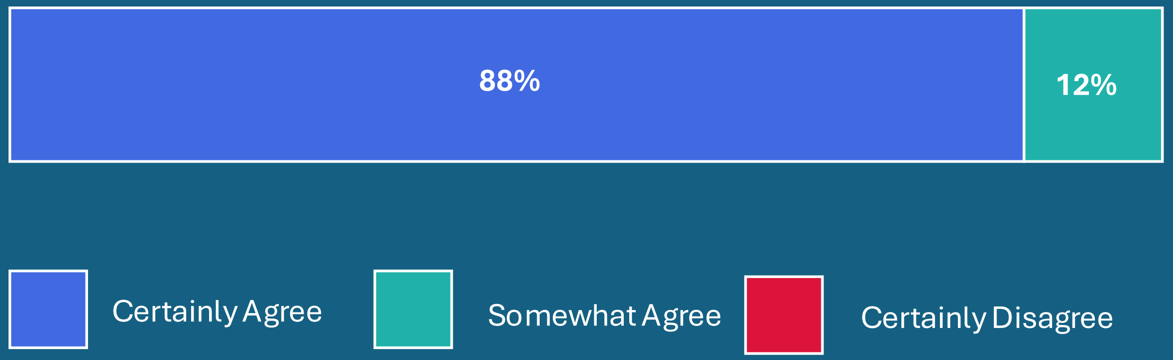
Increased risk from unprotected data channels



Top Risks & Threats

Misconfigured Data Pipelines is big risk

Adversaries increasingly exploit misconfigured data pipelines to exfiltrate sensitive data, as compromising an entire pipeline yields greater returns than attacking runtime transactions.



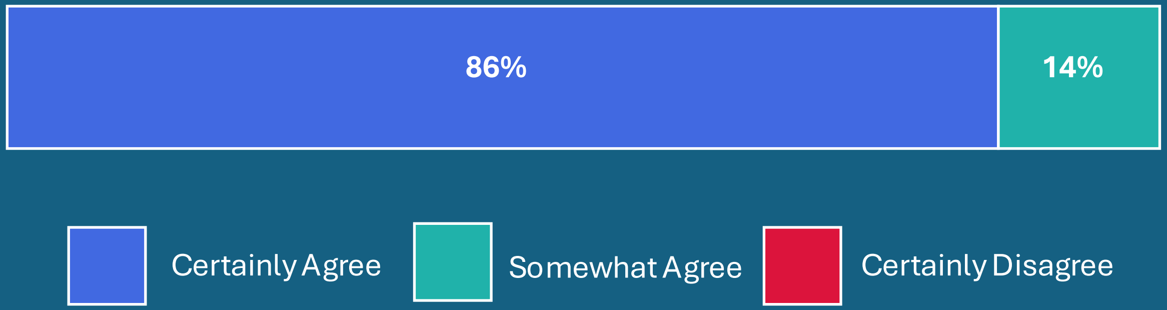
- **Data pipelines have become one of the highest-value targets** for adversaries.
- Pipelines are often **built fast by data and engineering teams** to enable analytics and AI – security and governance arrive late.
- They rely heavily on **cloud services, connectors, secrets, and permissions**, and a single misconfiguration can expose entire datasets.
- If Attackers compromise that “pipeline layer,” they can exfiltrate **huge volumes of sensitive data in one go**, often with better stealth and higher ROI than going after front-end apps.

Top Risks & Threats

AI Supercharges Existing Attacks

- This is not about totally new, exotic attack types. It's about **making old attacks much faster, smarter, and cheaper**.
- Attackers can upskill rapidly using AI, closing the gap with more sophisticated adversaries.
- The net effect: **the gap between low-skill and high-skill attackers shrinks**.

AI-driven agents will very soon automate credential theft and compromise authentication communication channels, significantly shortening the time it takes attackers to exploit exposed accounts.

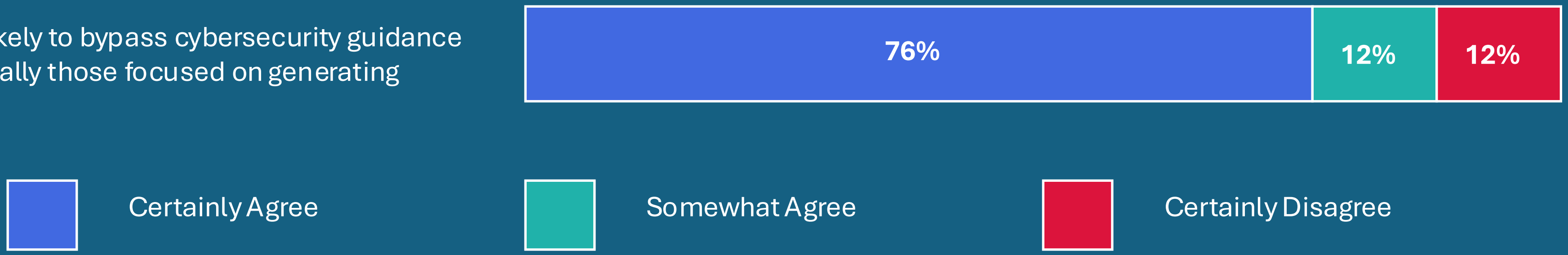


Top Risks & Threats

Human Bypass and Shadow AI Are Inevitable — Guardrails Must Be Built-In

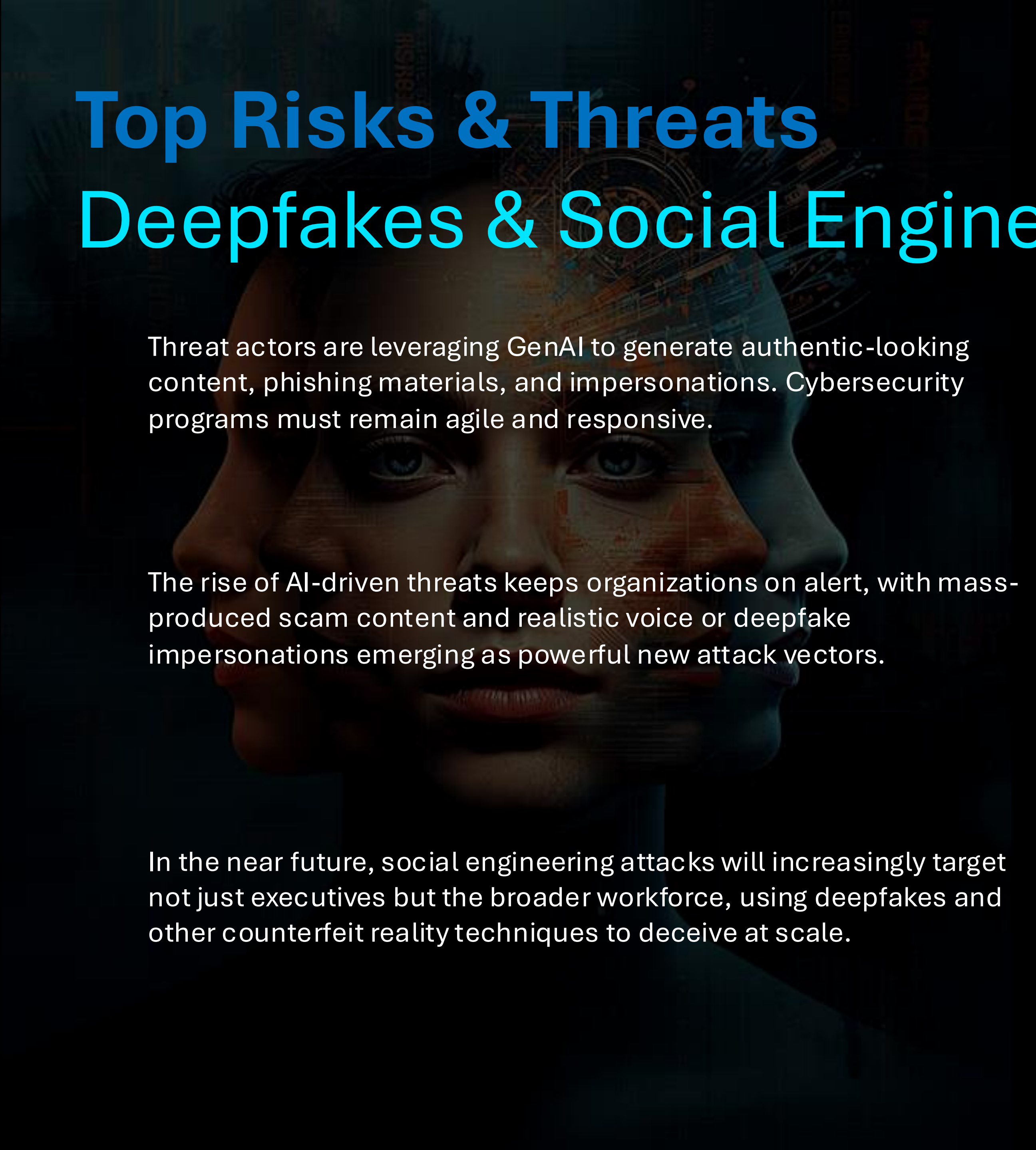
- Business technologists under time pressure will bypass security guidance. *"If using GenAI securely is harder than using it unsafely, people will choose unsafe by default."*
- Unapproved tools for content and code creation create visibility and compliance blind spots.
- This means traditional "policy on paper" will not be enough; safeguards need to be embedded into the tools people actually use.

Almost all of business technologists are likely to bypass cybersecurity guidance to meet pressing business goals — especially those focused on generating content or writing code.



Top Risks & Threats

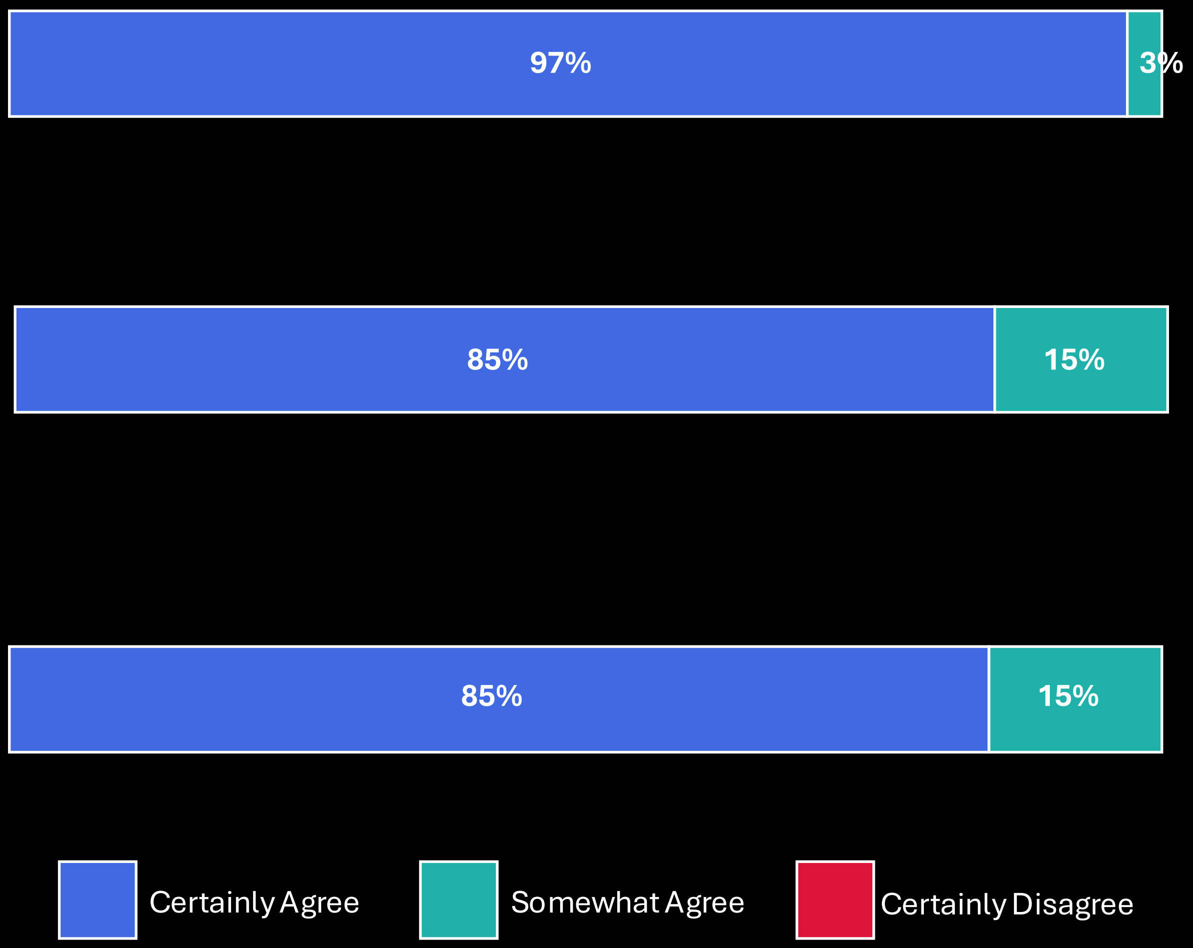
Deepfakes & Social Engineering



Threat actors are leveraging GenAI to generate authentic-looking content, phishing materials, and impersonations. Cybersecurity programs must remain agile and responsive.

The rise of AI-driven threats keeps organizations on alert, with mass-produced scam content and realistic voice or deepfake impersonations emerging as powerful new attack vectors.

In the near future, social engineering attacks will increasingly target not just executives but the broader workforce, using deepfakes and other counterfeit reality techniques to deceive at scale.



Top Risks & Threats
Deepfakes & Social Engineering

“Deepfakes Turn Old Tricks Into New-Generation Scams”

- “Scam Content Is Now Mass-Produced and Multi-Modal”
- “We’re not facing ‘better spam’; we’re facing industrial-grade impersonation at the click of a button.”

“Social Engineering Risk Extends Beyond the C-Suite”

- Anyone who can approve a payment, reset a password, or access sensitive data—whether they’re in Finance, HR, Support, Procurement, the IT helpdesk, or even a junior role—is now a high-value target, regardless of their title.”

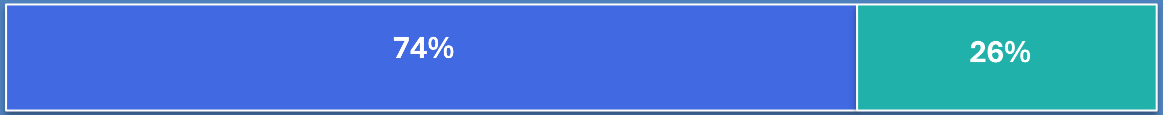
“Seeing and Hearing Are No Longer Proof”

- *Visual and audio trust anchors are broken*.
- The organizations need verification processes that don’t depend solely on what we see or hear.

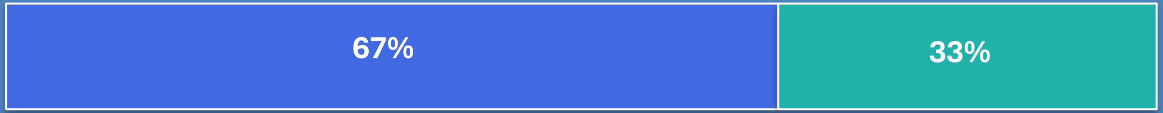
Top Risks & Threats

Third-Party Risks

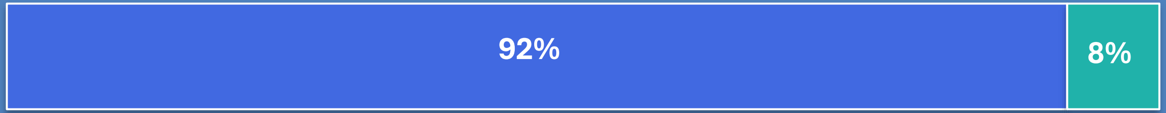
Unless going after a specific target, attackers commonly exploit weaknesses in AI supply chains and cloud infrastructures, as these yield high-impact results with the least effort.



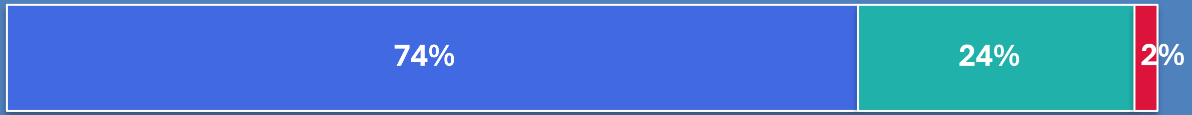
In the coming years, most malicious attacks against enterprise AI will stem from poisoning of software supply chains and core infrastructure technology stacks.



As vendors race to launch new features, many rely on third-party LLMs, APIs, and external libraries. This growing dependence introduces privacy concerns and third-party risk management challenges.



Open-source models and data science software are new AI attack vectors being targeted.



🟦 Certainly Agree 🟩 Somewhat Agree 🟥 Certainly Disagree

AI Supply Chain and Infrastructure Attacks

The increasing reliance on third-party vendors introduces substantial risks, amplifying potential exploits and vulnerabilities in supply chains and affecting overall security posture. Addressing these risks is crucial for organizational integrity.

Many future attacks on enterprise AI are expected to come from poisoned models, libraries, and infrastructure stacks—making software supply-chain security and model integrity central concerns.

CISO CONNECT

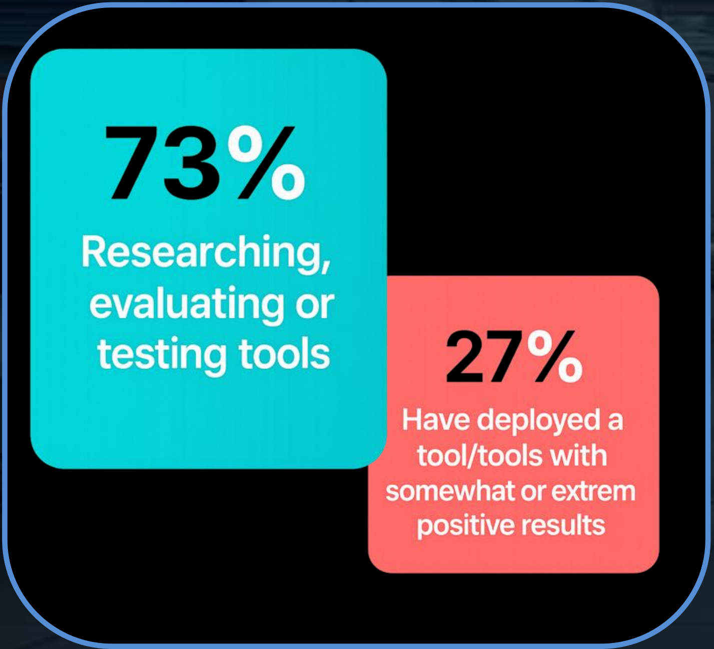
CISO CONNECT

THE ADOPTION OF AI SECURITY PRODUCTS

The immaturity of GenAI in security is a concern — but experimentation remains essential to keep pace with rapidly evolving AI threats.

THE ADOPTION OF AI SECURITY PRODUCTS

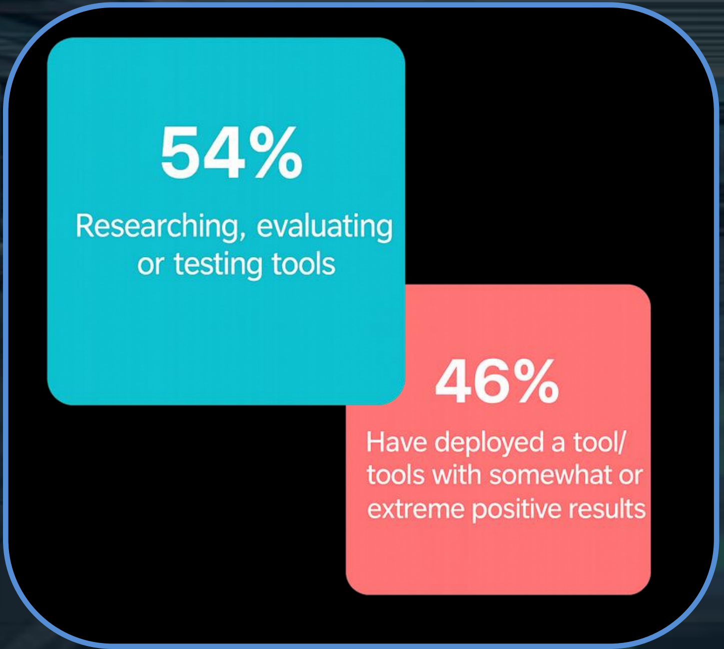
SECURING AI



73%
Researching, evaluating or testing tools

27%
Have deployed a tool/tools with somewhat or extrem positive results

SECURING WITH AI



54%
Researching, evaluating or testing tools

46%
Have deployed a tool/ tools with somewhat or extreme positive results

Even though many AI security products are still immature, CISOs are moving ahead.

- ✓ Most are actively researching and testing tools, while a smaller but meaningful share have already deployed solutions with positive results.
- ✓ As businesses push for rapid AI adoption, cybersecurity teams no longer have the luxury of waiting for the market to fully mature.
- ✓ Not only the business opportunities but also the risks are significant, and AI-driven threats are evolving too quickly to justify a wait-and-see approach.

AI in SECURITY

Security and risk management leaders remain cautiously optimistic about the potential of GenAI, as only a small percentage are currently achieving measurable results.

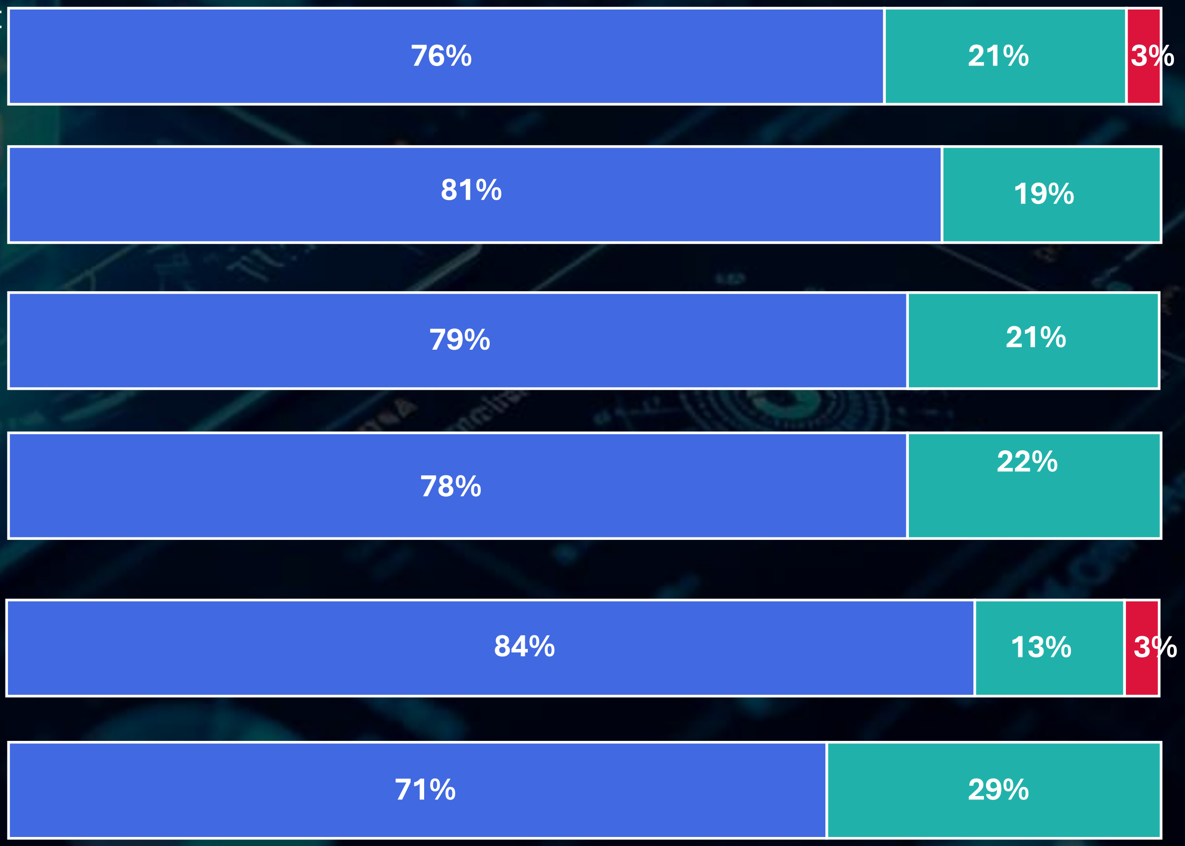
GenAI hype in security offers potential benefits yet risks wasted effort and disillusionment.

Organizations still struggle to align AI outcomes with tangible business goals, highlighting a need for clearer success metrics.

Almost all of successful AI initiatives in cybersecurity will remain tactical — centered on task automation and process augmentation — rather than full role replacement.

Despite significant investment and progress, GenAI's ability to orchestrate complex, agentic workflows remains immature, with key limitations still unresolved.

Organizations will need to aim for 'good enough' and focus on basic skill augmentation in the near term, as early implementations of generative cybersecurity AI have shown mixed output quality.



🟦 Certainly Agree 🟩 Somewhat Agree 🟥 Certainly Disagree

CISO CONNECT

Hype Is High, Outcomes Are Mixed

GenAI is still **struggling to manage** complex operations effectively.

Challenges in AI Workflow integration

- There is broad recognition of a **hype wave** around GenAI in security. Many organizations have invested significantly, but only a minority report **consistently measurable, production-level results**.
- Complex, multi-step “agentic” workflows are considered immature and fragile.
- Early implementations show inconsistent output quality and require close human supervision.
- Most successful initiatives so far are **tactical and narrow**, focused on specific tasks.

AI Augments People, Can’t Replace Them...Yet...

- Successful AI initiatives focus on task automation and augmentation, not full role replacement.
- GenAI is best positioned as a skilled assistant: drafting, summarizing, correlating, and recommending, rather than expecting fully autonomous security decision-making.
- This reduces resistance from teams and clarifies where human accountability lives.

AI Benefits in Security

Expectations are high – the benefits are not fully matching but advancing rapidly.

CISO CONNECT

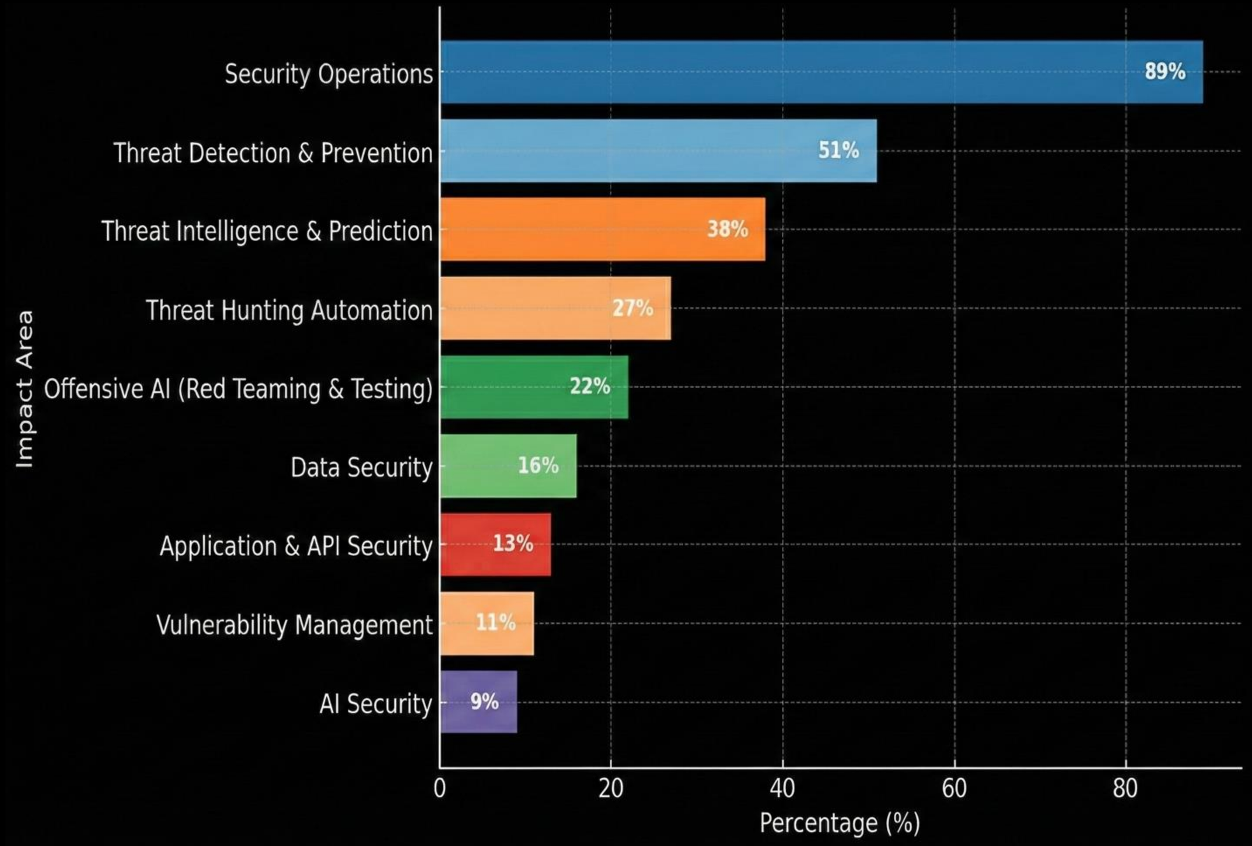
INSIGHTS AND BENEFITS

CISO CONNECT

Security Operations is the First Big Winner From AI

- Respondents consistently point to Security Operations as the area where AI will create the most value.
- Key benefits they see are faster incident handling, fewer false positives, and richer, more scalable threat hunting.
- *“AI changes the economics of the SOC — more signal, less noise, with similar or even fewer people.”*

In which areas of security will AI security tools have the most impact?

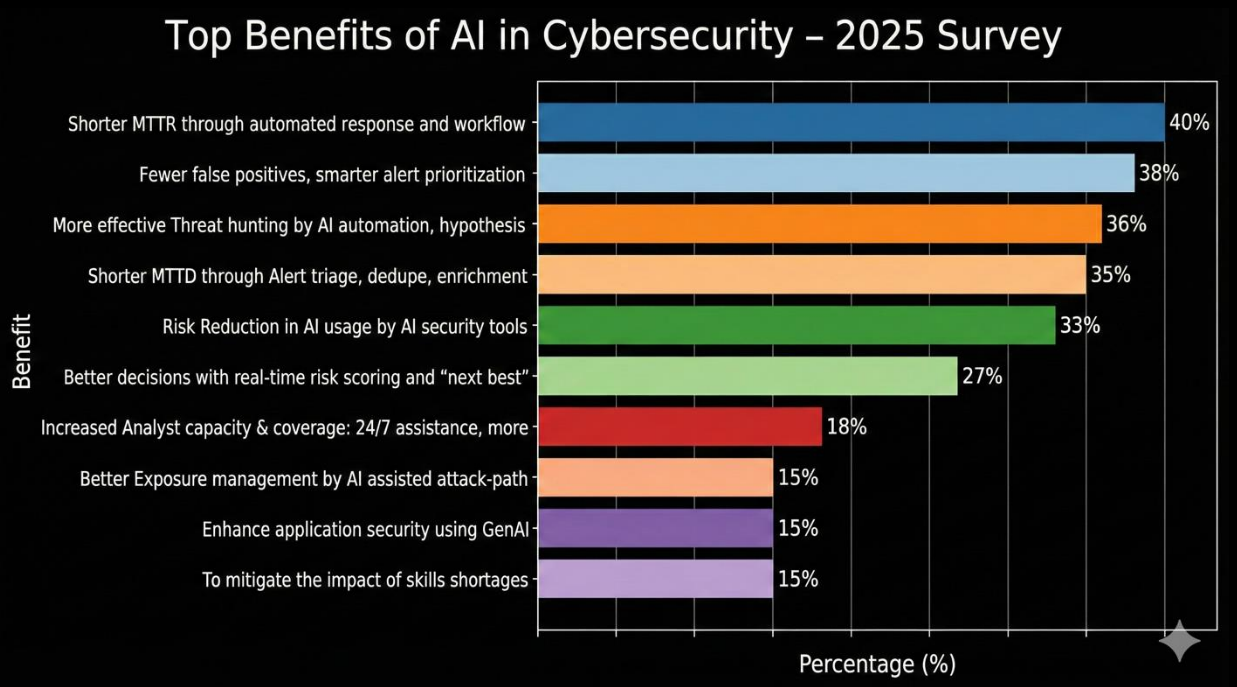


Expectations from AI in Security

Faster, Smarter Incident Handling

- Top expected benefits: shorter MTTR via automated response & workflow, fewer false positives with smarter alert prioritization, and more effective threat hunting
- Benefits such as coverage/24×7 assistance, exposure management, and skills-shortage mitigation are there, but secondary.

Top Ten Benefits of AI adoption in Security

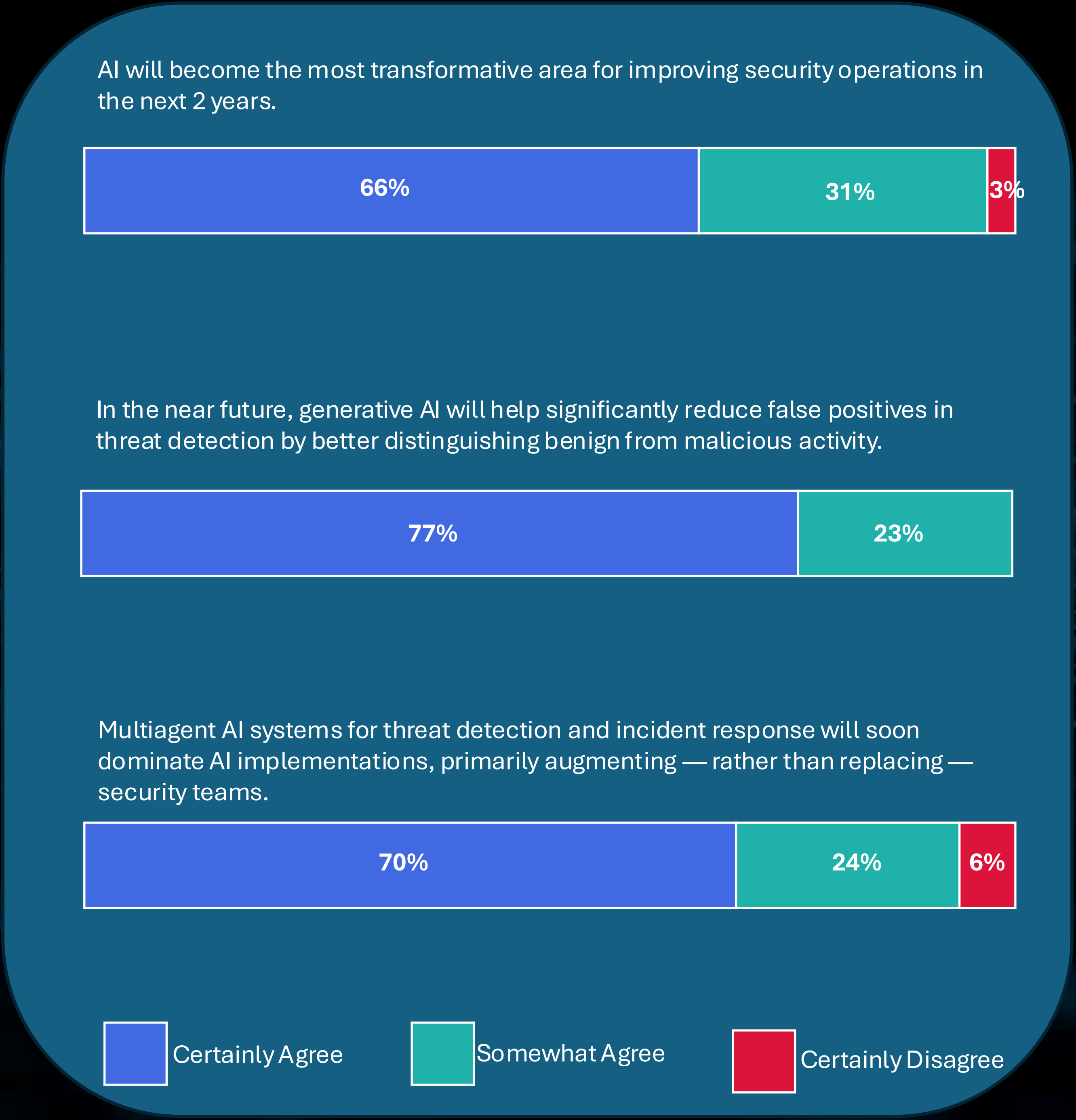


Future SOC Vision

Despite the Hype and the Mixed Outcomes, Security Operations remain the Primary Beneficiary of AI.

SOC of the Future:

SOC Is the Primary Beneficiary of AI



AI will become the most transformative area for improving security operations in the next 2 years.

In the near future, generative AI will help significantly reduce false positives in threat detection by better distinguishing benign from malicious activity.

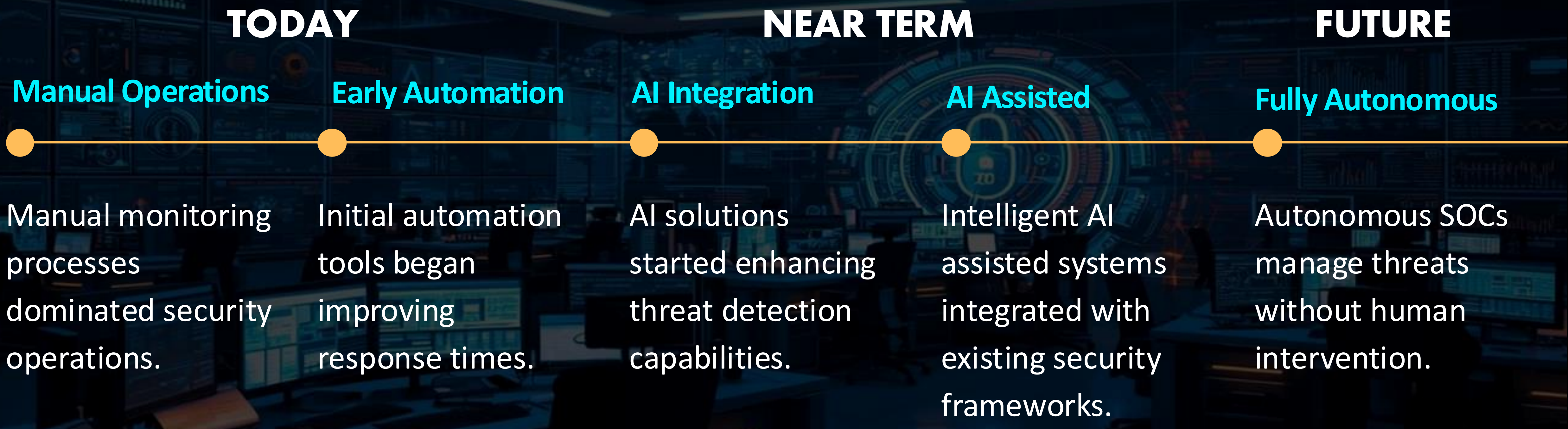
Multiagent AI systems for threat detection and incident response will soon dominate AI implementations, primarily augmenting — rather than replacing — security teams.

Timeline

Today → “Manual heavy”
Near Term → “AI-assisted”
Future SOC → “AI-native”

- AI is seen as a way to **change the economics of the SOC**: more coverage and higher quality decisions without requiring linear increases in headcount. This is where organizations expect the most tangible value in the near term.
- **Multi-agent AI systems** for detection and incident response are expected to **augment, not replace**, security teams.

SOC Evolution Timeline



TODAY

NEAR TERM

FUTURE

Manual Operations

Manual monitoring processes dominated security operations.

Early Automation

Initial automation tools began improving response times.

AI Integration

AI solutions started enhancing threat detection capabilities.

AI Assisted

Intelligent AI assisted systems integrated with existing security frameworks.

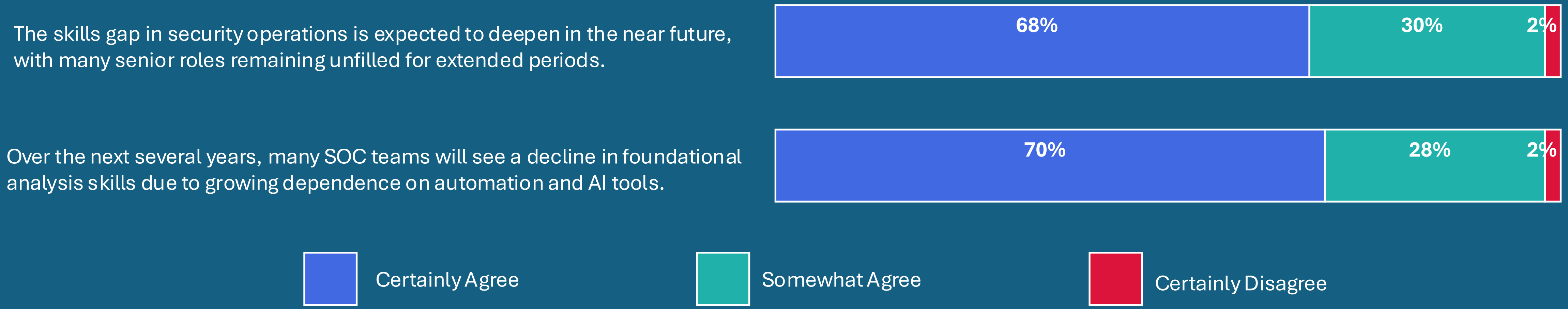
Fully Autonomous

Autonomous SOCs manage threats without human intervention.

SOC of the Future:

AI-Augmented SOC With a Skills Dilemma

- Security teams broadly believe AI will transform SOC performance, but at the same time, leaders worry that over-reliance on automation will deepen skills gaps and erode foundational analysis capabilities if not managed carefully.
- Training and career paths must preserve and grow foundational analysis skills“Protect skills at each stage”.
- AI must be used to *train* better analysts, not to deskill them.
- So the challenge is to invest in AI while also intentionally investing in people.



The skills gap in security operations is expected to deepen in the near future, with many senior roles remaining unfilled for extended periods.

Over the next several years, many SOC teams will see a decline in foundational analysis skills due to growing dependence on automation and AI tools.

CISO CONNECT

Strategic Implications for Security Leaders

"This is not simply a technology shift; it is a structural change in how organizations make decisions, manage risk, and run security operations."

Taken together, the survey points to a clear agenda for CISOs:

- **Lead with business-aligned use cases**, not tools.
- **Elevate data governance** as the cornerstone of safe AI.
- **Invest in SOC-focused AI** where value is most immediate.
- **Build trustworthy AI platforms** that integrate security, compliance, and observability by design.
- **Design for human reality**—shadow AI, skill gaps, and bypass behavior are facts, not edge cases.
- Pair every AI investment with a **talent and skills plan**.

"AI is the future"

Secure Your AI Future

CISO CONNECT
An Exclusive CISO Platform

For your valuable contributions pleaese contact:
gokhan@cybridge.tech