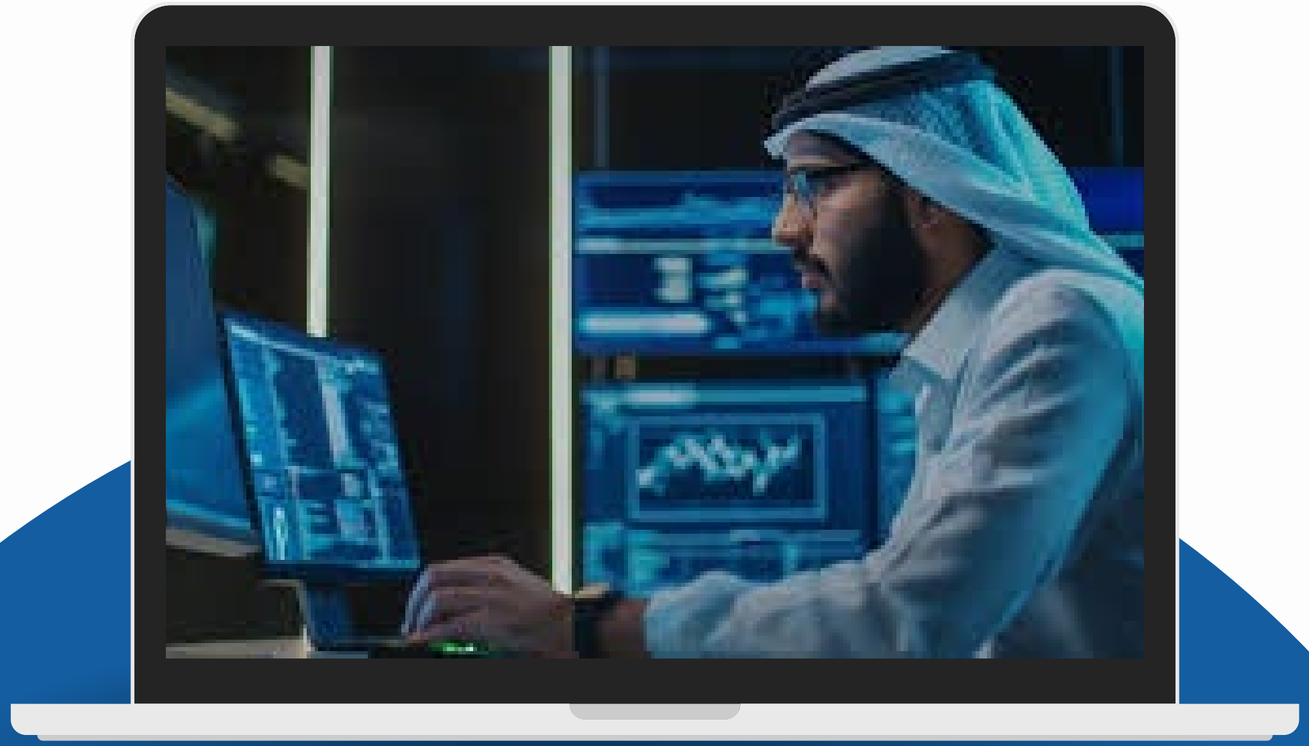
SHIELD AI

Generative AI Challenges:

Data Leaks, Shadow AI and Regulatory Responses

OMAINTEG FM 2026 a Presentation

By: Mustapha Annouh, CEO SHIELD AI



FIRST : YOU

Q1: Do your Organization allow the use of GenAi ?

Q2: Do you know what happens to your data when you trust GenAI?

Overview

Introduction

Generative AI is transforming industries with unprecedented automation, innovation, and efficiency gains , but it also introduces critical risks such as data leaks, shadow AI usage, and evolving regulatory pressures. With enterprises reporting millions of sensitive records exposed through tools like Microsoft Copilot, and over 80% showing signs of unsanctioned AI adoption, the urgency to implement robust data governance, cybersecurity controls, and compliance frameworks has never been greater.

This presentation explores the challenges and opportunities of securing AI ecosystems, examining how regulatory responses, combined with proactive risk management and defense-in-depth strategies, can safeguard your organizations while enabling them to harness AI responsibly and competitively.

About us

SHIELD AI is a sovereign cybersecurity SaaS protecting organizations from the risks of Generative AI. Our platform delivers **real - time data leak prevention, anonymization, and AI governance** to safeguard sensitive information across finance, healthcare, energy, and government.

By auditing shadow AI, ensuring compliance with **ISO 27001, NIST, NSDAI, and the EU AI Act** and deploying our AI Shield Stack, we enable enterprises to innovate securely. Based in Europe but with International expansion, **we build trusted and resilient AI ecosystems** for our clients that transform regulation into advantage.

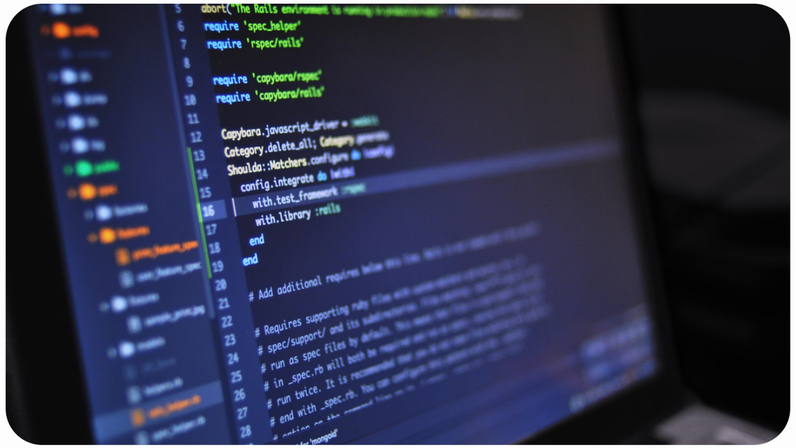
Company Overview

I am Mustapha Annouh, Co-Founder and **CEO of SHIELD AI**, with over 22 years of experience in **cybersecurity, governance, risk & compliance (GRC) and artificial intelligence**, leading transformative projects across defense, finance, energy, and international organizations.

The Generative AI Boom Market & Adoption

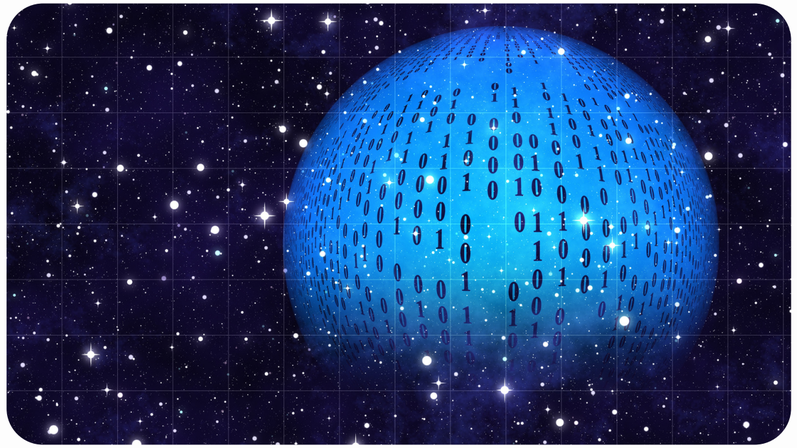
Market

- Ma rket projected to reach USD 66.62 B by 2025
- Gartner forecasts USD 644 B spending in 2025 (+ 76% vs 2024)



Revenu

51% of firms see revenue ↑ ⩾10%



ROI

ROI: $1 → ~3.7× return

78% of organizations increased GenAI spend in 2025

STATISTICS

The cost of cybersecurity incidents linked to Generative AI has skyrocketed in just a few years, moving from negligible levels in 2020 to tens of millions by 2024. This surge is exponential, driven by shadow AI, massive data leaks, and mounting regulatory enforcement.

Statistics

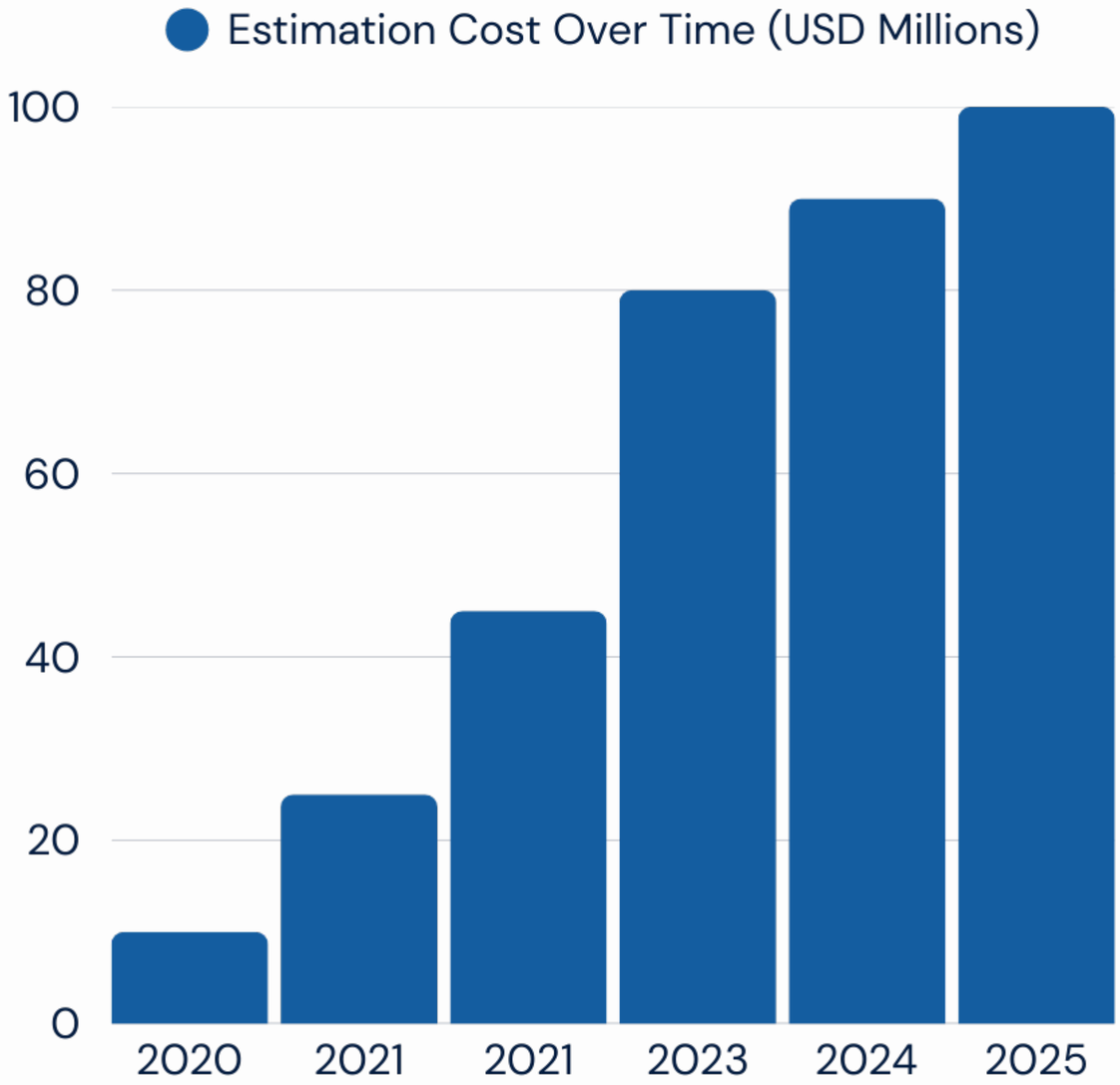
GenAI Risk Exposure is Accelerating

+300%
Sensitive data exposure

57%
Files with confidential info

80%
Shadow AI activity in orgs

+ $670k
Extra cost per breach



AI = New Challenges

01

Data Leaks & Exposure in GenAI

- Microsoft Copilot accessed ~3M sensitive records/org (H1 2025)
- 57% of shared files had sensitive data (up to 70% in some sectors)
- ~15% of employees pasted sensitive data into public LLMs
- ~40% of orgs report AI privacy incidents

02

Shadow AI The Invisible Threat

- Accounts for ~20% of breaches
- Breach cost premium: +$670K to $4.5M per incident
- Only 17% block confidential data uploads
- 98% of employees use unsanctioned apps
- 80%+ show signs of shadow AI activity

03

Attackers Use AI Too

- 16% of breaches involve AI-driven attacks
- 37% phishing, 35% deepfake impersonation
- AI reduces phishing creation from 16h → 5min
- 70–80% of Shadow AI traffic evades monitors

AI = New Opportunities

work
Level Taxonomy

vel Taxonomy provides a clear
rotect data in the GenAI era. It
n - Usability blocking risky data from
stems then ensures Privacy
through encryption and
n. Traceability brings visibility and
ross the AI lifecycle, while
uarantees full data removal when

se four levels transform AI from a
a trusted, accountable, and
stem.

Non -usability : block risky data

Privacy preservation : DP, masking, encryption

Traceability : lineage & audit

Deletability : ensure full removability

How to start ?

As Saudi Arabia advances its Vision 2030 and National Strategy for Data & AI (NSDAI), adopting AI securely is not just a technological choice but a national priority. Defining clear objectives for controlled, compliant, and trusted AI will be essential to safeguard sensitive sectors while positioning the Kingdom as a global leader in responsible innovation.

Objective 01: Secure Adoption

Ensure every AI deployment is protected from data leaks through anonymization, governance, and strict access controls, enabling safe integration across business functions.

Objective 02: Regulatory Alignment

Stay ahead of AI regulations and standards (EU AI Act, NIS2, GDPR, NSDAI, UAE AI 2031) by embedding compliance into every AI initiative from the start.

Objective 03: Trusted Innovation

Foster a culture where AI drives productivity and competitiveness while remaining transparent, auditable, and resilient against risks like Shadow AI and adversarial use.

SHIELD AI
THANK YOU!

Mustapha Annouh

CEO & CoFounder

+ 32 471 35 63 06

www.shieldai.ai

Brussels, Belgium

“I don’t know these people, but they seem nice!”

Our Team

Mustapha Annouh
Co-Founder
CEO / CIO

Primael Bruant
Co-Founder
CTO / COO

Our services

Proxy Mode Transparent "Fire - and - Forget" AI Audit	Extension Mode Intelligent Browser - Level Protection	Gateway Mode PI- First Data Protection
Ag entless drop - in Sits inline with outbound AI traffic to silently discover every AI/LLM (incl. Shadow AI) and mirror flows —no workflow change. **Real - time telemetry to AICP** Streams Indicators of Data Leak (PII/PHI/PCI, secrets, code, contracts, metadata) with user/app context and risk scoring. **Scheduled Audit P ack** After 30/60/90 days, Suveris delivers a signed audit pack per AI app: counts & severity of leaks, affected data classes, exfil paths, teams, trends, and sample evidence + remediation heatmap.	**Web Extension Installation** Browser extension installs seamlessly to identify and protect sensitive information using real - time data masking —no disruption to user workflows. **Real - time telemetry to AICP** Streams Indicators of Data Leak (PII/PHI/PCI, secrets, code, contracts, metadata) with user/app context and risk scoring. **AICA Compliance & Specialized Agents** AI Compliance Assistant (AICA) enables selection of compliance standards and deploys dedicated agents that discover specific data categories and risks.	**API Gateway Integration** Seamlessly integrate with your existing applications and services through our RESTful API gateway for automatic data protection. **Real - time Data Anonymization** Automatically detect and anonymize sensitive data in API calls before they reach public AI services, ensuring compliance and security. **Category Detection & Classification** Advanced ML models identify and categorize sensitive data types (PII, PHI, financial, secrets) with detailed reporting and analytics.