Kammil Mahajan

CEO, Advice Bytes & Sector8 AI

AI Security as Strategic Risk

IVI Summit 2026
20 Years of Impactful Research – What's Next?

Introduction

Kammil Mahajan

20+ years of IT and Cybersecurity at Google, Facebook, Quantcast & Maynooth University.

Entrepreneur & Founder
Lecturer, PhD researcher in AI Security

CISM Certified Information Security Manager

COBIT An ISACA® Framework

ATU Ollscoil Teicneolaíochta an Atlantaigh / Atlantic Technological University

UCD DUBLIN

SECTOR8

AIDVICE BYTES

Otals

instazap

Maynooth University
National University of Ireland Maynooth

Quantcast

Meta

Google

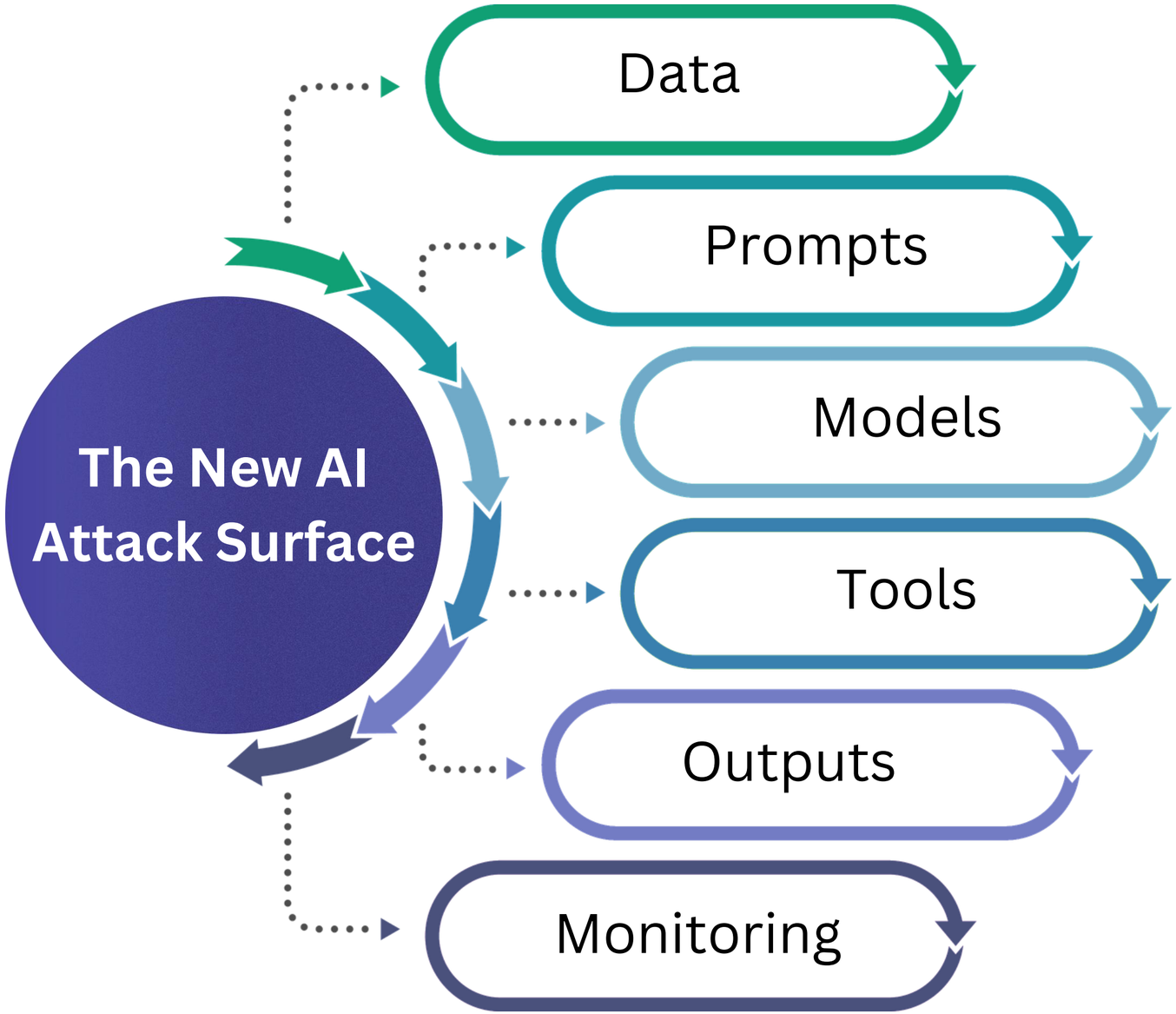
What changed in 2026

2024–25 was “people using ChatGPT

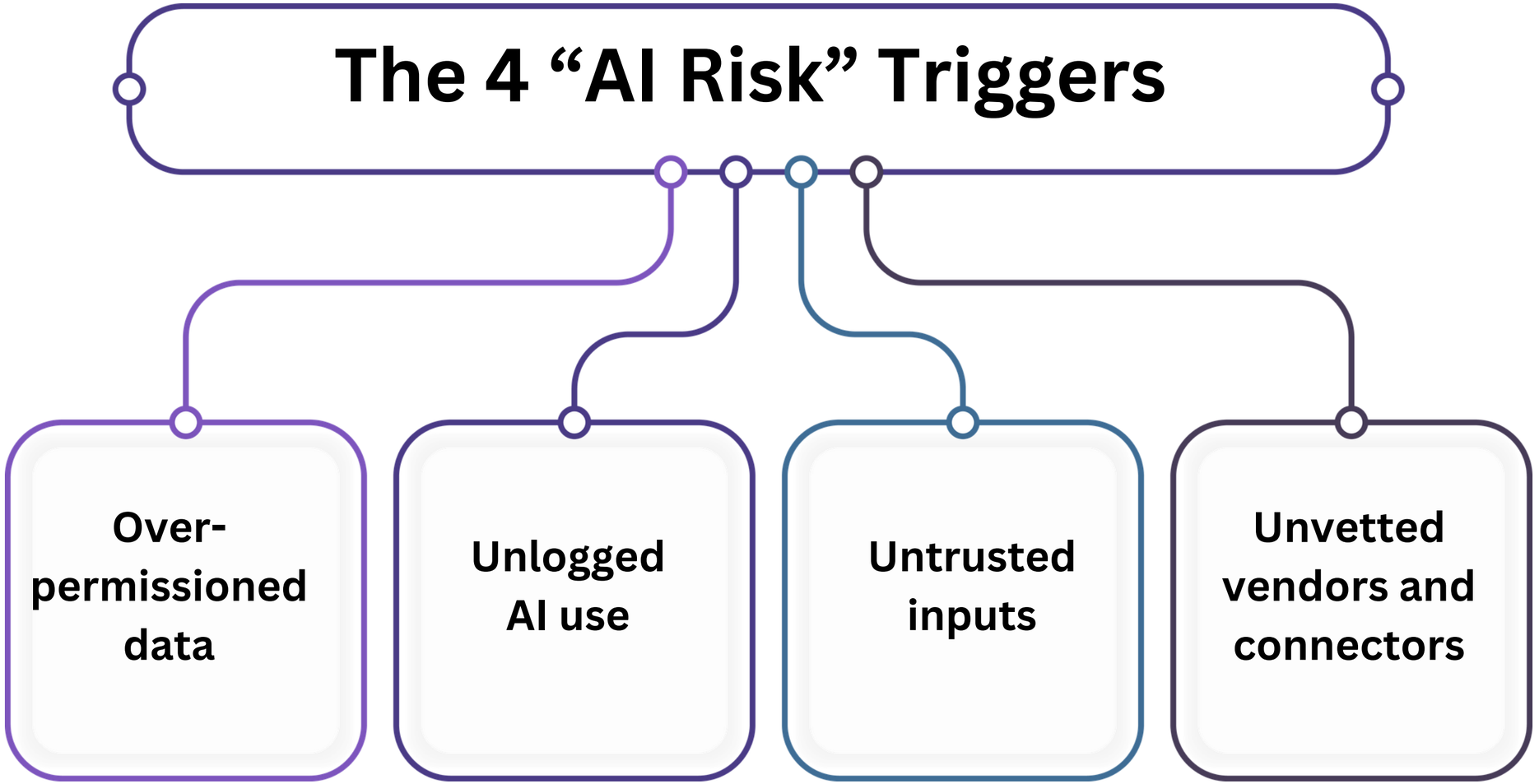
2026 is “AI plugged into tools” (email, CRM, ticketing, docs, finance ops).

AI Breaks Old Security Assumptions

OLD WORLD	NEW WORLD
Code is the attack surface	Data becomes the attack surface
Apps follow rules	Agents can take actions
Testing is periodic	AI changes continously

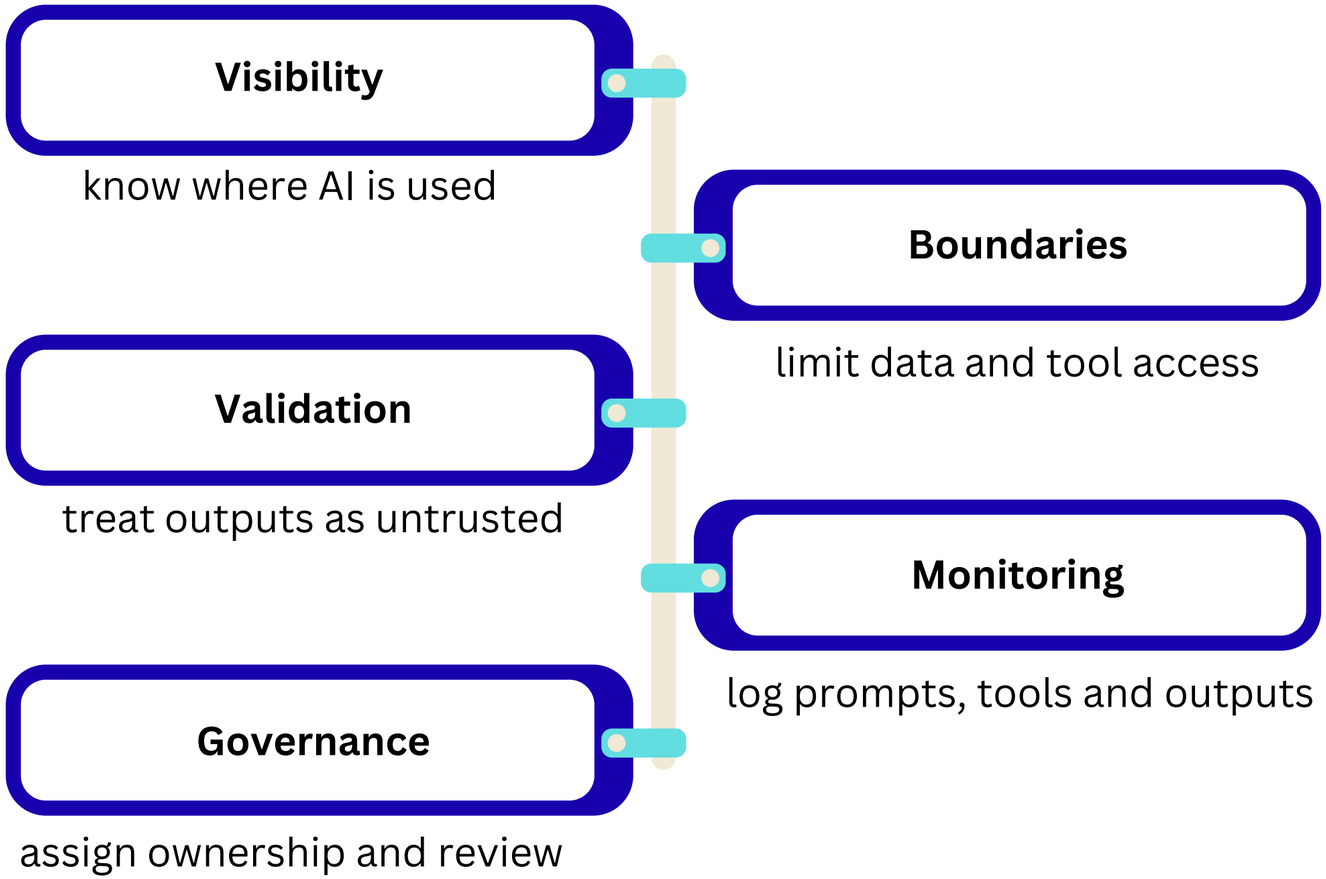

Data
Prompts
Models
Tools
Outputs
Monitoring
The New AI Attack Surface

The 4 “AI Risk” Triggers

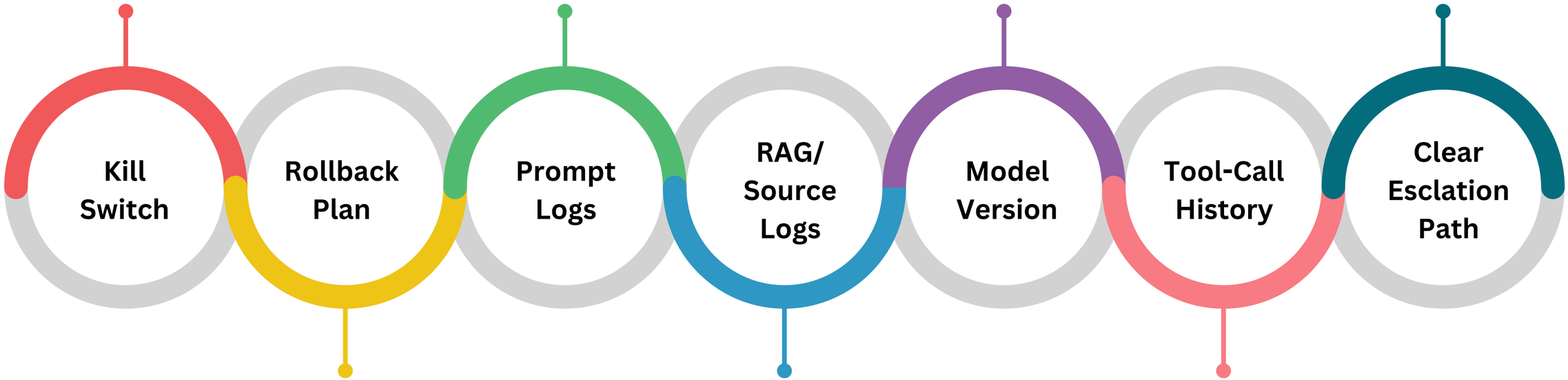


Why This Becomes Board-Level Risk

Controls That Actually Work



AI Incident Response Will Be Different



Three Questions to Leave With

Q1

Where is AI already being used?

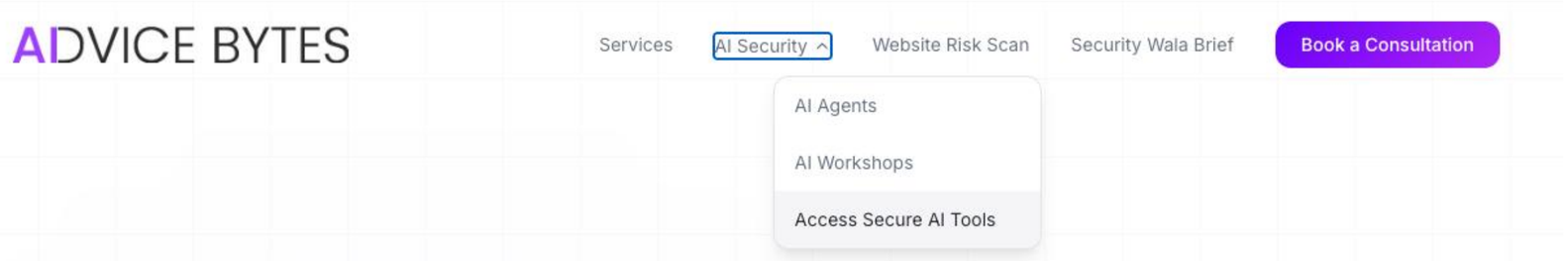
Q2

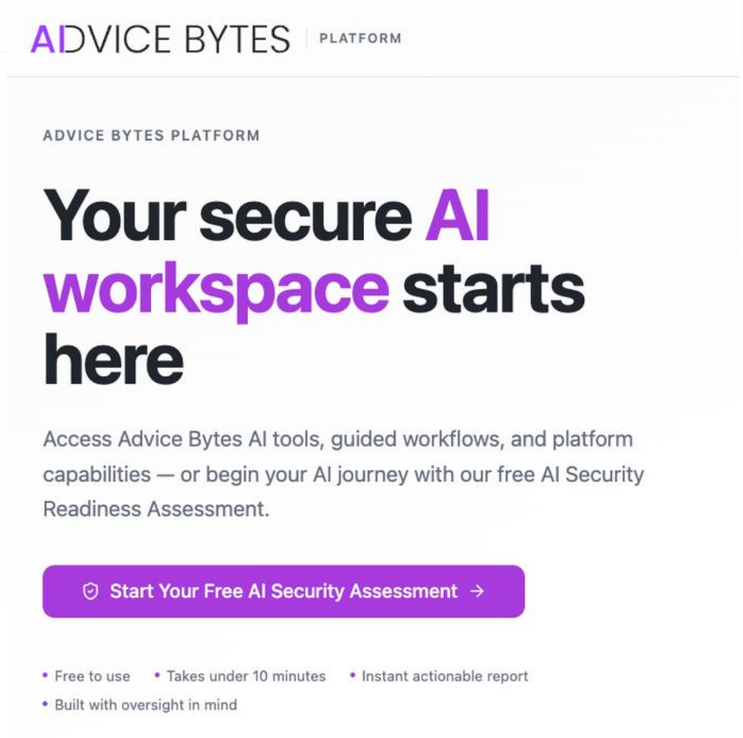
What data and tools can it access?

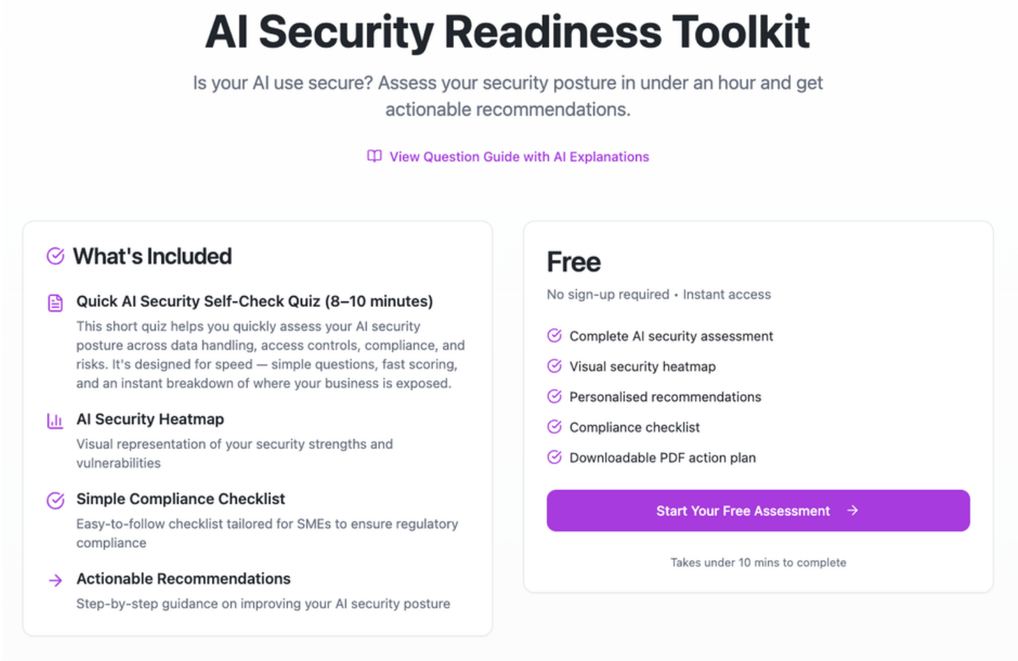
Q3

Who owns the risk when AI acts?

Start your AI Security journey today







ADVICE BYTES

SECURING TODAY.
FUTURE-PROOFING TOMORROW.

SECTOR8

SECURE THE INFINITE LOOP OF AI/ML

Kammil Mahajan He/Him

Helping SMEs adopt AI securely | Tech Strategist | Speaker | PhD Researcher - AI Security

AdviceBytes

Atlantic Technological University

Zero Trust: a simple, practical guide for leaders and teams

By Kamil Mahajan — Sector8 AI / Advice Bytes Executive Summary:...

by Kammil Mahajan · 4 min read

The CISO's role in the digital age: AI and cyber security

Executive summary AI changes how businesses make decisions and...

by Kammil Mahajan · 4 min read

AI Security in 2026: What to Watch & Lessons From a...

2025 will be remembered as the year the AI ecosystem grew up and brok...

by Kammil Mahajan · 7 min read

Securing AI Agents at Runtime — Why AI Security is Not...

Executive Summary AI has crossed a threshold. It's no longer a passive...

by Kammil Mahajan · 4 min read

Protecting Public Information: Practical Data Management f...

Author: Kammil Mahajan Organisation: Advice Bytes...

by Kammil Mahajan · 3 min read

Can We Trust the AI Agents Driving Our Sustainable Future?

By Kamil Mahajan PhD Researcher in AI Security | CEO, Advice Bytes...

by Kammil Mahajan · 3 min read

Why AI Security Is Dubai's Next Big Challenge

Dubai is rapidly positioning itself as a global leader in artificial intelligenc...

by Kammil Mahajan · 2 min read

Shadow AI: The Next Data Breach Waiting to Happen

How Unmonitored AI Usage is Creating Blind Spots in Enterprise...

by Kammil Mahajan · 3 min read

Top 3 AI Security Trends to Watch in 2025

As AI tools become more accessible, so do the opportunities for...

by Kammil Mahajan · 2 min read

What to Expect from an AI Security Audit

Artificial Intelligence (AI) is revolutionizing industries, offering...

by Kammil Mahajan · 2 min read

Clawdbot went viral and the security problems started...

What Clawdbot is (short) Clawdbot is an open-source personal assistant...

by Kammil Mahajan · 4 min read

What the EU AI Act Means for SMEs: A Practical Take

Executive Summary The EU AI Act marks the world's first...

by Kammil Mahajan · 5 min read

Agentic AI security: M&A wave and what it means for your...

Executive summary Vendor consolidation in agentic AI security ...

by Kammil Mahajan · 4 min read

Where to start with AI in your business: a practical step-by-...

One question I get in every AI security masterclass is simple: whe...

by Kammil Mahajan · 3 min read

Optimizing Business Processes with AI by 2030

Author: Kammil Mahajan, PhD Researcher – AI Security in SMEs...

by Kammil Mahajan · 3 min read

The Next Social Engineering Threat – When Automation...

In 2024 alone, the use of autonomous AI agents grew by ove...

by Kammil Mahajan · 3 min read

From Black Box to Secure Box

Making LLMs Safer, Transparent, and Auditable in the Enterprise Executiv...

by Kammil Mahajan · 2 min read

AI Security is the New Cybersecurity

Why LLMs, Agents, and AI Systems Need Dedicated Security...

by Kammil Mahajan · 2 min read

Securing Large Language Models (LLMs): Safeguarding...

Large Language Models (LLMs), like OpenAI's GPT and others, have...

by Kammil Mahajan · 3 min read

OpenAI vs. DeepSeek - AI Model Theft Controversy

1. Investigation – How It Started OpenAI, in collaboration with...

by Kammil Mahajan · 3 min read

How AI Vulnerabilities Almost Cost a Business Millions

Imagine this: A healthcare SME invests heavily in AI to streamline...

by Kammil Mahajan · 2 min read

Regulatory and Ethical Considerations in AI Security:...

Artificial intelligence (AI) is reshaping industries, driving innovation, and...

by Kammil Mahajan · 4 min read

2025 Cybersecurity Trends: How Organizations Can Stay...

The "Cybersecurity Forecast 2025" report by Google Cloud delivers...

by Kammil Mahajan · 3 min read

The Role of AI in Cyber Defense: Revolutionizing How...

Cybersecurity is no longer just about firewalls and antivirus software. As...

by Kammil Mahajan · 4 min read

AI-Powered Cyber Threats: The Next Frontier in Cybersecurity

As businesses and individuals increasingly adopt artificial...

by Kammil Mahajan · 3 min read

Building the Bridge Between Cybersecurity and AI Security...

As technology evolves at an unprecedented pace, cybersecurity...

by Kammil Mahajan · 3 min read

5 Ways to Protect Your Privacy in the Digital Age

As the digital age continues to bring all of our lives into one streamlined...

by Kammil Mahajan · 4 min read

Best Practices to Protect Your Data Even When You're a...

Even small businesses expect to one day grow up. That's why so many...

by Kammil Mahajan · 5 min read

Protect your business from cyber threats with cyber...

Traditional insurance policies typically cover physical damage or...

by Kammil Mahajan · 3 min read

How Operational Excellence Can Make Your Company Mor...

There is a growing awareness that organizations need to adopt an...

by Kammil Mahajan · 4 min read

Thank You

Kammil Mahajan
CEO, Advice Bytes & Sector8 AI

Founder, Advisor, PhD Researcher & Lecturer

kammil@advicebytes.com

+353 87 038 5555