VICTORIA PARK PLAZA
London

2ND DECEMBER
2026

AI SEC SUMMIT

Securing AI in the Business

Understanding AI in Security

Part of the e-Crime & Cybersecurity Congress Series

AKJ ASSOCIATES

The AI Sprawl

AI SEC SUMMIT

The CISO's AI problem is no longer simply whether employees are using ChatGPT. It is AI sprawl across two fronts: user-adopted tools appearing outside approved channels, and AI being embedded-often opaquely-inside security platforms, SaaS products, developer tools and operational workflows. Every new copilot, browser extension, model endpoint, plug-in and autonomous security feature creates another path through which sensitive data can leave the organisation, permissions can be overextended, or decisions can be made without a clear audit trail.

The result is a control problem: security teams may know which applications they have bought, but not which models those applications call, what data they retain, how prompts are logged, whether outputs are used to retrain systems, or what happens when an AI-enabled security tool takes action automatically.

The number of incidents involving users sending sensitive data to generative AI applications has doubled over the previous year, with the average organisation now recording 223 GenAI-related data-policy violations each month. European research found that AI and personal-cloud violations most commonly involved regulated data, followed by source code, intellectual property, passwords and API keys. IBM's 2025 breach research found that one in five studied organisations experienced a breach linked to shadow AI, while organisations with high levels of unapproved AI usage incurred up to $670,000 in additional breach costs. Among organisations reporting an AI-related security incident, 97% lacked appropriate AI access controls.

The risk is also moving beyond accidental disclosure. One report found that risky AI prompts rose by 97% during 2025, with around 90% of organisations encountering risky prompts and approximately one in every 41 prompts classified as high risk during one observed period. More recent 2026 research found that indirect prompt-injection detections rose roughly fivefold between March and May, while some sectors were seeing serious data-exposure risk in close to one in every 17 AI interactions.

The AI Sprawl

AI SEC SUMMIT

For CISOs, that means AI systems must now be treated as both a new data-egress channel and a new attack surface: models can be manipulated, agents can inherit excessive privileges, and AI-enhanced security products can propagate bad decisions at machine speed. The strategic challenge is therefore to make AI governable without making the business route around security. Blanket prohibition simply drives activity further into shadow AI. The more credible model is an enterprise AI control plane: discover every AI service and embedded model, classify the data flowing into it, bind access to identity and least privilege, assess vendors and model supply chains, log prompts and autonomous actions, and impose explicit human-approval thresholds for high-impact decisions. Most importantly, CISOs need visibility across both sides of the equation-AI used by the workforce and AI used by the security stack itself. Without that unified view, organisations risk buying AI to improve cyber defence while simultaneously creating an expanding layer of unmanaged cyber risk.

Companies see AI as a critical tool for staying ahead of threats and managing increasingly complex digital environments.

However, 94% of global businesses believe that AI will negatively affect their cyber risk exposure within the next three to five years. In the UK, 66% of businesses surveyed are concerned that AI-driven attacks will increase significantly in both complexity and scale during this period.

AI Sec will look at how cybersecurity professionals can stay ahead of this rapidly evolving environment. Join our real-life case studies and in-depth technical sessions from the most sophisticated teams globally.

Key Themes

AI SEC SUMMIT

The AI Sec Summit will cover the critical topics in both securing organisational adoption of AI...

Data Protection, Privacy & Confidentiality Leakage Risks	Preventing unintentional data exfiltration into LLMs. Guardrails for prompt injection, retention, training-data exposure and shadow AI.
Secure AI Model Development & MLOps Hardening	Supply-chain risks in model weights, training pipelines, and open-source components. Securing feature stores, model registries, datasets and automated deployment paths.
AI-Augmented Cyber Attacks	Adapt detection and control frameworks for automated phishing, synthetic identities, deepfake authorisation, and other offensive AI-enabled attacks.
Human-AI Interaction & Control Boundaries	Preventing automation bias, over-trust, and "rubber-stamping" of AI outputs. Designing human-in-the-loop vs human-on-the-loop architectures.
Operational Resilience & AI Failure management	AI as a potential single point of failure. Resilience testing for autonomous agents, chain-of-thought suppression, fall back modes and kill-switch design.
Regulatory Landscape, Compliance & Liability	EU AI Act high-risk controls, UK principles-based approach, US AI EO, NIS2, DORA, GDPR. Mapping these into control frameworks, RCSAs, and testing cycles.

Key Themes

AI SEC SUMMIT

...and the critical topics around AI in security including:

AI-Driven Identity Security & Insider Threat Detection	Models flagging impossible travel, anomalous privilege escalation, sensitive-data access, AI-agent misuse. Detection of compromised API keys and model-to-model interactions.
AI-Powered Vulnerability Discovery & Code Security	Models that scan codebases, laC, and microservices for exploitable patterns. AI accelerated fuzzing and automated patch recommendation.
AI Anti-Phishing & Social Engineering Defences	Real-time detection of AI-generated phishing, deepfake voice/video attacks, and synthetic identities. Behavioural biometrics and intent modelling for high-risk approvals.
AI for Supply-Chain & Dependency Risk	Detecting malicious libraries, poisoned datasets, adversarial model weights and compromised training pipelines. AI-driven analysis and anomaly detection.
AI-Enhanced SOC Operations	Triage copilots, incident-response assistants, and automated enrichment of alerts. Natural language correlation across logs, chats, tickets, detections and threat intel.
Intelligent Threat Detection & Behavioural Analytics	ML models learning normal vs anomalous identity, access, network and API patterns. Adaptive baselining for LLM usage.

Why Sponsor?

AI SEC SUMMIT

AI-Sec is where CISOs, security architects, DPOs and operational-risk leaders come to understand one of the most urgent challenges in modern cybersecurity: how to secure their organisations against the risks introduced by AI. As enterprises deploy GenAI, agentic automation and AI-enabled workflows across every business line, they are creating new attack surfaces, new data-exfiltration vectors, and new governance exposures faster than existing controls can keep up.

AI-Sec gives sponsors a platform to put their solutions directly in front of the people under pressure to secure LLM integrations, protect sensitive data flowing through AI tools, prevent model manipulation and prompt-injection attacks, and ensure compliance with fast-tightening regulations. If you help organisations make AI safe, trustworthy, private and resilient, this is the room you need to be in.

But AI-Sec is equally about the opportunity: how AI is transforming cybersecurity itself. Security leaders know they cannot meet rising threat volumes, soaring log data and shrinking headcount without augmentation—and they are actively seeking next-generation tools that use AI to deliver faster detection, higher fidelity alerts, automated responses, behavioural analytics, and predictive defence. **This is a one-time chance for AI-leaders to displace incumbents with buyers willing to trade up now!**

Sponsors at AI-Sec get a unique forum to demonstrate how their AI-augmented platforms materially change the economics and effectiveness of security: reducing noise, accelerating triage, integrating intelligence, and enabling proactive defence architectures that were impossible even a year ago.

Whether you offer cutting-edge AI-driven security capabilities or the controls that make enterprise AI safe to deploy, AI-Sec puts your proposition at the centre of the most strategically important shift in the cybersecurity market today.

Why AKJ Associates?

AI SEC SUMMIT

A History of Delivery

For more than 25 years, AKJ Associates has been running been the world's most sophisticated closed-door meeting places for senior cyber-security professionals from government, law enforcement, intelligence and business.
For example, our annual London-based e-Crime Congress is still the largest invitation-only, Chatham House rules, gathering of the most senior information risk and security professionals from business and government in the world.
The UK Home Office sponsored the public sector delegation from 40 countries in 2002 and we are delighted to say they still do today.

Unrivalled Relationships

Events like this have enabled us to build relationships of trust with the most influential decision-makers at the full spectrum of public and private sector organisations in the UK, Europe, Asia and the Middle East.
By providing this audience with valuable insights and business intelligence over the past 25 years, we have built up the world's most significant community of professionals in cybersecurity.
We use this to develop new events; to conduct research to understand what cybersecurity professionals are doing, thinking and buying; and to market our conferences and other services.

Smart Lead Generation

We have also developed and trained one of the most effective marketing and telemarketing operations in the cybersecurity space.
Our in-depth knowledge of the marketplace allows us to design marketing outreach that consistently delivers the best audiences for the providers of critical cybersecurity infrastructure and solutions.
We connect vendors directly with B2B decision-makers. By combining unrivalled reach, deep knowledge of specialist markets and sophisticated marketing we engage buyers to deliver real results.

Plenary keynote speaking slots

AI SEC SUMMIT

Taking your message direct to decision-makers

The e-Crime Congress Series events offer sponsors the opportunity to deliver content in a number of different ways. Plenary speakers deliver their presentations on the day of the event from a fully featured AV stage to a face-to-face audience.

Their presentations can contain slides, video and audio and speakers can deliver their speeches from the podium or from any point on the stage.

Plenary presentations are 20 minutes long and take place in the main event auditorium guaranteeing access to the largest possible audience of cybersecurity professionals on the day.

Presentations are generally designed to be informative, topical and actionable, with the use of case studies and up-to-the-minute references to current developments. Double-handed talks with clients are also welcomed.

Education Seminars

AI SEC SUMMIT

Thought and product leadership to buyers

Sponsors can also choose to reserve Education Seminar slots for their speakers. At pre-defined points in the day, attendees will be notified that the main plenary sessions are making way for a series of in-depth technical break-outs.

These sessions of up to 30 attendees are held in break-out rooms and delivered live to attendees. They are an opportunity for vendors to deep-dive into a topical problem, technology or solution in front of a group of cybersecurity professionals who have self-selected as being interested in the topic being discussed.

They are also the ideal venue for solution providers to go into technical detail about their own products and services.

These Seminars run simultaneously, and attendees choose which session to attend. At the end of the Seminar, attendees are notified that Networking time is now available before the next Plenary session.

Exhibition Booths

AI SEC SUMMIT

Your team, your resources available in real-time

Sponsor packages that contain an Exhibition Booth give sponsors the opportunity to be present in the main networking area of the event.

At these booths, sponsor representatives can interact with delegates face-to-face, deliver messaging and technical information via video presentations, demo products using their own BYOD technology and to distribute printed marketing and product information.

The most senior cybersecurity solution buyers

AI SEC SUMMIT

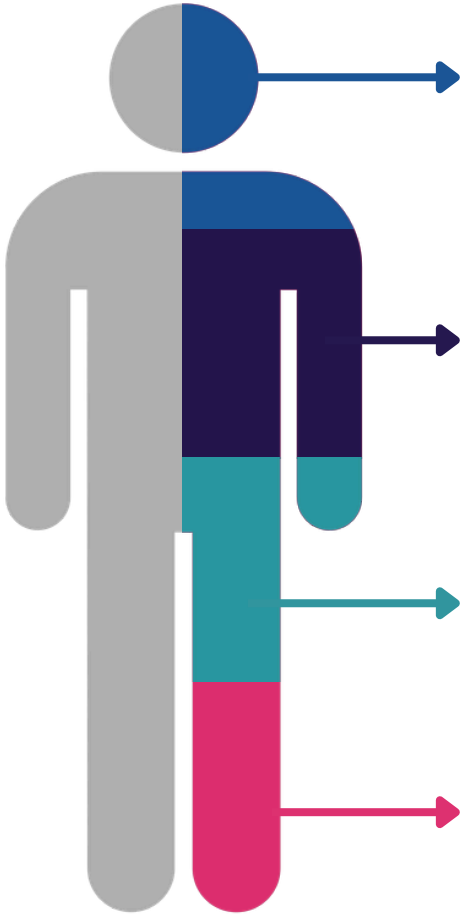
Getting access to the right people at the right time always increases lead generation and always increases profitable sales activity.

We understand that every vendor needs to sell more. That is the bottom line. This is even more necessary in the present situation.

AKJ Associates has been building relationships with senior information risk and security professionals for 25 years and our cybersecurity community is the largest of its kind globally.

We know the senior executives who drive strategy from the top, we know the enterprise architects who often control the largest budgets and we know the IT Security Leads and Engineers who so often dictate the purchase process.

All these job titles attend e-Crime & Cybersecurity Congress events.



Cyber-security

We have a 25-year track record of producing the events cyber-security professionals take seriously

Risk Management

We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance

We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy

We are a key venue for decision-makers with budget and purchasing authority

Why AKJ Associates?

AI SEC SUMMIT

We deliver the most focused selling opportunity

The e-Crime & Cybersecurity Congress has curated the largest community of genuine cybersecurity stakeholders to invite to our events.

Our reputation for hosting exceptional events with informative content, excellent networking opportunities and the best vendor partners means delegates know they are attending a quality event – and are willing to give up the time to attend.

Our delegates are invited by an in-house delegate liaison team who call senior security and privacy professionals at public and private sector companies with a personal invitation to attend

We follow up all registrations with further calls, emails on logistics requirements and reminders to ensure the best possible attendance.

The Best Delegates

The e-Crime & Cybersecurity Congress has the largest community of genuine cybersecurity stakeholders to invite to our events.
Our delegates are invited by an in-house delegate liaison team who call senior security and privacy professionals at public and private sector companies with a personal invitation to attend
We follow up all registrations with further calls, emails on logistics requirements and reminders to ensure the best possible attendance.

The Best Prospects

The e-Crime & Cybersecurity Congress prides itself on putting the key cybersecurity buyers and sellers together
To offer you the best prospects to network with, we don't invite academics, job seekers, consultants, non-sponsoring vendors or marketing service providers to this closed-door event.
The targeted networking breaks built into our agendas give you unrivalled opportunities to network, face-to-face, with the highest-quality prospects.

The Best Opportunities

AKJ Associates has never done trade shows. We see most value in working with a select number of the top vendor partners and offering those companies the best access to leads.
All booths offer the same opportunities with the same capacity and functionality regardless of the vendor company.
This is an opportunity to continue building pipeline in partnership with our outstanding 25-year reputation and the e-Crime & Cybersecurity Congress brand.

What Our Clients Say

AI SEC SUMMIT

OneSpan

AKJ Associates has never done trade shows. We see most value in working with a select number of the top vendor partners and offering those companies the best access to leads.
All booths offer the same opportunities with the same capacity and functionality regardless of the vendor company.
This is an opportunity to continue building pipeline in partnership with our outstanding 25-year reputation and the e-Crime & Cybersecurity Congress brand.

– **Sales Manager UK & I**

Red Helix

"AKJ are a pleasure to work with. A lot of work goes into making physical events a success, and with AKJ the team are there to support at each step. They ensure the events are a great success for both suppliers and end users alike."

– **Senior Digital Marketing Manager**

vmware Carbon Black.

“AKJ has been a valuable partner for us for a few years now, enabling us to build relationships and engage with the CISO community in a number of key territories across Europe. Our work with them has delivered way beyond expectations.”

– **Senior Marketing Manager**