e-Crime & Cybersecurity Congress Germany

27th Annual e-Crime & Cybersecurity Congress GERMANY

June 18th, 2026, Munich, Germany

A race against time: getting in front of the AI security problem

As much as it may seem like hype, AI adoption by business and the bad guys is a reality. Securing it is the biggest CISO challenge yet.

AKJ Associates

http://akjassociates.com/event/germany

e-Crime & Cybersecurity Congress Germany

Securing AI in the business, understanding AI as a threat vector, unwrapping AI in security tooling

The Bundesverband Digitale Wirtschaft (BVDW), Germany's digital economy association, recently released a detailed framework addressing ethical implementation of AI agent systems as the technology approaches mainstream adoption across marketing and business operations. The 25-page whitepaper arrives amid stark public resistance to autonomous AI, with BVDW-commissioned surveys revealing only 25% of Germans express willingness to delegate tasks to AI agents.

Businesses are taking a different view. According to a recent survey of 2,250 IT and cyber decision makers across 21 countries, 81% of global businesses are already using AI-driven tools as part of their cybersecurity strategy. This figure is even higher in the UK: 86% of businesses have incorporated AI.

The survey underscores that AI and automation are considered top priorities for improving cybersecurity over the next 12 months by 42% of organisations surveyed.

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.

Every sector is affected. Some, like retail innovate so fast to keep up with customers that they already have agentic and other AI across everything from inventory management to their e-commerce offerings. Others are moving more slowly. But as Boards demand the productivity and efficiency gains being promised by AI providers, pushing back against widespread AI deployment is difficult. Accenture has just announced that promotions will be linked to the frequency with which staff login to and use AI tools!

Securing this AI sprawl is critical. Ensuring data integrity becomes even more critical as it feeds into business-essential AI processes.

Organisations also need to defend against AI which is already acting as a force multiplier, enabling threat actors to execute, automate, and scale complex attacks with unprecedented speed, reducing the need for high-level human expertise. These attacks use generative AI to create tailored malware, conduct highly convincing social engineering, and autonomously map, simulate, and exploit network vulnerabilities in real time.

And what about the AI being deployed by your security vendors? Is it a new attack surface? Do you understand what they are doing? Do they?

All these topics, as well as the bread-and-butter issues, will be discussed at our latest e-Crime & Cybersecurity Congress. If you want access to the best insights, the most thought-provoking presentations, and the most senior and sophisticated network, it's must-attend.

The e-Crime & Cybersecurity Congress Germany will look at how security teams and the business must change their security model to secure AI systems and defend against AI-enabled attackers. Join our real-life case studies and in-depth technical sessions from the most sophisticated teams in the market.

e-Crime & Cybersecurity Congress Germany

Key Themes

Achieving visibility across ecosystems

From exposed initial access points, to complex IT/OT environments to roaming AI agents and other non-human machine identities, simply understanding your device and application landscape is a huge challenge. **Can you help with asset tracking and endpoint visibility? And what about anomaly detection after that?**

Data integrity a critical priority

In AI-powered business, corrupted data equals corrupted decisions. Pricing engines, demand forecasts and recommendation systems are only as trustworthy as their inputs. **CISOs must prioritise data lineage tracking, tamper detection, pipeline validation and cryptographic integrity controls across analytics and AI workflows**

Defending against the latest ransomware variants

Ransomware is effective precisely because it can exploit whatever weaknesses exist in your security architecture and processes. The threat and the actors are constantly evolving and that evolution is forcing the hands of government and causing havoc in the insurance market. **What can CISOs do to better defend against ransomware?**

Securing Agentic AI

Agentic systems don't just generate content — they act. CISOs must address model manipulation, prompt injection, data poisoning, tool-chain abuse and privilege escalation within AI agents executing transactions. **Governance must extend beyond ML pipelines into runtime controls, behavioural monitoring and kill-switch design**

Why zero trust, isolation and segmentation are key

Business ecosystems now include logistics APIs, fintech integrations, marketplace sellers, social-commerce platforms and SaaS pricing engines. Each connection expands attack surface. **Continuous third-party risk scoring, API security testing, software bill of materials (SBOM) validation and zero-trust segmentation become foundational, not optional.**

From Analysts to AI Supervisors

Security teams cannot scale headcount at the pace of digital transformation. The future SOC blends automation engineers, detection scientists and AI risk specialists. **Peer collaboration, shared intelligence and trusted industry forums become force multipliers in defending fast-moving retail environments.**

AKJ Associates

e-Crime & Cybersecurity Congress Germany

Key Themes

Making the best use of threat intelligence

In a preemptive security model, timing is everything — success depends on detecting and neutralizing threats before they become active incidents. To do this, security operations can't just rely on internal telemetry (e.g., endpoint or network logs). They need external, real-time context about emerging threats — **where do they get it?**

Improving continuous attack surface discovery

You need to know what attackers can see and what they can actually attack – and you need it on a continuous basis, not in some static inventory. Ideally you also need assets ranked by risk priority and put into the current threat and vulnerability context. **Is this feasible and is it cost effective?**

Adversary simulation and behavioural analysis

Automated adversary simulation
Identifies telemetry blind spots. They provide prioritized remediation guidance and control effectiveness metrics. They track progress trends and validate security ROIs as well as providing board and audit reporting.
How well do they work in practice?

Security Posture Management

Traditional vulnerability scanners don't handle cloud native architectures well.
Today's cloud environments spin up thousands of ephemeral assets without a traditional OS, without an IP address for long. **So how do you adapt to that dynamic, API-driven reality? How can traditional tools connect the dots – not just generate tickets?**

The power of automation

There's too much manual intervention in security. SOAR pulls data from SIEMs, EDRs, firewalls, cloud APIs, ticketing systems threat intelligence feeds, and even email servers and coordinates actions across tools via APIs and prebuilt integrations and intelligent playbooks. **Well, that's the theory. How does it work in the real world?**

Dealing with regulations

CISOs now must build a single coherent security program that simultaneously satisfies divergent regulatory demands; they must interpret vague legal standards into technical architectures, and they risk non-compliance if auditors, regulators, or courts interpret differently later; they face unrealistic expectations around incident reporting; and they face personal liability. **Can RegTech help?**

AKJ Associates

Why AKJ Associates?

e-Crime & cybersecurity GERMANY

A History of Delivery

For more than 20 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.

Global Engagement

We have run hundreds of events in the **UK, across Europe, the Middle East and Asia**, attracting **tens of thousands of delegates** in cybersecurity, data security and privacy.

These delegates range from C-suite CIOs, CTOs, CROs and C(I)SOs, to heads of enterprise architecture, desktop and network. They encompass all the senior professionals whose input drives security and privacy solution purchase decisions.

And as well as cross-sector events for both private and public sector, we also design and deliver sector-specific conferences for high-value, high-sophistication sectors including the legal sector, financial services and gambling and gaming.

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 20 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.**

Delivering your message direct to decision-makers

Plenary Speakers

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

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.

Your team and your resources available in real-time

Exhibition Booths

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.

Sponsors may wish to consider different ways to drive footfall to their booths.

For example, sponsors who have presented in Plenary or in an Education Seminar can close their presentations by directing the audience to their booths.

And there are additional gamification elements available, including sponsor-supplied prizes, that can effectively drive traffic to booths.

Delivering the most senior cybersecurity solution buyers

Our USP? We put buyers and sellers together

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

You will have access to the most senior buying audience in the cyber-security market.

AKJ Associates has been building relationships with senior information risk and security professionals for 20 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 of these job titles attend e-Crime & Cybersecurity Congress events.

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

Cyber-security
We have a 20-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

We deliver the most focused selling opportunity

Specific, actionable and relevant information for time-constrained industry professionals

The perfect platform for solution providers to deliver tailored advice to the right audience

Focus

Target growth

Each event represents a targeted opportunity to address the needs of a specific community whose need for your solutions and services is growing.

Leads

Boost sales

Sponsors can tailor messages to the needs of an audience that shares similar concerns and challenges, looking for solutions now.

Choice

Meet commercial aims

We work with sponsors to ensure they meet their commercial aims. We offer a number of sponsorship options, each providing specific benefits.

Value

Showcase solutions

Our events provide sponsors with a unique platform to showcase solutions, as well as provide advice on how best to solve delegates' key challenges.

e-Crime & Cybersecurity Congress Germany

Delegate Acquisition

- The e-Crime & Cybersecurity Congress has 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**.

Lead Sourcing

- 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. This **attention to quality over quantity** has been the hallmark of AKJ's events for 20 years.
- Each of our vendor partners will receive a delegate list at the end of the event.
- Through our targeted networking breaks built into our agendas you will have **unrivalled opportunities to network** with high-quality prospects with face-to-face networking at the event.

Get Your Message Across

- **Content is king,** which is why the e-Crime & Cybersecurity Congress prides itself on delivering informative and useful content, to attract senior audiences of decision-makers.
- Deliver an exclusive 20-min keynote presentation in the virtual plenary theatre, or host a 30-min targeted workshop session: good content drives leads to your booth, and showcases your company's expertise
- AKJ's in-house content / research team will complement the agenda with best practice from leading experts and senior security professionals from the end-user community
- If you are not presenting, the exhibitor booth offers the opportunity to share white papers and other resources for delegates to takeaway

Exclusivity Delivered

- 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.
- Our events keep the same ethos as when we first started 20 years ago, limiting vendor numbers. We will not be a hangar with hundreds of vendors competing for attention. We will keep our **events exclusive to give the best networking opportunities**.
- 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 and driving leads** in partnership with our outstanding 20-year reputation and the e-Crime & Cybersecurity Congress brand.

What our sponsors say about us

e-Crime & cybersecurity GERMANY

OneSpan

Sales Manager UK & I

"Firstly, a big thank you for yesterday — it was a fantastic event, and we really felt it was a great success. The quality of the attendees was excellent; people were genuinely engaged and very open to conversation. We had strong interest at the stand throughout the day, with many visitors eager to learn more about our solutions."

Red Helix

Senior Digital Marketing Manager

"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."

vmware | Carbon Black.

Senior Marketing Manager

"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."

Ninety five percent of our exhibitors and sponsors work with us on multiple occasions each year

Our sponsor renewal rate is unrivalled in the marketplace

This is because our sponsors generate real business at our events every year

AKJ Associates