

e-Crime & Cybersecurity Congress BENELUX



16th Annual e-Crime & Cybersecurity Congress BENELUX

24th November 2026, Amsterdam, Netherlands

Tomorrow's threats, yesterday's playbook

As legacy, human-paced security meets next-generation adversaries, how can already stretched security teams keep up?

AKJ Associates

Under Sustained Digital Attack

The Benelux region has entered a new and more dangerous phase of the cyber threat landscape. What was once a story of isolated breaches has become one of continuous, industrialised compromise — and the past twelve months have provided stark proof.

In February 2026, the Netherlands suffered what many analysts consider the most significant cybersecurity incident in Dutch history: the breach of telecom provider Odido, in which the ShinyHunters group used multi-stage social engineering — impersonating internal ICT staff to bypass multi-factor authentication — to exfiltrate the records of more than 6.5 million customers and 600,000 businesses.

In Belgium, a ransomware attack on AZ Monica hospital exposed a deeper structural weakness: at least five Belgian hospitals were impacted through a single shared patient registration software supplier, with roughly 71,000 patient records surfacing on the dark web. These organisations were not directly hacked — they were connected to someone who was.

In Luxembourg, in March 2026, attackers accessed data on state-managed devices at Luxembourg's central government IT centre (CTIE), prompting an emergency cabinet review.

These are not outliers. They are data points on a steep upward curve. European organisations now face the sharpest regional growth in cyber threats globally, with weekly attack volumes running 58% higher than just two years ago.

The geopolitical dimension is intensifying in parallel: Microsoft analysis shows Russian state-aligned cyber operations against NATO countries surged 25% in a single year, with Belgium and the Netherlands both ranking among the top targets.

And CISOs face a threat environment where both the volume and the sophistication of attacks are compounding simultaneously — and where the average dwell time between compromise and detection means that, for many organisations, extraction is complete before impact is even visible.

Conventional, human-paced defence cannot keep up with machine-paced offence. Signature-based tools, periodic reviews and manually triaged alerts were designed for a threat landscape that no longer exists. Organisations across the Benelux — from multinational headquarters and financial institutions to the SMEs that make up the backbone of the regional economy, and which now absorb the majority of attacks — must respond in kind: with AI-augmented security capabilities that detect anomalies in real time, correlate signals across cloud, endpoint and supply chain, and respond at machine speed.

Regulatory momentum reinforces the urgency, with NIS2 obligations now being enforced across all three countries and cyber insurers making capabilities such as EDR, MFA and tested incident response plans preconditions of cover.

This is the context in which we are convening the e-Crime and Cybersecurity Congress, Benelux: a dedicated regional forum bringing together the Benelux cybersecurity community — practitioners, decision-makers, regulators and solution providers — to confront this escalation head-on.

The e-Crime & Cybersecurity Congress Benelux will put delegates and vendors at the centre of the region's most urgent business conversation, in front of an audience actively seeking the next generation of defences. The threat has been upgraded. So how will the region's defences will be upgraded to match?

Key Themes: Building Better Security

Pre-emptive security, a change in operating model

Under a preemptive security model, timing is critical — success hinges on identifying and neutralising threats before they escalate into live incidents. Internal telemetry alone isn't enough for security operations to achieve this. They also need real-time, external context on emerging threats — **but where does that come from?**

Security Posture Management 2.0

Traditional security tooling assumes a stable estate. Cloud-native environments break that model — thousands of containers, functions and services spin up and vanish in minutes, visible only through APIs. Point-in-time scans and siloed alerts can't keep pace. **So what does managing security posture mean in that world — continuous context and prioritised risk, or just more tickets?**

See your surface: continuous attack surface discovery

You need visibility into your external attack surface as adversaries see it — every exposed asset, service and entry point — refreshed continuously, not captured in a static inventory. Each asset should also be risk-ranked against live threat and vulnerability data, so remediation targets what attackers will actually hit first. **Is this feasible and cost effective?**

Getting the most out of automation

Security still drowns in manual work — and SOAR promises salvation: pulling data from SIEMs, EDRs, firewalls, cloud APIs, and threat intel feeds, orchestrating responses through prebuilt integrations and "intelligent" playbooks. But integrations break, and automating a bad process just makes mistakes faster. **What does SOAR actually deliver in the real world?**

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?**

Whose Cloud risk is it anyway?

Cloud platforms may be secure, but customer-side risk isn't: misconfigured storage and permissions, sprawling APIs, federated identity gaps and misread shared-responsibility boundaries leave environments hard to map, let alone secure. **So is CSPM/CIEM tooling the answer? What about consolidating into CNAPP/CWPP? And how do you extend controls into SaaS providers and MSSPs? Can vendors help?**

Key Themes: AI and Quantum

Identity, authority, and control for non-human actors

CISOs must rethink core identity and governance frameworks, including the adoption of robust agent identity models (spanning machine, service, and workload identities), and clearly defined delegation structures that determine what authority an agent holds and who grants it. **What technologies can help them maintain visibility and control?**

Data protection and leakage risks

What does “insider threat” mean when the actor is non-human? For CISOs, the focus shifts to monitoring the behaviour of agents as well as users, developing capabilities to detect anomalous machine activity, and establishing effective controls that balance guardrails, detection, and containment. **Do you need AI defences to do that?**

AI anti-phishing and social engineering defences

AI is shifting defence from static filtering to behavioural detection at scale, flagging anomalies that rules / signatures miss. It can also enable pre-emptive defence against social engineering, identifying manipulation cues. The result is a move from reactive blocking to adaptive defence reducing both successful attacks and analyst workload. **Can you help?**

Who needs to be quantum-ready?

Anyone responsible for long-lived sensitive data or critical infrastructure has a quantum problem. That means banks, governments, telecoms, energy, healthcare whose datasets need to last decades. If your encryption protects value over time, you need crypto-agility and a migration path now, not when quantum arrives. **How does this work in the real world?**

Integrity and the AI-enabled supply chain

AI-native operating models imply dependence on a complex supply chain of foundation models, internal systems, and external APIs and orchestration layers that collectively produce legal work. Imagine the consequences of hacking such a system. **So how do CISOs stop that happening?**

Intelligent Threat Detection

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?**

Why AKJ Associates?



A History of Delivery

For more than 25 years, AKJ Associates has been running 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 & Cyber Security 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, manufacturing, retail, healthcare, CNI.

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**.

Delivering your message direct to decision-makers



Plenary Speakers

The e-Crime & Cyber Security 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.



AKJ Associates

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.



AKJ Associates

Delivering the most senior cybersecurity 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.

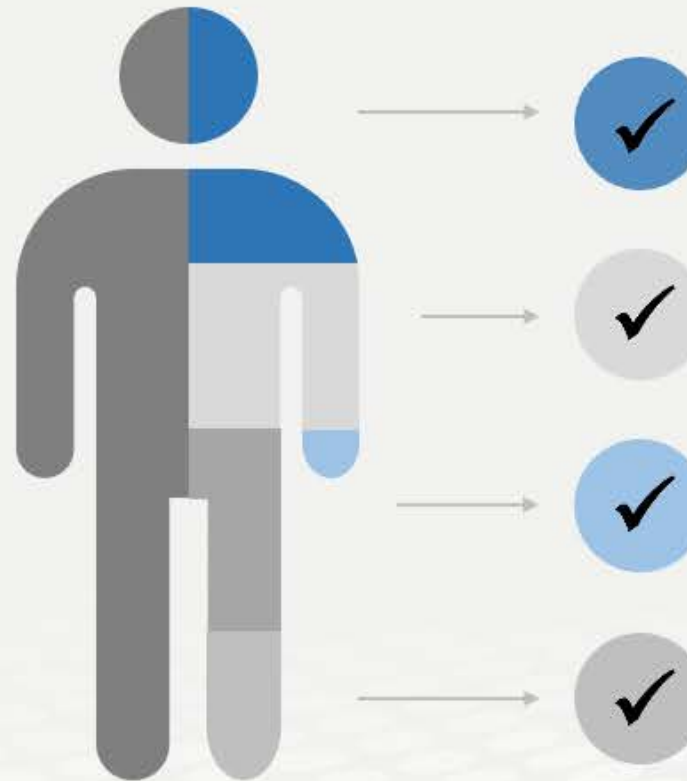
You will have access to the most senior buying audience in the cyber-security market.

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

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



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

Delivering the most focused selling opportunity



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 25 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.

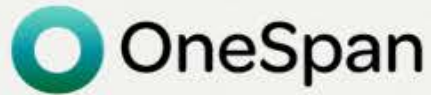
Get Your Message Across

- **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 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 25 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 25-year reputation and the e-Crime & Cybersecurity Congress brand.

What our sponsors say about us



"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."

Sales Manager UK & I



"Thank you for your email. I attended the event yesterday and have to say it was very well organised."

We were very happy with the turnout for our afternoon session as well - all in all, it was a very successful event!

Senior Marketing Executive



"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



"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. The events they hold are a great vehicle for discussing the latest challenges and our work with them has delivered way beyond expectations."

Senior Marketing Manager

95% percent of our exhibitors and sponsors work with us on multiple events each year.

This is because they generate real business at our events every year. Our sponsor renewal rate is unrivalled in the market.

AKJ Associates