

# Post event report



The 23<sup>rd</sup> e-Crime & Cybersecurity  
Germany

16<sup>th</sup> January 2025 | Frankfurt, Germany

## Strategic Sponsors



## Education Seminar Sponsors



## Networking Sponsor



“ I really enjoyed the time there, networking opportunities, speeches and meaningful conversations. I was impacted most by the geopolitical take on technology and the themes made me think a lot. I really recommend participation to this event, as it is not the average networking event but it adds a lot of value to individuals and the overall engaged Cybersec Community. ”

Senior Network Security Engineer,  
Berenberg Bank

“ The Cybersecurity Congress – a successful combination of specialist presentations and networking opportunities. The presentations – given by experienced practitioners – offered a broad view of current trends, regulatory challenges and solutions; and possible solutions. ”

Senior Referent Bereichsgrundsätze/  
Risikococontrolling – KfW Bankengruppe

Inside this report:

- Sponsors
- Key themes
- Who attended?
- Speakers
- Agenda
- Education Seminars



**Speakers**

Simon Brady,  
Event Chairman & Managing Editor  
**AKJ Associates Ltd**

Julian Dube, Information Security Officer  
**E.ON Digital Technology**

Kashif Husain,  
Information Security Officer  
**Nomura Continental Europe**

Ashar Javed,  
Head of Security Technology –  
Security Technology Section  
**Hyundai AutoEver Europe GmbH**

Dr. Martin Krämer,  
Security Awareness Advocate  
**KnowBe4**

Chuks Ojeme, Global Chief Information  
Security & Compliance Officer  
**Brenntag**

Sneha Parmar, ISO  
**Lufthansa Group Digital Hangar**

Florian Raack, Sales Engineer  
**Varonis**

Chris Robbins,  
Assistant Legal Attaché,  
LEGAT Berlin/Frankfurt Sub-office  
**Federal Bureau of Investigation**

Meri Roboci, AI Security Strategist  
**DWS Group**

Harald Roeder,  
Senior Solutions Engineer  
**Censys**

Manit Sahib,  
Ethical Hacker & Former Head of  
Penetration Testing & Red Teaming  
**Bank of England**

Christopher Schrauf,  
SIEM & Cybersecurity Architekt  
**Cyberproof**

Christian Schramm,  
Enterprise Sales Engineer  
**CrowdStrike**

Antony Seedhouse, Customer Engineer  
**Red Sift**

Filip Verloy, Field CTO EMEA & APJ  
**Rubrik**

Pietro Verzi,  
Partner Engineering, Global Security  
**Google Germany GmbH**

Tabatha von Koelichen,  
Regional Sales Director for DACH  
and Central Europe  
**Censys**

**Key themes**

Making the most of AI and ML

Building a next gen security architecture

What do regulators really want?

Cybersecurity as a service: the pros and cons

Developing the next generation of security leaders

Cybersecurity for SaaS/IaaS/PaaS

**Who attended?**



**Cyber-security**

We have a 15-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

| Agenda |   |
|--------|---|
| 08:30  | Registration & breakfast networking   |
| 09:20  | Chair's welcome   |
| 09:30  | <b>United in the fight against global cybercrime</b><br><b>Chris Robbins</b> , Assistant Legal Attaché, LEGAT Berlin/Frankfurt Sub-office, Federal Bureau of Investigation <ul style="list-style-type: none"> <li>• How do the FBI collaborate with German authorities to dismantle international cybercrime networks?</li> <li>• Insights into joint operations that target cybercriminal groups and disrupt their infrastructure</li> <li>• The role of cryptocurrency tracing in cutting off cybercriminal funding across borders</li> <li>• Strategies for public-private partnerships that enhance cybersecurity resilience in both nations</li> </ul>   |
| 09:50  | <b>Backup!: Cyber-recovery</b><br><b>Filip Verloy</b> , Field CTO EMEA & APJ, Rubrik <ul style="list-style-type: none"> <li>• Analysts predict that in 10 years, we will experience a successful ransomware attack approximately every 2 seconds</li> <li>• 96% of IT and security managers worldwide fear that their organisation will not be able to maintain business continuity after a cyber-attack, according to the new study 'The State of Data Security by Rubrik Zero Labs: The Hard Truths'</li> <li>• Attendees will learn how to increase their cyber-resilience.</li> </ul>   |
| 10:10  | <b>The cybersecurity crystal ball: Proactive threat detection with internet intelligence from Censys</b><br><b>Harald Roeder</b> , Senior Solutions Engineer, Censys;<br><b>Tabatha von Koelichen</b> , Regional Sales Director for DACH and Central Europe, Censys <ul style="list-style-type: none"> <li>• The state of cybersecurity in 2024: Emerging threats and the expanding attack surface</li> <li>• Why visibility matters: Uncovering hidden risks with comprehensive internet asset discovery</li> <li>• Real-time threat detection: Leveraging global internet scanning to identify vulnerabilities before attackers do</li> <li>• Actionable insights: How to integrate Censys into your security stack for maximum impact</li> </ul>   |
| 10:30  | <b>Redefining security strategy under EU AI Act: Prioritising human factors in AI integration</b><br><b>Meri Roboci</b> , AI Security Strategist, DWS Group <ul style="list-style-type: none"> <li>• Adapting security strategies to EU AI Act – Understand practical steps to align security practices with the EU AI Act's standards</li> <li>• Building trust in AI tools through human-centric design – Learn how to address biases, ethical issues, and build trust in AI systems for effective security operations</li> <li>• Incorporating human oversight in AI risk management – Discover methods to improve AI risk assessment and response with human input</li> </ul>   |
| 10:50  | Networking break  |
| 11:20  | <b>Navigating supply chain cyber-risks: The impact of regulations and geopolitical tension</b><br><b>Chuks Ojeme</b> , Global Chief Information Security Officer, Brenntag <ul style="list-style-type: none"> <li>• Mastering compliance challenges amid geopolitical tensions and escalating cyber-threats</li> <li>• Proactively mitigating advanced, volatile, and persistent threats to ensure seamless business continuity</li> <li>• Developing cost-efficient strategies to overcome global supply chain upheavals in 2025 and beyond</li> </ul>   |
| 11:40  | <b>Cybersecurity in the spotlight or the headlights?</b><br><b>Simon Brady</b> , Event Chairman & Managing Editor, AKJ Associates Ltd <ul style="list-style-type: none"> <li>• What does high profile mean for CISOs and other security staff?</li> <li>• Why regulation is a double-edged sword</li> <li>• The problem of transparency</li> <li>• The transition to true risk management – shake out and shake down</li> </ul>   |
| 12:00  | <b>Securing the modern enterprise: The power of Adaptive MXDR</b><br><b>Christopher Schrauf</b> , SIEM & Cybersecurity Architekt, Cyberproof; <b>Pietro Verzi</b> , Partner Engineering, Global Security, Google Germany GmbH <ul style="list-style-type: none"> <li>• The modern enterprise faces an ever-evolving threat landscape, characterised by sophisticated cyber-attacks and rapid technological advancements. This presentation will explore how organisations can build capabilities that adapt to changing landscape and new cyber-threats, using Adaptive MXDR.</li> <li>• Discussion points:                             <ul style="list-style-type: none"> <li>◦ The importance of a cloud native and modern SecOps platform</li> <li>◦ The need for threat intelligence to track cybercriminals activities</li> <li>◦ Increasing alert fidelity to enhance operational efficiency</li> <li>◦ Defining the outcomes that matters to drive continuous improvement</li> </ul> </li> </ul> |

| Agenda       |   |
|--------------|---|
| <b>12:20</b> | <b>Education Seminars</b><br><div style="display: flex; justify-content: space-between;"> <div style="width: 48%;"> <p><b>Red Sift</b><br/> <b>Email security today: The role of DMARC</b><br/> <b>Antony Seedhouse</b>, Customer Engineer, Red Sift</p> </div> <div style="width: 48%;"> <p><b>Varonis</b><br/> <b>Why do employees steal data from their own company? – Hunting insiders with Varonis</b><br/> <b>Florian Raack</b>, Sales Engineer, Varonis</p> </div> </div>  |
| <b>13:00</b> | Lunch & networking break  |
| <b>14:00</b> | <b>Enhancing web security without breaking the bank</b><br><b>Ashar Javed</b> , Head of Security Technology – Security Technology Section, Hyundai AutoEver Europe GmbH <ul style="list-style-type: none"> <li>• AI-powered custom WAF solutions</li> <li>• Undercovering strategies for finding needles in the haystack of daily web traffic</li> <li>• Maximising your existing security stack within budget</li> <li>• Raising the bar: Making attackers think twice</li> </ul>  |
| <b>14:20</b> | <b>Eight things your NG SIEM must do</b><br><b>Christian Schramm</b> , Enterprise Sales Engineer, CrowdStrike <ul style="list-style-type: none"> <li>• Many traditional SIEM and logging tools [crowdstrike.com] were developed more than a decade ago and can no longer adequately handle today’s data volumes. With the volume of log data growing faster than IT budgets, SecOps teams need a solution that can keep pace with the demands for speed, scalability and efficiency to support the growing volumes of data. Modern log management can deliver high performance and sub-second latency at low cost.</li> <li>• Learn from Christian Schramm, Sales Engineer at CrowdStrike: <ul style="list-style-type: none"> <li>◦ The typical drawbacks and blind spots of legacy SIEM systems</li> <li>◦ How changing security requirements have turned the SIEM market on its head</li> <li>◦ Eight key features to look for when evaluating your next SIEM system</li> </ul> </li> </ul>   |
| <b>14:40</b> | <b>The pivotal role of security culture in addressing CISO’s top challenges in 2025</b><br><b>Dr. Martin Krämer</b> , Security Awareness Advocate, KnowBe4 <ul style="list-style-type: none"> <li>• Information security professionals are navigating an increasingly complex threat landscape shaped by geopolitical shifts and rapid technological advancements. Key challenges include AI-driven threats, evolving regulatory demands, talent shortages, skill gaps, data security and privacy concerns, and the need to strengthen operational resilience</li> <li>• To address these issues effectively, professionals must harness the power of a strong security culture to drive sustainable, organisation-wide change. Attend this session to explore: <ul style="list-style-type: none"> <li>◦ How fostering a robust security culture can serve as a critical strategy in overcoming these pressing challenges</li> <li>◦ Leverage security culture as a strategic enabler</li> <li>◦ Navigate complex threat landscapes</li> <li>◦ Drive sustainable change to enhance organisational resilience</li> </ul> </li> </ul> |
| <b>15:00</b> | Networking break  |
| <b>15:30</b> | <b>Leveraging DORA TLPT (Threat-Led Penetration Testing) to enhance cyber-resilience</b><br><b>Manit Sahib</b> , Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England <ul style="list-style-type: none"> <li>• How DORA TLPT aligns seamlessly with TIBER-EU, CBEST &amp; DORA to enhance cyber-risk management</li> <li>• Discover the benefits of an EU-standard approach to threat-led testing</li> <li>• See how DORA TLPT boosts readiness for live system testing</li> <li>• Learn how to start using DORA TLPT for ongoing cyber-resilience and regulatory compliance</li> </ul>   |
| <b>15:50</b> | <b>Resourcing priorities in third-party risk management and supply chain security</b><br><b>Simon Brady</b> , Managing Editor & Event Chairman, AKJ Associates (Moderator);<br><b>Sneha Parmar</b> , ISO, Lufthansa Group Digital Hangar;<br><b>Chuks Ojeme</b> , Global Chief Information Security & Compliance Officer, Brenntag;<br><b>Julian Dube</b> , Information Security Officer, E.ON Digital Technology;<br><b>Kashif Husain</b> , Information Security Officer, Nomura Continental Europe <ul style="list-style-type: none"> <li>• Identifying, risk assessing and screening critical vendors – a job for who?</li> <li>• Defining contractual obligation: how do you enforce your security requirements, standards and data handling practices?</li> <li>• Approaches to continuous vendor monitoring: dealing with problem third parties</li> <li>• Incident response planning and managing third-party breaches</li> <li>• What about security vendors?</li> </ul>  |
| <b>16:30</b> | Chair’s closing remarks   |
| <b>16:35</b> | Conference close  |

| Education Seminars   |  |
|--|--|
| <p><b>Red Sift</b></p> <p><b>Email security today: The role of DMARC</b></p> <p><b>Antony Seedhouse,</b><br/>Customer Engineer, Red Sift</p>                                     | <ul style="list-style-type: none"> <li>• <i>Understanding the risk:</i> Explore the increasing prevalence of email spoofing and phishing attacks and their impact on businesses that lack robust domain protection</li> <li>• <i>Why DMARC matters:</i> Gain insights into how DMARC works to prevent email impersonation and safeguard your organisation’s email ecosystem</li> <li>• <i>DMARC trends and challenges:</i> Understand common challenges and what the data reveals about organisational progress in securing domains</li> <li>• <i>Streamlining with a managed OnDMARC provider:</i> Learn how using a managed DMARC provider such as Red Sift’s OnDMARC makes implementation and management straightforward, helping organisations achieve enforcement and stay secure without added complexity</li> <li>• <i>OnDMARC in action:</i> Hear how businesses have strengthened email security and protected their brands with OnDMARC</li> </ul>   |
| <p><b>Varonis</b></p> <p><b>Why do employees steal data from their own company? – Hunting insiders with Varonis</b></p> <p><b>Florian Raack,</b> Sales Engineer,<br/>Varonis</p> | <p>In our modern IT world, we are constantly focused on preventing external threats. However, we often overlook one of the biggest threats: insiders within our own ranks. Corporate espionage, high employee turnover, and corruption are just a few reasons why individuals might steal data from their own companies.</p> <p>Moreover, it only takes a single compromised identity for an attacker to transition from an outsider to an insider. These acts often go unnoticed because they occur under the guise of legitimate authorisation. Additionally, employees typically have access to far more data than they need to perform their jobs. Generative AI adds another layer of complexity to this issue.</p> <p><b>Attendees will learn:</b></p> <ul style="list-style-type: none"> <li>• How the Varonis Data Security Posture Management Platform can help you tackle this problem and effectively protect your data in a hybrid world</li> <li>• Remember, a data breach can never be undone</li> </ul> |