Post event report

Strategic Sponsors

censys

CROWDSTRIKE

CyberProof
A UST Company

KnowBe4

Recorded Future®

rubrik

THREATLOCKER

Education Seminar Sponsors

RED SIFT

VARONIS

Networking Sponsor

CybelAngel

“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

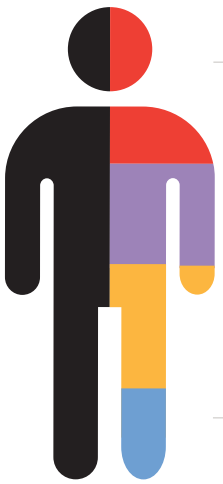
“The Cybersecurity Congress – a successful combination of specialist presentations and networking opportunities. The presentations – given by experienced practitioners – offered a broad view of current trends, regulatory challenges and solutions; and possible solutions.”
Senior Referent Bereichsgrundsätze/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

Inside this report:

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

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

Agenda

08:30	Registration & breakfast networking
09:20	Chair's welcome
09:30	**United in the fight against global cybercrime** **Chris Robbins,** Assistant Legal Attaché, LEGAT Berlin/Frankfurt Sub-office, Federal Bureau of Investigation • How do the FBI collaborate with German authorities to dismantle international cybercrime networks? • Insights into joint operations that target cybercriminal groups and disrupt their infrastructure • The role of cryptocurrency tracing in cutting off cybercriminal funding across borders • Strategies for public-private partnerships that enhance cybersecurity resilience in both nations
09:50	**Backup!: Cyber-recovery** **Filip Verloy,** Field CTO EMEA & APJ, Rubrik • Analysts predict that in 10 years, we will experience a successful ransomware attack approximately every 2 seconds • 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'. • Attendees will learn how to increase their cyber-resilience.
10:10	**The cybersecurity crystal ball: Proactive threat detection with internet intelligence from Censys** **Harald Roeder,** Senior Solutions Engineer, Censys; **Tabatha von Koelichen,** Regional Sales Director for DACH and Central Europe, Censys • The state of cybersecurity in 2024: Emerging threats and the expanding attack surface • Why visibility matters: Uncovering hidden risks with comprehensive internet asset discovery • Real-time threat detection: Leveraging global internet scanning to identify vulnerabilities before attackers do • Actionable insights: How to integrate Censys into your security stack for maximum impact
10:30	**Redefining security strategy under EU AI Act: Prioritising human factors in AI integration** **Meri Roboci,** AI Security Strategist, DWS Group • Adapting security strategies to EU AI Act – Understand practical steps to align security practices with the EU AI Act's standards • 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 • Incorporating human oversight in AI risk management – Discover methods to improve AI risk assessment and response with human input
10:50	Networking break
11:20	**Navigating supply chain cyber-risks: The impact of regulations and geopolitical tension** **Chuks Ojeme,** Global Chief Information Security Officer, Brenntag • Mastering compliance challenges amid geopolitical tensions and escalating cyber-threats • Proactively mitigating advanced, volatile, and persistent threats to ensure seamless business continuity • Developing cost-efficient strategies to overcome global supply chain upheavals in 2025 and beyond
11:40	**Cybersecurity in the spotlight or the headlights?** **Simon Brady,** Event Chairman & Managing Editor, AKJ Associates Ltd • What does high profile mean for CISOs and other security staff? • Why regulation is a double-edged sword • The problem of transparency • The transition to true risk management – shake out and shake down

12:00	**Securing the modern enterprise: The power of Adaptive MXDR**
	Christopher Schrauf, SIEM & Cybersecurity Architekt, Cyberproof; **Pietro Verzi,** Partner Engineering, Global Security, Google Germany GmbH
	• 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.
	• Discussion points:
	  ○ The importance of a cloud native and modern SecOps platform
	  ○ The need for threat intelligence to track cybercriminals activities
	  ○ Increasing alert fidelity to enhance operational efficiency
	  ○ Defining the outcomes that matters to drive continuous improvement

Agenda

12:20	**Education Seminars**
	Red Sift **Email security today: The role of DMARC** **Antony Seedhouse,** Customer Engineer, Red Sift
	Varonis **Why do employees steal data from their own company? – Hunting insiders with Varonis** **Florian Raack,** Sales Engineer, Varonis
13:00	Lunch & networking break
14:00	**Enhancing web security without breaking the bank**
	Ashar Javed, Head of Security Technology – Security Technology Section, Hyundai AutoEver Europe GmbH • AI-powered custom WAF solutions • Undercovering strategies for finding needles in the haystack of daily web traffic • Maximising your existing security stack within budget • Raising the bar: Making attackers think twice
14:20	**Eight things your NG SIEM must do**

	Christian Schramm, Enterprise Sales Engineer, CrowdStrike
	• 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.
	• Learn from Christian Schramm, Sales Engineer at CrowdStrike:
	  ○ The typical drawbacks and blind spots of legacy SIEM systems
	  ○ How changing security requirements have turned the SIEM market on its head
	  ○ Eight key features to look for when evaluating your next SIEM system

14:40	**The pivotal role of security culture in addressing CISO's top challenges in 2025**

	Dr. Martin Krämer, Security Awareness Advocate, KnowBe4
	• 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
	• 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:
	  ○ How fostering a robust security culture can serve as a critical strategy in overcoming these pressing challenges
	  ○ Leverage security culture as a strategic enabler
	  ○ Navigate complex threat landscapes
	  ○ Drive sustainable change to enhance organisational resilience

15:00	Networking break
15:30	**Leveraging DORA TLPT (Threat-Led Penetration Testing) to enhance cyber-resilience**
	Manit Sahib, Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England • How DORA TLPT aligns seamlessly with TIBER-EU, CBEST & DORA to enhance cyber-risk management • Discover the benefits of an EU-standard approach to threat-led testing • See how DORA TLPT boosts readiness for live system testing • Learn how to start using DORA TLPT for ongoing cyber-resilience and regulatory compliance
15:50	**Resourcing priorities in third-party risk management and supply chain security**
	Simon Brady, Managing Editor & Event Chairman, AKJ Associates (Moderator); **Sneha Parmar,** ISO, Lufthansa Group Digital Hangar; **Chuks Ojeme,** Global Chief Information Security & Compliance Officer, Brenntag; **Julian Dube,** Information Security Officer, E.ON Digital Technology; **Kashif Husain,** Information Security Officer, Nomura Continental Europe • Identifying, risk assessing and screening critical vendors – a job for who? • Defining contractual obligation: how do you enforce your security requirements, standards and data handling practices? • Approaches to continuous vendor monitoring: dealing with problem third parties • Incident response planning and managing third-party breaches • What about security vendors?
16:30	Chair's closing remarks
16:35	Conference close

Education Seminars	
Red Sift **Email security today: The role of DMARC** **Antony Seedhouse,** Customer Engineer, Red Sift	• *Understanding the risk:* Explore the increasing prevalence of email spoofing and phishing attacks and their impact on businesses that lack robust domain protection • *Why DMARC matters:* Gain insights into how DMARC works to prevent email impersonation and safeguard your organisation's email ecosystem • *DMARC trends and challenges:* Understand common challenges and what the data reveals about organisational progress in securing domains • *Streamlining with a managed OnDMARC provider:* 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 • *OnDMARC in action:* Hear how businesses have strengthened email security and protected their brands with OnDMARC
Varonis **Why do employees steal data from their own company? – Hunting insiders with Varonis** **Florian Raack,** Sales Engineer, Varonis	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. 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. Attendees will learn: • How the Varonis Data Security Posture Management Platform can help you tackle this problem and effectively protect your data in a hybrid world • Remember, a data breach can never be undone