# Post event report

## The 25th e-Crime & Cybersecurity Germany

24th June 2025 | Munich, Germany

### Strategic Sponsors

rubrik

RED SIFT

### Education Seminar Sponsors

CONTRAST SECURITY

Recorded Future®

> “I found the congress very exciting, especially the expert session really appealed to me! Apart from that, the speakers were really interesting and the topics exciting. The companies presented were also really exciting, even if there was little overlap for our direct use cases. But all in all, it was a congress where I didn't feel like I was at a pure sales event, which is unfortunately the case at many other congresses or events.”

**Head of IT Infrastructure and**
**IT Security,**
**Ju:niz**

> “First, I'd like to thank you for the well-organised event and for the complimentary breakfast, refreshments, and lunch. It was a great opportunity to connect with professionals in the field and gain valuable insights. As someone with a background in penetration testing, software development, project management, and embedded/automotive cybersecurity, I really appreciated the depth and structure of the event. The case studies were practical and the overall organisation was solid, with good opportunities to connect with peers in the industry.”

**Product Security Testing/**
**Incident Response,**
**Audi AG**

Inside this report:

## Key themes

What do regulators really want?

Building a next gen security architecture

Cybersecurity as a service: the pros and cons

Developing the next generation of security leaders

Making the most of AI and ML

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

Ulrich Baumann,
Partner & COO
Oikon LAW

Pascal Debus,
Head of the Quantum Security Technologies (QST) Research Group
Fraunhofer AISEC

Andreas Englisch,
IT Security Officer
European Aero Engine Consortium

Rainer Giedat,
Former Cyber Security Officer
Scalable GmbH

Sreedevi Jay,
Global Head of CERT
PagoNxt (a Santander company)

Prashant Joshi,
Head of Enterprise IT Security Architecture
Volvo Group

Waqas Jutt,
Global Lead SOC Architect
Intel Corporation

Klaus-E. Klingner,
Information Security Officer
Asambeauty

Nadim Lahoud,
SVP Operations
Red Sift

Nico Richters,
Account Director
Recorded Future

Meri Roboci,
AI Security Strategist
DWS Group

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

Paul Senkel,
Senior Solutions Engineer
Contrast Security

Agnès Terreau,
Country Data Protection and Security Officer
ManPower Group

Stefan Wiechers,
Enterprise Sales Engineer
Rubrik

Alexander Zhitenev,
Director of Corporate Systems & Head of IT Security
IFCO MANAGEMENT GmbH

| Agenda | |
|---|---|
| **09:00** | Breakfast networking & registration |
| **09:50** | Chair's welcome |
| **10:00** | **Beyond the algorithm: how Human Factors Can Make or Break AI adoption**<br>**Meri Roboci,** AI Security Strategist, DWS Group<br>• Why trust is not a given, and how to build AI literacy across your organisation<br>• Behavioural resistance & organisational culture<br>• Ethical decision-making & oversight<br>• The human-AI collaboration interface<br>• Real-world examples from finance-what went right, what went wrong, and why |
| **10:20** | **Cyber-resilience for the cloud**<br>**Stefan Wiechers,** Enterprise Sales Engineer, Rubrik<br>• Cloudfocus: How to implement robust cyber-recovery and threat containment across your cloud environments<br>• Beyond prevention: Ensure rapid response and recovery to minimise downtime and business disruption<br>• Stay operational under attack: How zero-trust architecture helps you maintain control and protect critical data – even during a ransomware event |
| **10:40** | **Security despite, for, and with Quantum Computers**<br>**Pascal Debus,** Head of the Quantum Security Technologies (QST) research group , Fraunhofer AISEC<br>• Security despite Quantum Computers: A call for action today<br>• Rethinking Quantum cybersecurity holistically<br>• Turning the tables: Using Quantum for cyber-defence |
| **11:00** | Networking break |
| **11:30** | **OT Security – A structured approach to securing industrial assets**<br>**Prashant Joshi,** Head of Enterprise IT Security Architecture, Volvo Group<br>• Understanding the growing sophistication of threats targeting industrial systems<br>• Building a multi-layered defence tailored to OT environments<br>• Common pitfalls and lessons learned |
| **11:50** | **Insights into current cybersecurity threats impacting individuals and organisations**<br>**Ulrich Baumann,** Partner & COO, Oikon LAW<br>• Regulatory obligations and legal strategies for safeguarding sensitive information<br>• AI and cyber-risk governance and navigating the implications of the EU AI Act<br>• Streamlining legal and technical requirements to meet evolving standards for cyber-resilience (NIS2 and ISO 27001) |
| **12:10** | **Education Seminars \| Session 1**<br>**Contrast Security**<br>**Solving application security without causing pain between shift left and shift right**<br>**Paul Senkel,** Senior Solutions Engineer, Contrast Security<br>**Recorded Future**<br>**Understanding DORA – Aligning cybersecurity and compliance**<br>**Nico Richters,** Account Director, Recorded Future |
| **12:50** | Lunch networking break |
| **14:00** | **PANEL DISCUSSION** **Battling nation-state hackers: Winning the cyber-war**<br>**Andreas Englisch,** IT Security Officer, European Aero Engine Consortium (Moderator);<br>**Sreedevi Jay,** Global Head of CERT, PagoNxt (a Santander company);<br>**Rainer Giedat,** Former Cyber Security Officer, Scalable GmbH;<br>**Waqas Jutt,** Global Lead SOC Architect, Intel Corporation<br>• How can organisations effectively leverage threat intelligence to proactively counter nation-state attacks? Can they?<br>• Do regulatory standards actually enhance defence against nation-state actors, or do they merely add compliance burdens without improving security?<br>• Are we doing enough to address supply chain vulnerabilities, or is this an overlooked entry point for nation-state threats?<br>• What strategic, forward-looking investments are essential for effectively countering the evolving tactics of APTs? |

## Agenda

| | |
|---|---|
| **14:30** | **Getting to grips with the new wave of domain-impersonation attacks**<br>**Nadim Lahoud,** SVP Operations, Red Sift<br>• Brand impersonation is a leading cyber-risk for CISOs and that demonstrating adequate mitigation is notoriously difficult<br>• Examine a framework that categorises the main vectors of brand impersonation and explains why technical controls are the first and most cost-effective line of defence<br>• Apply a step-by-step playbook for deploying these controls reliably at scale, illustrated by real-world case studies of organisations that solved the problem using Red Sift |
| **15:30** | **Ransomware 3.0: Weaponising AI for the next generation of ransomware attacks**<br>**Manit Sahib,** Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England<br>• LIVE DEMO – Inside the first AI-powered ransomware attack – See how my custom Agentic Ransomware Gang can take down a network in under 8 minutes<br>• Firsthand insights from real-world red team ops – from legacy tech and broken access controls to the critical lack of real-world security testing<br>• Why traditional security fails – compliance checklists and conventional tools don't stop modern ransomware<br>• What CISOs and security leaders must do now – real-world, field-tested steps to prove your controls work before attackers do it for you |
| **15:10** | Networking break |
| **15:40** | **Navigating the cloud responsibly**<br>**Rainer Giedat,** Former Cyber Security Officer, Scalable GmbH<br>• The cloud provider outlined my responsibilities – but how do I actually make it work?<br>• I've assigned roles within my DevOps team, but can they truly carry them out?<br>• What happens to cloud security if we don't have a firm grasp on our responsibilities?<br>• Services and workloads are people too, you know… |
| **16:00** | **PANEL DISCUSSION** **Securing future architectures**<br>**Manit Sahib,** Ethical Hacker & Former Head of Penetration Testing & Red Teaming, Bank of England (Moderator);<br>**Alexander Zhitenev,** Director of Corporate Systems & Head of IT Security, IFCO MANAGEMENT GmbH;<br>**Klaus-E. Klingner,** Information Security Officer, Asambeauty;<br>**Prashant Joshi,** Head of Enterprise IT Security Architecture, Volvo Group;<br>**Agnès Terreau,** Country Data Protection and Security Officer, ManPower Group<br>• How can security teams design resilient architectures to integrate and leverage emerging technologies such as AI, quantum computing, and IoT?<br>• What role does AI play in developing proactive rather than reactive security strategies?<br>• What are the best practices for integrating AI without disrupting legacy systems and existing workflows?<br>• How can organisations implement zero-trust principles and adaptive access controls to secure ever-evolving environments driven by AI and edge computing? |
| **16:30** | Chair's closing remarks |
| **16:35** | Conference close |

## Education Seminars

### Contrast Security

**Solving application security without causing pain between shift left and shift right**

**Paul Senkel,** Senior Solutions Engineer, Contrast Security

Developers complain about false positives, SOC teams suffer from alert fatigue. Developers shift left and security teams shift right, workflows disconnect and modern day workplace expectations, especially those of Generation Z, stretch processes to their limit; innovation slows while frustration builds up. Tooling is fragmented, collaboration breaks down, and AppSec becomes a source of friction rather than flow. In this talk, Paul shares hard-earned lessons from both sides of the software lifecycle – You'll learn more about the needs of the individuals on which your organisation relies, be able to reduce frustration both in development teams and the SOC, and bring security into the development process without slowing teams down. What if security didn't have to be a source of strain? What if we could find a way where both sides of the SDLC enable each other? The best security isn't just strong – it's seamless, supportive, and even fun.

Attendees will learn:

- Break down silos between Engineering, AppSec and the SOC to enable faster, safer delivery & deployment at scale
- Identify and eliminate hidden friction points caused by legacy tools and approaches
- Understand the Dev, AppSec and SOC teams' need for efficiency and autonomy at work and how to leverage the Gen Z's talents
- Turn fragmented AppSec practices into an integrated, scalable security capability

### Recorded Future

**Understanding DORA – Aligning cybersecurity and compliance**

**Nico Richters,** Account Director, Recorded Future

DORA is a new EU regulation requiring companies to make their digital systems more resilient to disruptions and cyber-attacks. It affects not only banks, but all key players in the financial system. DORA brings cybersecurity and compliance closer together than ever before. For security and IT teams, this means new priorities and increased responsibility. The requirements are complex: companies must adapt processes, reporting, and technical controls. One of the toughest parts is identifying and documenting risks in real time. Recorded Future provides the threat intelligence needed to detect risks early and support compliance reporting. This helps organisations meet regulatory demands more efficiently.

Attendees will learn:

- What the Digital Operational Resilience Act (DORA) is all about
- Why DORA is a game changer for security and IT teams
- Key challenges organisations face when implementing DORA
- How Recorded Future helps meet DORA compliance requirements