

# Post event report



The 2<sup>nd</sup>  
e-Crime & Cybersecurity Austria  
30<sup>th</sup> April 2025 | Vienna, Austria



## Strategic Sponsors



## Education Seminar Sponsors



## Networking Sponsor



“ Firstly, thank you once again for this top event. The presentations and also the speakers were not only characterised by enormous expertise, but also addressed interesting ‘side effects’ that in many respects are perhaps not originally associated with the topic of cybersecurity. These include the legal aspects and the ethical aspects from the user’s perspective. All in all, as I mentioned at the beginning, it was not only a very interesting event, at least for me, but also an instructive one, which once again made me aware of how important the topic of cybersecurity is not only for companies and organisations, but also for every user. ”

Analyst,  
Criminal Intelligence Service

Inside this report:

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



## Speakers

Christopher Schrauf, Senior SIEM & Cybersecurity Architekt  
**CyberProof**

Pietro Verzi, Partner Engineering Global Security Sales, Google on behalf of  
**CyberProof**

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

Eduardo Gonzalez, Global Advanced Cybersecurity Director  
**Banco Sabadell**

Florian Polt, Head of Group Security & Resilience  
**UNIQA Insurance Group**

Jerry Rijnbeek, Vice President Cloud & Security Technology  
**Rubrik**

Jonathan Armstrong, Partner  
**Punter Southall Law**

Marian Kühnel,  
Information Security Architect  
**ÖBB**

Philipp Amann, Group CISO  
**Austrian Post (Post AG)**

Daniele Sangion, CISO & CSO & Head of Digital Transformation  
**UniCredit Bank Austria**

Marlies Hofmann,  
Legal and Policy Officer  
**NCC-AT**

Lydia Lindner, Programme Manager  
**FFG & NCC-AT**

Matthias Lutz, Senior Account Manager  
**Cloudflare**

Michael Krüger, Senior Sales Engineer  
**Proofpoint**

Michael Lindner,  
Regional Sales Manager  
**Silverfort**

Nico Richters, Account Director  
**Recorded Future**

Sachin Loothra, Lead Solutions Architect  
**Telia**

Utz Nisslmüller, Security Specialist  
**City of Vienna**

Nikolaus Brandstetter, CISO  
**MM Group**

Florian Polt,  
Head of Group Security & Resilience  
**UNIQA Insurance Group**

Philipp Amann, Group CISO  
**Austrian Post (Post AG)**

## Key themes

Making the most of next gen tech: automation, AI and the rest

Ransomware – dealing with the new normal

Building a next gen security architecture

Cybersecurity for SaaS/IaaS/PaaS

What do regulators really want?

Can zero trust be done?

## 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	Breakfast networking & registration		
09:30	Chair's welcome		
09:40	<b>Strengthening cybersecurity competence in Austria and the EU</b> <b>Marlies Hofmann</b> , Legal and Policy Officer, NCC-AT & <b>Lydia Lindner</b> , Programme Manager, FFG & NCC-AT <ul style="list-style-type: none"> <li>The National Coordination Centre for Cybersecurity in Austria: Roles, impact, and strategic vision</li> <li>The European Cybersecurity Competence Centre: Mission, objectives, and governance</li> <li>Unlocking opportunities: EU funding for cybersecurity innovation and collaboration</li> </ul>		
10:00	<b>How Turkish escort websites made protecting the Eurovision Song Contest possible. Cybersecurity in a globally connected world</b> <b>Matthias Lutz</b> , Senior Account Manager, Cloudflare <ul style="list-style-type: none"> <li>The true art of cybersecurity lies in recognising patterns within complex contexts. Discover the story that links Turkish escort websites, the Eurovision Song Contest, the head of Iran's state-backed cyber-attack unit, and the entry ban of our CEO into Russia.</li> <li>Learn why it's essential for even regional companies to implement global security mechanisms</li> <li>Uncover the hidden connections between Turkish escort sites, Eurovision, and international cyber-warfare, explore how a regional incident led to a geopolitical ripple effect – including our CEO's ban from Russia and earn why global security strategies are crucial, even for locally operating companies</li> </ul>		
10:20	<b>Cyber-resilience for the Cloud</b> <b>Jerry Rijnbeek</b> , Vice President Cloud & Security Technology, Rubrik <ul style="list-style-type: none"> <li>Cloudfocus: How to implement robust cyber-recovery and threat containment across your cloud environments</li> <li>Beyond prevention: Ensure rapid response and recovery to minimise downtime and business disruption</li> <li>Stay operational under attack: How zero-trust architecture helps you maintain control and protect critical data – even during ransomware events</li> </ul>		
10:40	<b>AI-enhanced cybersecurity at Banco Sabadell</b> <b>Eduardo Gonzalez</b> , Global Advanced Cybersecurity Director, Banco Sabadell <ul style="list-style-type: none"> <li>AI as the new gold rush</li> <li>Impact on cybersecurity</li> <li>Regulations and frameworks for AI</li> <li>Leveraging AI for cybersecurity</li> <li>Creating a custom machine learning model</li> </ul>		
11:00	Networking break		
11:30	<b>FIRESIDE CHAT: Mitigating personal liability: The changing climate for security professionals</b> <b>Jonathan Armstrong</b> , Partner, Punter Southall Law <ul style="list-style-type: none"> <li>The changing politics of security</li> <li>Current cases</li> <li>Social media scrutiny</li> <li>Insurance options for CISOs</li> <li>Golden parachutes and legal support</li> </ul>		
12:00	<b>Cybersecurity in the age of genAI – human-centric security to protect against modern cyber-risks; Proofpoint–Customer Session</b> <b>Michael Krüger</b> , Senior Sales Engineer, Proofpoint <ul style="list-style-type: none"> <li>In this session, we will uncover hidden risks of GenAI and inform you how to protect your employees &amp; data.</li> <li>The risks associated with GenAI and how GenAI can be misused by threat actors and by employees</li> <li>How to gain insight into the use of GenAI in your organisation, enforce acceptable use policies and train employees</li> <li>How a human-centred approach to security can prevent the loss of sensitive data</li> </ul>		
12:20	<b>Education Seminars</b> <table> <tr> <td> <b>Recorded Future</b>  <b>Understanding DORA – Aligning cybersecurity and compliance</b>  <b>Nico Richters</b>, Account Director, Recorded Future </td><td> <b>Silverfort</b>  <b>Protection of service accounts: A luxury or an urgent necessity for highly privileged non-human identities?</b>  <b>Michael Lindner</b>, Regional Sales Manager, Silverfort </td></tr> </table>	<b>Recorded Future</b> <b>Understanding DORA – Aligning cybersecurity and compliance</b> <b>Nico Richters</b> , Account Director, Recorded Future	<b>Silverfort</b> <b>Protection of service accounts: A luxury or an urgent necessity for highly privileged non-human identities?</b> <b>Michael Lindner</b> , Regional Sales Manager, Silverfort
<b>Recorded Future</b> <b>Understanding DORA – Aligning cybersecurity and compliance</b> <b>Nico Richters</b> , Account Director, Recorded Future	<b>Silverfort</b> <b>Protection of service accounts: A luxury or an urgent necessity for highly privileged non-human identities?</b> <b>Michael Lindner</b> , Regional Sales Manager, Silverfort		

Agenda		
13:00	Lunch & networking break	
14:00	<b>Securing critical infrastructure with IAM in an elevated threat landscape</b> <b>Sachin Loothra</b> , Lead Solutions Architect, Telia <ul style="list-style-type: none"><li>Evolving threat landscape and its impacts on critical infrastructure</li><li>Regulations on critical infrastructure and demands towards IAM</li><li>How IAM solutions can be setup to meet the demands</li></ul>	
14:20	<b>Defending against multi-channel and multi-media AI-fuelled social engineering</b> <b>Dr. Martin Krämer</b> , Security Awareness Advocate, KnowBe4 <ul style="list-style-type: none"><li>Phishing emails are a popular choice for social engineering but by far not the only one. Messaging services, social media platforms, corporate communication channels, and online meetings are all communication channels leveraged to manipulate people</li><li>Attackers increasingly launch multi-channel attacks. No longer are cybercriminals limited to text-based communication. Voice and even video are frequently used in business contexts to communicate information. Thanks to new AI capabilities, text, voice, and video can now be easily manipulated or synthesised. Cybercriminals leverage the power of AI and multi-channel communication to step up their manipulation game</li><li>Join this session to learn; how cybercriminals are changing tack, what that means for your organisation and how you should prepare for it</li></ul>	
14:40	<b>How CyberProof and Google transformed a healthcare provider's security operations with Adaptive MxDR</b> <b>Christopher Schrauf</b> , Senior SIEM & Cybersecurity Architekt, CyberProof & <b>Pietro Verzi</b> , Partner Engineering Global Security Sales, Google on behalf of CyberProof <ul style="list-style-type: none"><li>Healthcare organisations face unique cybersecurity challenges that require innovative solutions</li><li>In this session, CyberProof and Google will show how their partnership delivered adaptive MxDR services for a leading healthcare provider. We'll walk you through a real-world case study, showing how we overcame security challenges and achieved significant business outcomes</li><li>Learn about; the client's business problem statement and security challenges, how CyberProof and Google collaborate to deliver better security, together and business outcomes, including measurable improvements in security and higher ROI</li></ul>	
15:00	<b>EXECUTIVE PANEL DISCUSSION</b>	<b>Future-proofing security architectures</b> <b>Marian Kühnel</b> , Information Security Architect, ÖBB; <b>Philipp Amann</b> , Group CISO, Austrian Post (Post AG); <b>Daniele Sangion</b> , CISO & CSO & Head of Digital Transformation, UniCredit Bank Austria <ul style="list-style-type: none"><li>How can security teams design resilient architectures to accommodate and leverage new technologies like AI, quantum computing, and IoT?</li><li>What role does AI play in developing proactive, rather than reactive, security postures?</li><li>Best practices for integrating AI without disrupting legacy systems or existing workflows</li><li>How can organisations implement zero-trust principles and adaptive access controls to secure evolving environments driven by AI and edge computing?</li></ul>
15:30	Networking break	
16:00	<b>Herding cats: Building a security governance structure that actually works</b> <b>Florian Polt</b> , Head of Group Security & Resilience, UNIQA Insurance Group <ul style="list-style-type: none"><li>Navigating conflicting legal requirements and diverse stakeholders</li><li>Creating a governance blueprint and aligning roles across entities</li><li>Tackling legal complexities while maintaining sanity</li><li>Real-world insights, practical lessons, and governance war stories</li></ul>	
16:20	<b>EXECUTIVE PANEL DISCUSSION</b>	<b>Battling nation-state hackers: Winning the cyber-war</b> <b>Utz Nisslmüller</b> , Security Specialist, City of Vienna; <b>Nikolaus Brandstetter</b> , CISO, MM Group; <b>Florian Polt</b> , Head of Group Security & Resilience, UNIQA Insurance Group; <b>Philipp Amann</b> , Group CISO, Austrian Post (Post AG) <ul style="list-style-type: none"><li>How can organisations effectively leverage threat intelligence to proactively counter nation-state attacks? Can they?</li><li>Do regulatory standards actually enhance defence against nation-state actors, or do they merely add compliance burdens without improving security?</li><li>Are we doing enough to address supply chain vulnerabilities, or is this an overlooked entry point for nation-state threats?</li><li>What strategic, forward-looking investments are essential for effectively countering the evolving tactics of APTs?</li></ul>
16:50	Chair's closing remarks	<b>17:00</b> Conference close

## Education Seminars

**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

**Silverfort****Protection of service  
accounts: A luxury or an  
urgent necessity for highly  
privileged non-human  
identities?****Michael Lindner**, Regional  
Sales Manager, Silverfort

Machine-to-Machine (M2M) accounts, also known as service or non-human accounts, are essential to IT infrastructure but pose significant security risks if not properly protected.

**Attendees will learn:**

- Why are service accounts a prime target for attackers?
- How can compromised service accounts enable lateral movement?
- Why is their security often insufficient, and how can organisations gain visibility?
- What strategies ensure the long-term protection of these privileged identities?