

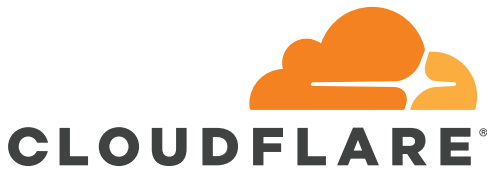
# Post event report



The inaugural  
e-Crime & Cybersecurity Austria

7<sup>th</sup> May 2024 | Vienna, Austria

## Strategic Sponsors



## Education Seminar Sponsors



Inside this report:  
Sponsors  
Key themes  
Who attended?  
Speakers  
Agenda  
Education Seminars



## Speakers

Philipp Amann,  
Group Chief Information Security Officer  
**Austrian Post (Post AG)**

Orion Beci, Cyber Adviser, Austria,  
CEE & Eastern Mediterranean  
**Marsh**

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

Kevin Breuer,  
Sales Engineer  
**LogRhythm**

Günter Esch,  
Managing Director  
**SEPPmail**

Christoph Gruber,  
Head of IT Security  
**UNIQA IT Services, GmbH**

Dominic Haussmann,  
Specialist Solutions Engineer –  
Zero Trust  
**Cloudflare**

Elsa Lischka,  
Senior IT Security Architect  
**OMV**

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

Julian Kanitz,  
Lead Sales Engineer DACH  
**Recorded Future**

Marian Kühnel,  
Information Security Architect  
**ÖBB**

Strahinja Miljkovic,  
Former Deputy CISO  
**Prinzhorn Group**

Paolo Passeri,  
Principal Sales Engineer and Cyber  
Intelligence Specialist  
**Netskope**

Heidelinde Rameder,  
CISO  
**Borealis, AG**

Manit Sahib,  
Ethical Hacker  
**The Global Fund**

Frank Schwaak,  
Field CTO EMEA  
**Rubrik**

Gabriel Stein,  
System Engineer  
**SUSE**

Andrea Szeiler,  
Global CISO  
**Transcom**

## Key themes

- NIS2 – changing the game in cybersecurity?
- Ransomware – dealing with the new normal
- Managing insider threats at a time of crisis
- From cybercrime to cyberwar
- Cloud incident response
- Embracing risk management
- The pros and cons of managed services
- Here comes real cybersecurity regulation
- Developing the next generation of security leaders
- Are AI/ML solutions the answer?
- From threat/security to risk/resilience
- Is ransomware just going to get worse?

## 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 and networking break		
09:30	Chairman's welcome		
09:40	<b>NIS2 – walking the regulatory talk</b> <b>Philipp Amann</b> , Group Chief Information Security Officer, Austrian Post (Post AG) <ul style="list-style-type: none"> <li>• The EU's approach to data governance</li> <li>• Mapping EU regulations to national legislation to organisations</li> <li>• How to NIS2 in practice?</li> </ul>		
10:00	<b>Cyber-threat landscape – one step ahead with the connectivity cloud</b> <b>Dominic Haussmann</b> , Specialist Solutions Engineer – Zero Trust, Cloudflare <ul style="list-style-type: none"> <li>• Cyber-threat situation Internet and Germany</li> <li>• Why security training for employees falls short</li> <li>• What you can do today to close one of the biggest attack vectors</li> </ul>		
10:20	<b>Third-party risk management from a third-party perspective</b> <b>Andrea Szeiler</b> , Global CISO, Transcom <ul style="list-style-type: none"> <li>• Understanding your third parties and the risks they bring to your organisation</li> <li>• Different approaches to third-party risk management and their pros and cons</li> <li>• Responsibility sharing matrix</li> <li>• Working together</li> </ul>		
10:40	<b>Education Seminars   Session 1</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;"> <b>Recorded Future</b>  <b>Unveiling the dark secrets of i-SOON: Insights into China's cyberspionage ecosystem</b>  <b>Julian Kanitz</b>, Lead Sales Engineer DACH, Recorded Future               </td> <td style="width: 50%; padding: 5px;"> <b>SEPPmail</b>  <b>From postcard to a sealed letter – why and how the quality of email communication can and should be improved</b>  <b>Günter Esch</b>, Managing Director, SEPPmail               </td> </tr> </table>	<b>Recorded Future</b> <b>Unveiling the dark secrets of i-SOON: Insights into China's cyberspionage ecosystem</b> <b>Julian Kanitz</b> , Lead Sales Engineer DACH, Recorded Future	<b>SEPPmail</b> <b>From postcard to a sealed letter – why and how the quality of email communication can and should be improved</b> <b>Günter Esch</b> , Managing Director, SEPPmail
<b>Recorded Future</b> <b>Unveiling the dark secrets of i-SOON: Insights into China's cyberspionage ecosystem</b> <b>Julian Kanitz</b> , Lead Sales Engineer DACH, Recorded Future	<b>SEPPmail</b> <b>From postcard to a sealed letter – why and how the quality of email communication can and should be improved</b> <b>Günter Esch</b> , Managing Director, SEPPmail		
11:20	Networking break		
11:50	<b>The business of being a CISO</b> <b>Simon Brady</b> , Managing Editor & Event Chairman, AKJ Associates (Moderator) <b>Philipp Amann</b> , Group CISO, Austrian Post (Post AG) <b>Heidelinde Rameder</b> , CISO Borealis, AG <b>Andrea Szeiler</b> , Global CISO, Transcom <ul style="list-style-type: none"> <li>• The role of the CISO as security regulation increases (NIS2, DORA etc.)</li> <li>• Compliance versus security as a true business driver</li> <li>• The cyber-talent shortage – real or illusion?</li> <li>• Adopting a risk-based approach to securing budgets</li> </ul>		
12:20	<b>Reducing the financial impact of cyber-attacks</b> <b>Frank Schwaak</b> , Field CTO EMEA, Rubrik <ul style="list-style-type: none"> <li>• Proactively reduce the attack surface</li> <li>• Determine the 'blast radius' of an attack</li> <li>• Restore the environment without re-infection</li> <li>• Respond to NIS2, DORA and GDPR compliance</li> </ul>		
12:40	<b>Education Seminars   Session 2</b> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;"> <b>LogRhythm</b>  <b>From threat detection to threat prediction: How generative AI is transforming cybersecurity strategies</b>  <b>Kevin Breuer</b>, Sales Engineer, LogRhythm               </td> <td style="width: 50%; padding: 5px;"> <b>SUSE</b>  <b>We need to talk about security in our containerised workloads</b>  <b>Gabriel Stein</b>, System Engineer, SUSE               </td> </tr> </table>	<b>LogRhythm</b> <b>From threat detection to threat prediction: How generative AI is transforming cybersecurity strategies</b> <b>Kevin Breuer</b> , Sales Engineer, LogRhythm	<b>SUSE</b> <b>We need to talk about security in our containerised workloads</b> <b>Gabriel Stein</b> , System Engineer, SUSE
<b>LogRhythm</b> <b>From threat detection to threat prediction: How generative AI is transforming cybersecurity strategies</b> <b>Kevin Breuer</b> , Sales Engineer, LogRhythm	<b>SUSE</b> <b>We need to talk about security in our containerised workloads</b> <b>Gabriel Stein</b> , System Engineer, SUSE		
13:20	Lunch		

Agenda	
<b>14:20</b>	<p><b>Cyber-insurance as a last line of defence</b></p> <p><b>Orion Beci</b>, Cyber Adviser, Austria, CEE &amp; Eastern Mediterranean, Marsh</p> <ul style="list-style-type: none"> <li>• Key claims data and current insights</li> <li>• Shedding light on risks and ways to boost your cyber-insurance protection</li> <li>• Boosting your insurability</li> </ul>
<b>14:40</b>	<p><b>Why identity alone is not enough for a zero trust strategy</b></p> <p><b>Paolo Passeri</b>, Principal Sales Engineer and Cyber Intelligence Specialist, Netskope</p> <ul style="list-style-type: none"> <li>• The new reality of living in a hyperconnected online world requires a new approach to security, where multiple elements must be taken into account, besides simply blocking/allowing access to a specific service or the user identity to enforcing granular permissions</li> <li>• Learn why the context is important to enforce a granular and effective security policy</li> <li>• Discover which are the elements that must be considered, besides identity, to adopt an effective zero trust strategy</li> <li>• Understand how the different security controls, such as data protection, threat protection, behaviour analytics, cooperate to protect the modern enterprise</li> </ul>
<b>15:00</b>	<p><b>Understanding the basics of social engineering</b></p> <p><b>Dr. Martin J. Krämer</b>, Security Awareness Advocate, KnowBe4</p> <ul style="list-style-type: none"> <li>• Social engineering is popular among attackers, with studies indicating more than 80% of attacks involve human error</li> <li>• Learn why social engineering is a problem and why it is so successful</li> <li>• Through the illustration of basic scientific concepts, understand how attackers use tricks to exploit the 'human factor'</li> <li>• Discover how organisations can protect their employees and what countermeasures can be put in place</li> </ul>
<b>15:20</b>	<p><b>Cyber-audit mastery: Navigating strategies for success</b></p> <p><b>Christoph Gruber</b>, Head of IT Security UNIQA IT Services, GmbH</p> <ul style="list-style-type: none"> <li>• Understanding the purpose: Clarifying the objectives and goals of cyber-audits</li> <li>• Working with auditors to facilitate a smooth audit process and address concerns effectively</li> <li>• Achieving collaboration and communication across all parties</li> <li>• How do we engage our boards and achieve public accountability?</li> </ul>
<b>15:40</b>	Networking break
<b>16:00</b>	<p><b>LIVE DEMONSTRATION</b> <b>Weaponising AI for cyber-attacks &amp; offensive operations</b></p> <p><b>Manit Sahib</b>, Ethical Hacker, The Global Fund</p> <ul style="list-style-type: none"> <li>• Overview &amp; threat landscape: How AI is being leveraged in the wild for malicious activities</li> <li>• Weaponising AI for offensive operations: Running AI through the cyber kill chain</li> <li>• ChatGPT or [insertnamehere]GPT: What's the level of effort required to build your own AI?</li> <li>• LIVE DEMO: AI in action</li> </ul>
<b>16:20</b>	<p><b>TECHNOLOGY PANEL DISCUSSION</b></p> <p><b>Elsa Lischka</b>, Senior IT Security Architect, OMV  <b>Strahinja Miljkovic</b>, Former Deputy CISO, Prinzhorn Group  <b>Marian Kühnel</b>, Information Security Architect, ÖBB  <b>Manit Sahib</b>, Ethical Hacker, The Global Fund</p> <ul style="list-style-type: none"> <li>• How do you see the future of AI in security evolving, and what steps can be taken to ensure its responsible and effective use in protecting against cyber-threats?</li> <li>• What are your thoughts on the outsourcing model in security, and how can organisations ensure that they are effectively managing the risks and benefits associated with outsourcing their security functions?</li> <li>• What are your thoughts on the shared responsibility model in security, and how can organisations effectively implement this model to ensure the security of their systems and data?</li> </ul>
<b>16:50</b>	Closing remarks
<b>17:00</b>	Conference end

Education Seminars	
<p><b>LogRhythm</b></p> <p><b>From threat detection to threat prediction: How generative AI is transforming cybersecurity strategies</b></p> <p><b>Kevin Breuer</b>, Sales Engineer, LogRhythm</p>	<ul style="list-style-type: none"> <li>• Evolution from detection to prediction</li> <li>• Simulation of attack scenarios</li> <li>• Threat intelligence automation</li> <li>• Predictive risk assessment</li> <li>• Improve Security Operations Centre (SOC) efficiency</li> <li>• Integration with existing systems</li> </ul>
<p><b>Recorded Future</b></p> <p><b>Unveiling the dark secrets of i-SOON: Insights into China's cyberspionage ecosystem</b></p> <p><b>Julian Kanitz</b>, Lead Sales Engineer DACH, Recorded Future</p>	<p>This presentation sheds light on the recently uncovered data breach of i-SOON, a China-based cybersecurity company involved in offensive cyber-espionage operations for Chinese government clients.</p> <p><b>What attendees will learn:</b></p> <ul style="list-style-type: none"> <li>• Revelation of the recently uncovered data breach of i-SOON</li> <li>• Insights into the inner workings of China's cyberspionage ecosystem</li> <li>• Raising awareness of the evolving landscape of cyber-threats</li> </ul>
<p><b>SEPPmail</b></p> <p><b>From postcard to a sealed letter – why and how the quality of email communication can and should be improved</b></p> <p><b>Günter Esch</b>, Managing Director, SEPPmail</p>	<p>98% of written communication between companies and their external partners and customers takes place via email. It should therefore be a matter of course to protect this channel in particular. There are technologies that have proven themselves in practice, but are still not used across the board. Here is a brief overview of the threats, organisational measures, the available technical protection mechanisms and how these can be used optimally and in a user-friendly way.</p> <ul style="list-style-type: none"> <li>• Email is the number 1 gateway for attackers</li> <li>• Organisational measures</li> <li>• Technical measures</li> <li>• Plus and minus</li> </ul>
<p><b>SUSE</b></p> <p><b>We need to talk about security in our containerised workloads</b></p> <p><b>Gabriel Stein</b>, System Engineer, SUSE</p>	<p>Securing your container workloads with modern security tools that gives you peace of mind. Let's talk also about Zero Trust and why it is so important.</p> <p><b>What attendees will learn:</b></p> <ul style="list-style-type: none"> <li>• Why are our standard tools are not enough?</li> <li>• Containerised workloads and security concerns</li> <li>• Protecting your modern workloads</li> </ul>