

# Post event report



The 22<sup>nd</sup> e-Crime & Cybersecurity  
Germany

30<sup>th</sup> January 2024 | Frankfurt, Germany

## Strategic Sponsors



## Education Seminar Sponsors



## Networking Sponsors



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



**Speakers**

Bettina Bassermann, Business Strategist, Pre-Sales DACH, **SUSE**

Christian Buhrow, Regional Sales Director, **SpyCloud**

Rupert Collier, VP Global Sales, **RangeForce**

Gulnara Hein, CISO, Chintai; Moona Ederveen-Schneider, Executive Director EMEA, **FS-ISAC**

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

Bernd Knippers, Senior Sales Engineer DACH, **Recorded Future**

Dr. Jesus Luna Garcia, Cybersecurity Governance – Cloud and AI, **Robert Bosch GmbH**

Dominik Mauer, Analyst & Cooperation Manager, **Federal Criminal Police Office/Bundeskriminalamt, Cybercrime Division**

Tom McVey, Solution Architect, **Menlo Security**

Sonia Neffati, Regional Chief Security Officer, Europe, **Mastercard**

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

Giovanni Pascale, **Proofpoint**

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

Riccardo Riccobane, Head of CSO Security Assurance & Head of Operational Resilience, **DWS**

Gerhard Sahner, Business Development Mobile Intelligence, **JT Global**

Stefan Schmutge, Director Sales Engineering, **Rubrik**

Marvin Schneider, Customer development, **Cloudflare**

Thomas Schuchmann, Senior Director Sales Engineering Germany, **Rubrik**

Nikolei Steinhage, Enterprise Sales Engineer DACH, **CrowdStrike**

Roland Stritt, **SentinelOne**

Dr. Timo Wandhöfer, Group CISO, **Klößner & Co**

Julian Wulff, Director, Cyber Security Central Europe, **Red Sift**

**Key themes**

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

**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			
08:00	Registration and networking break		
08:50	Chairman's welcome		
09:00	<p><b>Fighting cybercrime is teamwork! – Co-operating with the police in cyber-attacks on companies</b></p> <p><b>Dominik Mauer</b>, Analyst &amp; Cooperation Manager, Federal Criminal Police Office/Bundeskriminalamt, Cybercrime Division</p> <ul style="list-style-type: none"> <li>• What is the current situation in the field of cybercrime?</li> <li>• Who is responsible in the event of a cyber-attack on a company and who are the contacts?</li> <li>• Why is it important for a company to cooperate with the police in the event of a cyber-attack?</li> <li>• Myth check: reservations about cooperation with the police and our answers to them</li> </ul>		
09:20	<p><b>Why 24 is the answer to all questions in the cybersecurity environment!</b></p> <p><b>Thomas Schuchmann</b>, Senior Director Sales Engineering Germany, Rubrik &amp; <b>Stefan Schmugge</b>, Director Sales Engineering, Rubrik</p> <ul style="list-style-type: none"> <li>• Do you know the difference between resilience and resistance? How does resilience and resistance differ in data security and which is really more effective for businesses?</li> <li>• Are cyber-incidents really the biggest business risk? Why are cyber-risks becoming more of a management focus and what does this mean for businesses?</li> <li>• Are we investing enough and in the right things? Despite increasing security spending, why are cyber-attacks still a problem and what could we do differently?</li> <li>• How can we do better? What strategies are there to not only minimise the risk of a cyber-attack, but also to mitigate its potential consequences?</li> </ul>		
09:40	<p><b>Looking back at the threat landscape in 2023 (And what to expect for 2024)</b></p> <p><b>Paolo Passeri</b>, Principal Sales Engineer and Cyber Intelligence Specialist, Netskope</p> <p>This session will provide an overview of the main security trends observed in 2023, providing some indications on what to expect for 2024.</p> <ul style="list-style-type: none"> <li>• Cloud and SaaS adoption continue to rise in enterprise environments with users constantly adopting new apps and increasing their use of existing apps</li> <li>• Adversaries, recognising this trend, are abusing and targeting popular apps in their operations more frequently, with social engineering having become the most common method used to gain access into victims' environments</li> <li>• In parallel, the utilisation of Generative AI apps, virtually non-existent in the enterprise a year ago, has increased exponentially exposing organisations to new risks such as corporate data leakage and themed social engineering campaigns</li> </ul>		
10:00	<p><b>Threatcasting: disrupt the threat and enable the future</b></p> <p><b>Sonia Nefati</b>, Regional Chief Security Officer, Europe, Mastercard</p> <ul style="list-style-type: none"> <li>• Using threatcasting to model a range of possible and potential futures and threats in a complex and uncertain environment</li> <li>• Working with organisations via subject matter expert (SME) interviews, workshops and operationalisation exercises</li> <li>• Identifying indicators that threats or desirable futures are manifesting</li> <li>• Suggestions and actions that can be taken to disrupt the threat or enable the future</li> </ul>		
10:20	<p><b>Education Seminars   Session 1</b></p> <table border="1"> <tr> <td> <p><b>Menlo Security</b>  <b>Browser security – the proven prevention layer for enterprise cybersecurity</b>  <b>Tom McVey</b>, Solution Architect, Menlo Security</p> </td> <td> <p><b>SpyCloud</b>  <b>Ransomware revealed: The changing landscape of ransomware and data exploitation</b>  <b>Christian Buhrow</b>, Regional Sales Director, SpyCloud</p> </td> </tr> </table>	<p><b>Menlo Security</b>  <b>Browser security – the proven prevention layer for enterprise cybersecurity</b>  <b>Tom McVey</b>, Solution Architect, Menlo Security</p>	<p><b>SpyCloud</b>  <b>Ransomware revealed: The changing landscape of ransomware and data exploitation</b>  <b>Christian Buhrow</b>, Regional Sales Director, SpyCloud</p>
<p><b>Menlo Security</b>  <b>Browser security – the proven prevention layer for enterprise cybersecurity</b>  <b>Tom McVey</b>, Solution Architect, Menlo Security</p>	<p><b>SpyCloud</b>  <b>Ransomware revealed: The changing landscape of ransomware and data exploitation</b>  <b>Christian Buhrow</b>, Regional Sales Director, SpyCloud</p>		
11:00	Networking break		
11:30	<p><b>The Utopia of European Cybersecurity Certification – automation of compliance</b></p> <p><b>Dr. Jesus Luna Garcia</b>, Cybersecurity Governance – Cloud and AI, Robert Bosch GmbH</p> <ul style="list-style-type: none"> <li>• The challenges and opportunities of the upcoming certifications derived from the European Cybersecurity Act</li> <li>• The benefits of automating traditional cybersecurity certification processes, summarising practical experiences related to the upcoming EU certification scheme for cloud services (EUCS)</li> <li>• How automation can support cybersecurity certifications related to new EU regulations (e.g., NIS2, and AI Act)? A view on our ongoing activities</li> </ul>		
11:50	<p><b>The cyber-threat landscape Germany</b></p> <p><b>Marvin Schneider</b>, Customer development, Cloudflare</p> <ul style="list-style-type: none"> <li>• Cyber-threat landscape Internet and Germany</li> <li>• Why employee security training falls short</li> <li>• What you can do today to shut down one of the biggest attack vectors</li> </ul>		
12:10	<p><b>NIS 2.0 – Burden or Opportunity?</b></p> <p><b>Roland Stritt</b>, SentinelOne</p> <ul style="list-style-type: none"> <li>• The introduction of the NIS 2.0 directive (Network and Information Security Directive) represents a significant development in the cybersecurity landscape</li> <li>• What does NIS 2.0 mean for your company?</li> <li>• This presentation aims to provide food for thought and highlight opportunities and challenges that companies may face in the course of implementing NIS 2.0</li> <li>• Insights and ideas for managers and security experts</li> </ul>		

## Agenda

<b>12:30</b>	<b>Email authentication: Are you ready for stringent email acceptance rules at Google and Yahoo?</b>	
	<p><b>Giovanni Pascale</b>, Proofpoint</p> <p>To help address the high number of fraudulent emails hitting their users' accounts, Google and Yahoo announced new email authentication requirements that could impact your company's deliverability. The new requirements will be enforced as early as 1st February 2024. Join our session to hear from our subject matter expert Giovanni Pascale on key aspects of the new requirements, such as SPF, DKIM, DMARC, and DMARC alignment. We will discuss:</p> <ul style="list-style-type: none"> <li>• Overview of the new requirements</li> <li>• Overview of SPF and DKIM and things to consider</li> <li>• The role of DMARC and the challenges associated with getting alignment</li> <li>• Tools, technology and resources to help reduce the impact to your organisation</li> </ul>	
<b>12:50</b>	<b>Education Seminars   Session 2</b>	
	<p><b>Recorded Future</b>  <b>Insights into the dark web: cybercrime forums, markets and threats to watch out for</b>  <b>Bernd Knippers</b>, Senior Sales Engineer DACH, Recorded Future</p>	<p><b>SUSE</b>  <b>Network traffic visibility &amp; zero trust security in Kubernetes environments</b>  <b>Bettina Bassermann</b>, Business Strategist, Pre-Sales DACH, SUSE</p>
<b>13:30</b>	Lunch and networking break	
<b>14:30</b>	<b>The role of CISO in the evolving new frontiers of cybersecurity regulations</b>	
	<p><b>Chuks Ojeme</b>, Global Chief Information Security &amp; Compliance Officer, Brenntag</p> <ul style="list-style-type: none"> <li>• NIS2: What does it imply?</li> <li>• How does it affect the role of a CISO</li> <li>• Regulations and geo-politics, the impact on cyber-risk management</li> </ul>	
<b>14:50</b>	<b>It's all about readiness! Why you may have been doing cyber-training wrong!</b>	
	<p><b>Rupert Collier</b>, VP Global Sales, RangeForce</p> <p>Rupert will provide some insights into the following:</p> <ul style="list-style-type: none"> <li>• How realistic, hands-on, simulation-based readiness training helps companies elevate cyber-skills, fill specialist staffing gaps, and save training budget</li> <li>• How and why a focussed, continuous, cyclical training programme called AR(2) uses a unique combination of self-paced learning and live-fire team exercises to improve their security team's ability to detect, contain, and remediate cyber-attacks</li> <li>• How and why this approach is much more effective and efficient than old fashioned classroom-based, instructor-led, certification-centric methodologies</li> <li>• How some other German customers have seen huge benefits for their SOC and cyber-defence teams from the RangeForce platform</li> <li>• How RangeForce makes it easier to personalise relevant training for larger teams with a diverse range of backgrounds and skill sets</li> </ul>	
<b>15:10</b>	<b>The challenges of NIS2: Just compliant or also secured?</b>	
	<p><b>Nikolei Steinhage</b>, Enterprise Sales Engineer DACH, CrowdStrike</p> <p>NIS2 stellt viele Unternehmen vor enorme Herausforderungen. Statt NIS2 einfach nur als eine Compliance-Anforderung zu betrachten, wollen wir zwei Fragen in den Mittelpunkt stellen:</p> <ul style="list-style-type: none"> <li>• Wie kann man die Anforderungen schnell umsetzen (time-to-value)?</li> <li>• Wie kann man NIS2 nutzen, um flexible auf zukünftige Herausforderungen reagieren zu können?</li> <li>• Wie lassen sich trotz NIS2 Kosten sparen?</li> </ul>	
<b>15:30</b>	<b>Education Seminars   Session 3</b>	
	<p><b>JT Global</b>  <b>Fraud prevention, AML, and KYC with mobile intelligence</b>  <b>Gerhard Sahner</b>, Business Development Mobile Intelligence, JT Global</p>	<p><b>Red Sift</b>  <b>The anatomy of online fraud: How AI is changing the battlefield in favour of the attacker and what we can do about it</b>  <b>Julian Wulff</b>, Director, Cyber Security Central Europe, Red Sift</p>
<b>16:10</b>	Networking break	
<b>16:30</b>	<b>Why CISOs should care about resilience</b>	
	<p><b>Dr. Timo Wandhöfer</b>, Group CISO, Klöckner &amp; Co</p> <ul style="list-style-type: none"> <li>• Resilience is what you need when security has failed its DR and BCP. So what is the role of the CISO in these activities?</li> <li>• If companies assume successful hacks, then should they divert resources away from security that is doomed to fail to DR/BCP?</li> <li>• Shouldn't we be taking a different approach to security itself: should CISOs focus on protecting key business processes not simply data?</li> <li>• What do CISOs bring to the resilience party?</li> </ul>	
<b>16:50</b>	<b>CISO Panel Discussion</b>	
	<p><b>Chuks Ojeme</b>, Global Chief Information Security &amp; Compliance Officer, Brenntag (Moderator);  <b>Gulnara Hein</b>, CISO, Chintai;  <b>Moona Ederveen-Schneider</b>, Executive Director EMEA, FS-ISAC;  <b>Riccardo Riccobane</b>, Head of CSO Security Assurance &amp; Head of Operational Resilience, DWS;  <b>Ashar Javed</b>, Head of Security Technology – Security Technology Section, Hyundai AutoEver Europe GmbH</p> <ul style="list-style-type: none"> <li>• Integrating cybersecurity into wider enterprise risk management frameworks</li> <li>• Becoming a more strategic partner to the business?</li> <li>• Building resilience against third-party security threats</li> <li>• Web 3.0 and the next generation of the internet: securing new technologies and services</li> <li>• Preparing for NIS2</li> </ul>	
<b>17:30</b>	Conference close	

Education Seminars	
<p><b>JT Global</b></p> <p><b>Fraud prevention, AML, and KYC with mobile intelligence</b></p> <p><b>Gerhard Sahner</b>, Business Development Mobile Intelligence, JT Global</p>	<p>The use of real-time mobile intelligence data for customer authentication based on verified subscriber data from mobile network operators enables a higher level of security, especially in the fields of finance and e-business. These mobile data are already being used to establish robust cybersecurity measures, combat cybercrime, and reduce risks associated with mobile fraud. Additionally, they provide the ability to verify SIM integrity, identify high-risk transactions, and conduct age verification. Furthermore, they contribute to assessing the creditworthiness of customers for Buy Now, Pay Later (BNPL) and credit services. Gerhard Sahner's (Jersey Telecom) presentation offers an interesting overview of the various possibilities of this innovative technology.</p>
<p><b>Menlo Security</b></p> <p><b>Browser security – the proven prevention layer for enterprise cybersecurity</b></p> <p><b>Tom McVey</b>, Solution Architect, Menlo Security</p>	<p>According to Google, 98% of attacks originate from internet usage and 80% of those target end user browsers – sadly all too successfully. Combine this stark reality, with users' relentless demand for new SaaS and private applications, often collaborating with external stakeholders, and security pros are always running to stand still.</p> <p><b>Join us for a practical session where we will cover:</b></p> <ul style="list-style-type: none"> <li>• <b>Security</b> – The proven value of robust browser security across managed and unmanaged devices – automating browser configuration and establishing enhanced browser forensics</li> <li>• <b>Connectivity</b> – Your users and third parties need access to SaaS applications, private web apps and data, including the use of GenAI. We share how organisations are enhancing user protection and productivity while reducing the cost and complexity of solutions such as VDI</li> <li>• <b>Compliance</b> – How browser security supports organisations striving to comply with key NIS 2 requirements for incident management and prevention</li> </ul> <p>We will provide real world examples of how to increase cyber-prevention through improved browser security including a case study of a major German car manufacturer.</p>
<p><b>Recorded Future</b></p> <p><b>Insights into the dark web: cybercrime forums, markets and threats to watch out for</b></p> <p><b>Bernd Knippers</b>, Senior Sales Engineer DACH, Recorded Future</p>	<p>The dark web is a hidden area of the World Wide Web and operates through specialised software that allows users and websites to remain anonymous. In this presentation, we will discuss the nature of the dark web and the potential threats it poses, as well as appropriate detection and defence strategies through applied threat intelligence.</p>
<p><b>Red Sift</b></p> <p><b>The anatomy of online fraud: How AI is changing the battlefield in favour of the attacker and what we can do about it</b></p> <p><b>Julian Wulff</b>, Director, Cyber Security Central Europe, Red Sift</p>	<p>There are a few key components in the making of online fraud. Some of these elements are becoming an order of magnitude faster to execute for attackers thanks to Generative AI. But not everything about this new technology is a gift to attackers, and there are some common-sense things that organisations can do to defend themselves more effectively.</p> <ul style="list-style-type: none"> <li>• What makes a very effective online fraud?</li> <li>• How is Generative AI accelerating and making fraud easier to carry out effectively?</li> <li>• What actions can we take to counteract this? How can defenders use Generative AI themselves?</li> </ul>

Education Seminars	
<p><b>SpyCloud</b></p> <p><b>Ransomware revealed: The changing landscape of ransomware and data exploitation</b></p> <p><b>Christian Buhrow</b>, Regional Sales Director, SpyCloud</p>	<ul style="list-style-type: none"> <li>• Trends in the shifting ransomware landscape, including frequency of attacks, costs to organisations, and emerging new threats to be aware of</li> <li>• The riskiest entry points, as well as the connection between specific infostealer malware infections and the probability that a company will subsequently experience a ransomware event</li> <li>• Gaps in remediation that are contributing to a proliferation of entry points for follow-on ransomware attacks</li> <li>• A live demonstration on how to turn recaptured darknet data into your greatest defence against ransomware, next gen account takeover &amp; online fraud</li> </ul>
<p><b>SUSE</b></p> <p><b>Network traffic visibility &amp; zero trust security in Kubernetes environments</b></p> <p><b>Bettina Bassermann</b>, Business Strategist, Pre-Sales DACH, SUSE Software Solutions Germany GmbH</p>	<p>Deep network visibility is the most important part of container security at runtime.</p> <p>With traditional perimeter-based security, administrators use firewalls to isolate or block attacks before they reach the workload. Inspecting container network traffic reveals how an application communicates with other applications and is the only way to stop attacks before they reach the application or workload. NeuVector is the only 100% open source security platform for containers with continuous auditing throughout the lifecycle.</p> <ul style="list-style-type: none"> <li>• Supply chain security</li> <li>• Vulnerability and compliance management</li> <li>• Zero-day attack prevention</li> <li>• Perform Deep Packet Inspection (DPI)</li> <li>• Monitor east-west and north-south container traffic</li> </ul>