Post event report

The 20th e-Crime & Cybersecurity Germany

18th January 2023 | Frankfurt, Germany

Strategic Sponsors

BeyondTrust

corelight

LastPass

MANDIANT NOW PART OF Google Cloud

proofpoint

SECLORE

Education Seminar Sponsors

CROWDSTRIKE

FORESCOUT

RAPID7

RELIAQUEST

Networking Sponsors

mnemonic

Branding Sponsors

RED BUTTON DDoS Experts

> “I found the day very interesting, as always. My conclusion would then be: e-Crime offers a great mix of lectures, from information on the subject of threat risks to the best products to protect yourself. Networking opportunities are of course always the best. The lecture from the BSI was particularly interesting from a different perspective, instead of always dealing with day-to-day business to get busy.”

Head of Development

> “As always, the e-Crime Congress in Frankfurt was a very good event, with very good speakers and lectures, and an excellent supporting programme (industrial exhibition and catering) – I really liked it. Keep it up!”

Business Information Security Officer

> “Many thanks for the valuable and very well organised event. For me personally, the following lectures were the most valuable:
> - Forescout: “Why automated visibility...”
> - Client: “Why threat intel for your company too...”
> - ReliaQuest: “The future of security operations...””

Leader CERT Team

> “Many thanks. I really liked the event again and, although AKJ Associates has held excellent digital events in recent years, the face-to-face format is better suited for networking in addition to dealing with the content of the topics. I was able to have very good conversations again. It's nice that the BSI was represented with its annual report and the other contributions also gave me plenty of impetus for the challenges of 2023.”

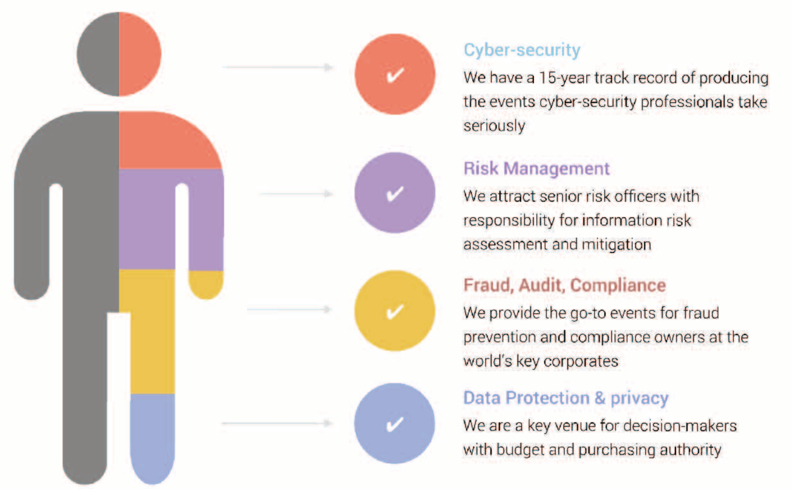
CISO

Inside this report:

Key themes

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

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

Peter Aicher,
Senior Security Solutions Engineer
Rapid7

Florian Augthun,
Senior Cybersecurity Architect
Ströer

Babak Badkube,
Head of DACH G2M & Sales
Reliaquest

Moona Ederveen-Schneider,
Executive Director Europe
FS-ISAC

Francisco Z. Gaspar,
Lead CyberSecurity Architect
Telefónica Germany

Sybil Kleinmichel,
Group Information Security Officer
Citigroup Global Markets Europe AG

Christian Husemeyer,
Consulting Systems Engineer
Mandiant

Isabel Muench, Head of IT – Security Situational Awareness
Federal Office for Security in Information Technology (BSI)

Chuks Ojeme, Global Chief Information Security and Compliance Officer
Brenntag

Christoph Pontau, Solutions Engineer
BeyondTrust

Dr. Dominik Raub,
Chief Information Security Officer
Crypto Finance AG

Ralf Schmitz
Corelight

Jasbir Singh,
Partner and Managing Director Europe
Seclore Technologies

Bert Skaletski, Resident CISO, EMEA
Proofpoint

Peter van Zeist,
Principal Solutions Consultant
LastPass

Sven von Kreyfeld,
Senior Cybersecurity Consultant
Forescout

Dr. Timo Wandhöfer,
Chief Information Security Officer
Deutsche WertpapierService Bank AG

Nicolas Wehmeyer, Services Sales Manager, Central & Eastern Europe
CrowdStrike

Agenda

08:00	Registration and networking break
08:50	Chairman's welcome
09:00	**The most important findings about cyber-threats for Germany** **Isabel Muench,** Head of IT – Security Situational Awareness, Federal Office for Security in Information Technology (BSI) • Analysis of the evolving threat landscape – danger signals for CISOs • Information from the most important incidents • Suggestions on where the focus of security measures should be
09:20	**Data-centric security for data protection | Every Digital Asset | Everywhere** **Jasbir Singh,** Partner and Managing Director Europe, Seclore Technologies In this session we will explore: • How to protect your organisation against insider threats • How to ensure secure collaboration • Mitigating third-party risk by protecting your data everywhere • Data-centric security as a cornerstone to staying compliant
09:40	**Network transparency with Open NDR** **Ralf Schmitz,** Corelight • Networks are the veins of modern businesses, and data is the lifeblood that flows through them. Networks carry all the applications and data needed to operate in today's digital world • With an Open Network Detection and Response solution, whether the exchange of data is on-premises or in the cloud, you can better understand your environment and ongoing attacks can be stopped and contained • The rich network data from the sensors, can be combined with advanced analytics capabilities, such as machine learning and analytics • This greatly simplifies workflows for analysts and frees up your team to respond to security incidents and search for undetected threats
10:00	**Regulation is the training wheels for real security** **Dr. Timo Wandhöfer,** Chief Information Security Officer, Deutsche WertpapierService Bank AG • What does regulation mean in the banking sector? • How has regulation changed? • Why is this trend important? • What can be learned from it for other industries?
10:20	**Education Seminars | Session 1** **Forescout** **Why automated visibility and classification should be the foundation of any mature IT security operation** **Sven von Kreyfeld,** Senior Cybersecurity Consultant, Forescout **Rapid7** **How Metasploit and Velociraptor is leading to one of the most agile SOCs** **Peter Aicher,** Senior Security Solutions Engineer, Rapid7
11:00	Networking break
11:30	**Securing client assets – in the context of escalating cyber-threat** **Dr. Dominik Raub,** Chief Information Security Officer, Crypto Finance AG • Blockchain vs classical assets from a cyber-threat exposure perspective • Information security threat landscape and securing client assets as central protection goals for a blockchain asset company • Using secure hardware and sound security architecture to mitigate risks and secure client assets • Residual risks to client assets and further recommended defences
11:50	**The remote access challenge – Is VPN obsolete?** **Christoph Pontau,** Solutions Engineer, BeyondTrust In this speaker session we explain: • How zero-trust networks can replace VPN solutions • How to implement a zero-trust solution in your organisation and the technologies Microsoft and other vendors have available for providing secure remote access to users • Replacing traditional VPN solutions with zero-trust • Most important steps to zero-trust maturity • Zero-trust for privileged account access
12:10	**The human security gap – How bad password habits endanger your company** **Peter van Zeist,** Principal Solutions Consultant, LastPass • Which behaviour of your employees leads to security gaps • How to find unsafe passwords and stop using them • How to establish a password management that not only closes security gaps, but also engages all employees

Agenda

12:30 **Education Seminars | Session 2**

CrowdStrike
How managed services effectively protect organisations from threats
Nicolas Wehmeyer, Services Sales Manager, Central & Eastern Europe, CrowdStrike

Reliaquest
The future of security operations: Threat intelligence, automation, and data-stitching
Babak Badkube, Head of DACH G2M & Sales, Reliaquest

13:10 Lunch and networking break

14:00 **EXECUTIVE PANEL DISCUSSION** **Information security domain and defining protection requirements**

Moderated by Sybil Kleinmichel, Group Information Security Officer, Citigroup Global Markets Europe AG;
Dr. Timo Wandhöfer, Chief Information Security Officer, Deutsche WertpapierService Bank AG;
Dr. Dominik Raub, Chief Information Security Officer, Crypto Finance AG

- Peer review of 'Information Domain' – calibrating our definitions
- How to define the scope of a cybersecurity management system
- Protection requirements – defending the best
- DACH CISO knowledge sharing

14:30 **Why threat intel is relevant for your organisation – Mandiant & Google Cloud join forces**

Christian Husemeyer, Consulting Systems Engineer, Mandiant

- Traditional focus of CTI-teams: WHO is targeting us WHY? And HOW will they attack us?
- But: Requirements of Mandiant CTI-customers are getting more and more specific recently:
- Which TTPs (mapped to MITRE ATT&CK) are relevant for me? Are there targeted campaigns against my org or vertical?
- TIBER assessments, customised intelligence-reports, benchmarking of CTI capabilities, support in training/CTI capability development…
- Outlook: Added value customers can expect from the combined Intel-sources and analysis-capabilities of Mandiant and Google going forward

14:50 **Protecting people. Defending data**

Bert Skaletski, Resident CISO, EMEA, Proofpoint

- Protect people. Defend data
- Follow a people-centric approach for your security

15:10 **The mindset, tactics of threat actors and building resilience**

Chuks Ojeme, Global Chief Information Security and Compliance Officer, Brenntag

- How threat actors choose their targets
- Launching and coordinating the attack process
- Responding to an escalating infiltration

15:30 Networking break

16:00 **Is it safe now?**

Florian Augthun, Senior Cybersecurity Architect, Ströer

- Is security finally sorted? If so what about all the latest acronyms DLP, APT or IDS – just hype?
- Don't forget or underestimate security basics
- Why the human factor should be central in security organisations

16:20 **EXECUTIVE PANEL DISCUSSION** **Future challenges**

Moderated by Chuks Ojeme, Global Chief Information Security and Compliance Officer, Brenntag;
Dr. Timo Wandhöfer, Chief Information Security Officer, Deutsche WertpapierService Bank AG;
Moona Ederveen-Schneider, Executive Director Europe, FS-ISAC;
Francisco Z. Gaspar, Lead CyberSecurity Architect, Telefónica Germany

Stepping back from the day-to-day necessities, what challenges in firms' digital environments cause greatest problems for the information security programme? How does the information security function mitigate and alleviate the burden on their IT and business colleagues to solve them? This panel will look at the challenges posed by:

- Overall technology landscape complexity
- 'Digital' transformations of the business/products
- Testing and measuring the effectiveness of the cybersecurity control environment
- Incident response and problem management
- Ensuring the same coverage/visibility over cloud environments as on-prem
- Managing supply chain risk in a world less tolerant to long delays around supplier assurance (post covid)
- Web 3.0 and the next generation of the internet: securing new technologies and services which are inherently decentralised?

16:50 Chairman's closing remarks

17:00 Conference close

Education Seminars	
CrowdStrike **How managed services effectively protect organisations from threats** **Nicolas Wehmeyer,** Services Sales Manager, Central & Eastern Europe, CrowdStrike	Implementing an effective endpoint security programme practically can be difficult. The necessary tools often require detailed knowledge. In addition, proper implementation, support and maintenance often require extensive resources. As a result, many organisations and institutions fail to get the most out of the endpoint security technologies they acquire. Learn how to save resources for other value-added activities in this training session. Key topics: • Insights on the current threat landscape from the perspective of the CrowdStrike Threat Hunting and Overwatch teams • The difference between MDR and EDR and how you can benefit from them • How MDR Services protect organisations worldwide from threats • How MDR Services work with organisations' own resources and SOCs
Forescout **Why automated visibility and classification should be the foundation of any mature IT security operation** **Sven von Kreyfeld,** Senior Cybersecurity Consultant, Forescout	Increasingly complex, dynamic and distributed IT infrastructures pose a challenge for any IT security team. This is compounded by the fact that qualified IT security professionals are often scarce and expensive. Limited visibility and poor integration of security solutions compound this challenge, adding manual processes to an already overburdened security team. In this presentation, we would like to show how an automation solution can help to reduce complexity in IT security and at the same time help to establish real-time transparency, classification and controls. This allows IT security teams to focus on more important tasks/ improving IT security. In this session, we will cover: • How to achieve real-time, unified visibility of all connected assets across IT, OT, and IoT environments • How automatic classification of all connected assets forms the basis for security controls and compliance management • How integration with third-party security solutions and ITSM can orchestrate system-wide response to attacks or non-compliance
Rapid7 **How Metasploit and Velociraptor is leading to one of the most agile SOCs** **Peter Aicher,** Senior Security Solutions Engineer, Rapid7	Cybersecurity can only work together! Rapid7 is widely known in the cybersecurity community with its Metasploit and Velociraptor projects, among others. We believe that security is the responsibility of all technology users, vendors and integrators and that collaboration is the only way to achieve long-term change. Rapid7 shares security information and tools gained widely within the community to help our counterparts learn, grow and develop new skills, and support each other in addressing and tackling issues affecting cybersecurity. A collaboration of equals. From which everyone ultimately benefits. In this seminar, you will learn: • How the experience gained from our Metasploit and Velociraptor projects leads to one of the most agile SOCs • In which technologies the gained experience can be used profitably • How the insights are made available to our customers for easy use

Education Seminars	
Reliaquest **The future of security operations: Threat intelligence, automation, and data-stitching** **Babak Badkube,** Head of DACH G2M & Sales, Reliaquest	Enterprises are working to get the ROI out of their existing tools as well as accelerate their ability to detect, investigate, and respond. In attempting to accomplish these two goals, enterprises are considering a single data lake that stores their security data. There are several challenges with this approach from additional costs of data egress from cloud providers to the simple fact that the enterprise data will never be in one place. At ReliaQuest, we take a different approach using data-stitching and distributed investigations. In this talk, we will discuss the pros and cons of centralising security data and how an approach of data stitching solves those challenges. • Security operations today • Security’s ‘big data’ problem • Data lakes vs Data stitching • Security operations platform • Data stitching in action