Post event report

Strategic Sponsors

CLOUDFLARE

corelight

CROWDSTRIKE

GATEWATCHER

MANDIANT | Google Cloud

paloalto NETWORKS

proofpoint.

Education Seminar Sponsors

b!nalyze

Cribl

Recorded Future®

RED SIFT

RELIAQUEST

SUSE

Networking Sponsor

mimecast

Branding Sponsors

netskope

Lookout

> “Finally a cybersecurity congress with high relevance and high content density, very informative. The topics are up-to-date and valuable, no overlaps, covering lot of topics from network to user to kubernetes security. Exhibitors and sponsors are relaxed and professional. Pleasant networking of the participants, great exchange. From now on, this event will be on my calendar regularly. See you next year.”
>
> **IT Operations & Projects, Bavaria Film**

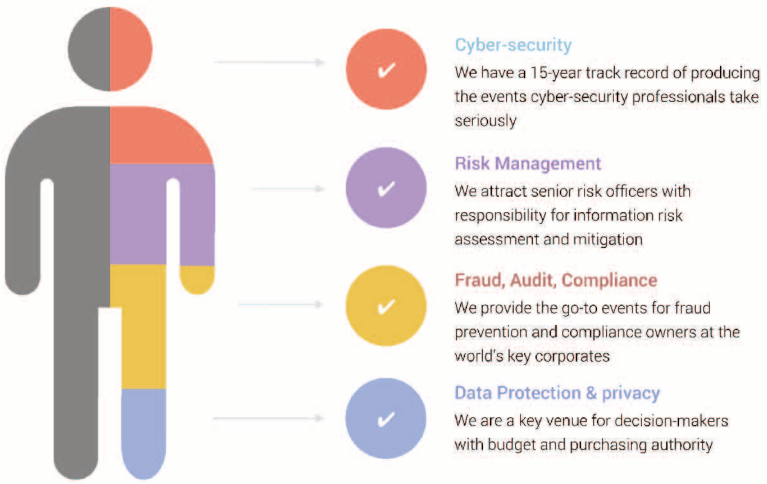
> “The recent e-Crime & Cybersecurity Congress brought together in-depth analyses of current threats and practical solutions. The programme, consisting of technical workshops, lectures and networking opportunities, was well structured and up-to-date. The thematic breadth of the lectures, presented by industry experts, was impressive. The workshops offered participants the opportunity to gain hands-on experience and learn new skills. The exchange during the networking sessions was valuable, new contacts were made and existing relationships were deepened. Overall, the Congress was a rewarding experience for IT professionals; one looks forward to the next event with anticipation.”
>
> **Senior Cyber Security Engineer, Flughafen München**

Inside this report:

Key themes

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

Who attended?



Speakers

Monika Atanasova, Global Head of Cyber TPRM, Raiffeisen Group – Switzerland

Ali Baccouche, Information Security & Data Privacy Officer - EMEA, Texas Instruments

Babak Badkube, Head of DACH G2M & Sales, ReliaQuest

Andreas Bechter, Solutions Engineer Strategic, Cloudflare

Maximilian Bode, Consulting Sales Engineer, Mandiant

Fabrice Delouche, Europe Senior Sales Director, Binalyze

Matt Ellison, Director of Sales Engineering EMEA and APAC, Corelight

Andreas Englisch, Chief Information Security Officer, AssetMetrix

Francisco Z. Gaspar, Lead Cybersecurity Architect, Telefónica Germany

Gerald Hahn, Country Manager for DACH, Central and Eastern Europe, Gatewatcher

Oliver Hoppe, Technical Architect, Cribl

Max Imbiel, Deputy Group CISO, N26

Sreedevi Jay, Head of Cyber Threat Unit for EU, PagoNxt

Oliver Karow, Director Technical Sales, Proofpoint

Bernd Knippers, Senior Sales Engineer DACH, Recorded Future

Peter Leimgruber, Manager Systems Engineering, Palo Alto Networks

Peter Machat, Vice President, DACH, Red Sift

Holger Moenius, NeuVector Sales Executive DACH, Benelux, Nordics & South, SUSE

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

Rainer Rehm, Information Security Officer, Zooplus AG

Christian Schramm, Sales Engineer, CrowdStrike

Andrea Szeiler, Global CISO, Transcom

Agenda	
08:00	Registration and networking break
08:50	Chairman's ¨
09:00	**Third-party risk management from a third-party perspective** **Andrea Szeiler,** Global CISO, Transcom • Understanding your third parties and the risks they bring to your organisation • Different approaches to third-party risk management and their pros and cons • Responsibility sharing matrix • Working together
09:20	**Why is SASE and Zero Trust so successful?** **Peter Leimgruber,** Manager Systems Engineering, Palo Alto Networks • 'Zero Trust' as a security concept is not only obvious for security experts • SASE solves the challenges of user mobility and distributed locations • A consistent, comprehensive set of rules for every user and all applications • A security solution against which each attack can only be used once is very expensive for attackers!
09:40	**The cyber-threat landscape Germany** **Andreas Bechter,** Solutions Engineer Strategic, Cloudflare • Cyber-threat landscape Internet and Germany • Why employee security training falls short • What you can do today to shut down one of the biggest attack vectors
10:00	**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
10:20	**Education Seminars | Session 1** **Cribl** **How to optimise your security data and reduce SOC TCO with data pipelines** **Oliver Hoppe,** Technical Architect, Cribl **SUSE** **Importance of Zero Trust security in Kubernetes environments** **Holger Moenius,** NeuVector Sales Executive DACH, Benelux, Nordics & South, SUSE
11:00	Networking break
11:30	**FIRESIDE CHAT: Shaping the future of cyber TPRM by unlocking the potential of automation & digitalisation – Lessons learned & best practices, case study** **Monika Atanasova,** Global Head of Cyber TPRM, Raiffeisen Group – Switzerland • Main aspects of the cyber TPRM programme • Security assessments workflow automation • Comprehensive cyber TPRM profiling • Reporting: KPIs/KRIs cyber risk cockpit • AI & threat intelligence
11:50	**Risk factor supply chain attacks** **Oliver Karow,** Director Technical Sales, Proofpoint • What are the most common tactics used in supply chain attacks and what ways and means do attackers use? • How can you prepare your company and effectively defend against attacks? • What are the benefits of proactive monitoring?
12:10	**By the numbers of today's top cyber-trends and attacks** **Maximilian Bode,** Consulting Sales Engineer, Mandiant • A look back at Mandiant's Incident Response investigations in 2022 • 2023 conclusions and trends • Interesting results from RedTeaming and cloud assessments

Agenda

12:30 — Shake the box: Understanding network evidence in an encrypted and containerised world

Matt Ellison, Director of Sales Engineering EMEA and APAC, Corelight

- The network was easy to study and provided defenders a compelling vantage point
- Today's networks are significantly more complex – greater complexity & greater risk
- Does network monitoring still offer defenders a compelling vantage point?
- Understand why network evidence is a critical element in any balanced defensive strategy

12:50 — Education Seminars | Session 2

Recorded Future **Infostealer malware – Why is it not enough to be aware of leaked credentials?** **Bernd Knippers,** Senior Sales Engineer DACH, Recorded Future	Red Sift **You can't fight the invisible – Let us check your attack surface** **Peter Machat,** Vice President, DACH, Red Sift

13:30 — Lunch and networking break

14:30 — Canaries: Deciding on the undecidable

Andreas Englisch, Chief Information Security Officer, AssetMetrix

- The 'decision problem' in IT security
- False positives vs False negatives: Pick your poison
- Rookie CISO's dilemma
- Canaries as an underrated class of detective controls
- why Canaries can Help Small Companies more than honeypots

14:50 — The network does not lie – Network analysis, the power of connection

Gerald Hahn, Country Manager for DACH, Central and Eastern Europe, Gatewatcher

- Network traffic monitoring
- Threat identification
- Optimisation of security operations
- Real-time response to attacks
- Increase cyber-resilience

15:10 — From relentless adversaries to resilient businesses

Christian Schramm, Sales Engineer, Crowdstrike

- We will share with you the latest insights, trends and current events from the threat landscape
- Learn how attacker activity has evolved in 2022
- Here's what our predictions look like for 2023

15:30 — Education Seminars | Session 3

Binalyze **The growing role of DFIR in resilient incident response strategies** **Fabrice Delouche,** Europe Senior Sales Director, Binalyze	ReliaQuest **The future of security operations: Threat intelligence, automation, and data-stitching** **Babak Badkube,** Head of DACH G2M & Sales, ReliaQuest

16:10 — Networking break

16:30 — EXECUTIVE PANEL DISCUSSION — CISO priorities

Max Imbiel, Deputy Group CISO, N26 (Moderator);
Sreedevi Jay, Head of Cyber Threat Unit for EU, PagoNxt;
Francisco Z. Gaspar, Lead Cybersecurity Architect, Telefónica Germany;
Ali Baccouche, Information Security & Data Privacy Officer - EMEA, Texas Instruments;
Rainer Rehm, Information Security Officer, Zooplus AG

- How does legacy cybersecurity thinking and technology have to change?
- Prioritising cybersecurity initiatives in the absence of any easy way to quantify cyber-risks
- How much is enough? Are CISOs under budget pressure? Is there pressure to outsource?
- The cyber-talent shortage – real or illusion?

17:10 — Conference close

Education Seminars	
Binalyze **The growing role of DFIR in resilient incident response strategies** **Fabrice Delouche,** Europe Senior Sales Director, Binalyze	• Cybersecurity and the growing revolution powered by DFIR • The benefits of speed and automation with DFIR • Leveraging DFIR to reduce caseloads, dwell time, and alert fatigue • Empowerment, resilience, and enhanced security posture thanks to DFIR
Cribl **How to optimise your security data and reduce SOC TCO with data pipelines** **Oliver Hoppe,** Technical Architect, Cribl	Managing the flood of noisy, high-volume security data (logs, events, traces etc.) means the difference between detecting a breach and missing a critical alert. This session will explore how 'data pipelines' put choice and control over data back into the hands of security teams, helping get the right data, in the right formats, to the right places, all while reducing your SOC TCO and overall security data management complexity. Key topics and takeaways during this seminar include: • How to streamline onboarding and routing of new data sources into your SIEM/XDR platforms without complexity or increased costs • How to enrich security data in real time with threat intel, GeoIP, asset information and more for faster threat response • How to collect, filter, redact, normalise, transform, and route data from any source to any destination within your existing data infrastructure • How to eliminate vendor lock-in and control your data storage, formatting, and processing
Recorded Future **Infostealer malware – Why is it not enough to be aware of leaked credentials?** **Bernd Knippers,** Senior Sales Engineer DACH, Recorded Future	The presentation will discuss Infostealer malware and cover the following topics: • Various forms of Infostealer malware, their distribution, threat potential and ways to protect against them • Why being aware of leaked credentials is not enough to protect against Info Stealer malware • Why existing security controls like MFA are no longer sufficient to deal with the growing threat of Infostealer malware • Importance of modern intelligence to address modern threats
Red Sift **You can't fight the invisible – Let us check your attack surface** **Peter Machat,** Vice President, DACH, Red Sift	Have you ever been affected by an expired SSL or certificate taking down your website or service? Did you ever pay an invoice because of a phishing email? Did one of your suppliers or customers respond and act on an email, because it looked like you had sent it? It might not have happened to you yet, but you might know someone who has been affected. Join us to understand how Red Sift's platform helps you to: • Stop phishing and spoofing emails before they happen • Get a full picture of your public facing assets incl. certificates • Understand why CTEM (Continuous Threat Exposure Management) is something organisation's need to be addressing now

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
SUSE **Importance of Zero Trust security in Kubernetes environments** **Holger Moenius,** NeuVector Sales Executive DACH, Benelux, Nordics & South, SUSE	Deep network visibility is the most critical part of run-time container security. In traditional perimeter-based security, administrators deploy firewalls to quarantine or block attacks before they reach the workload. Inspecting container network traffic reveals how an application communicates with other applications and it's the only place that can stop attacks before they reach the application or workload. SUSE NeuVector is the only 100% open source Zero Trust container security platform with continuous audits throughout the full lifecycle. • Perform Deep Packet Inspection (DPI) • Real-time protection with the industry's only container firewall • Monitor 'east-west' and 'north-south' container traffic • Capture packets for debugging and threat investigation