Post event report

The 23rd e-Crime & Cybersecurity Germany

11th June 2024 | Munich, Germany

Strategic Sponsors

Akamai

ANOMALI®

ARMIS®

netskope®

paloalto NETWORKS

proofpoint®

rubrik

SUSE

Education Seminar Sponsors

b!nalyze

BRANDEFENSE

cradlepoint
PART OF ERICSSON

SUSE

Networking Sponsor

CybelAngel

66 It was a great event and I participated in all sessions during the day. Looking forward to available slides from the speakers. Thanks again for the invitation and great organisation of the event! 99
Vice President Engineering, Akirolabs

66 Lots of interesting and new topics, good selection of speakers and panellists. The conversations during the breaks were also helpful and stimulating. I will definitely be back next year, possibly with my own presentation again. As always, the location was perfectly chosen and prepared. 99
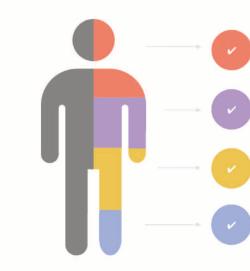**Head of Security, SKY Deutschland**

Key themes

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 come the cybersecurity regulators

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?

NIS2 – changing the game in cybersecurity?

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

Thomas Barkias, Principal Supervisor – Cyber Resilience, ICT, Crypto & Operational Risk,
European Central Bank

Marcel Alexander Bayer, Named Account Manager, **Proofpoint**

Michele De Donno, Ethical Hacker, **Sky Deutschland GmbH**

Francisco Z. Gaspar, Lead Cybersecurity Architect, **Telefónica Germany**

André Heller, Director Solution Architects DACH, **Armis**

Max Imbiel, CISO, **Bitpanda Asset Management**

Steve Jackson, Senior Vice President of Growth, **Binalyze**

Sreedevi Jay, Head of Cyber Threat Unit for EU,
PagoNxt (A Santander Company)

Sheetal Joseph, Director, Cybersecurity, **Isar Aerospace**

Klaus-E. Klingner, Information Security Officer, **Assambeauty**

Frank Lange, Technical Director, EMEA, **Anomali**

Seamus Lennon, Vice President of Operations for EMEA, **ThreatLocker**

Ivan Majdan, Regional Sales Manager CEUR, Security Division,
Cradlepoint by Ericsson

Ralf Mutzke, Director Cyber Security, **Aon Deutschland**

Mahmut Kamil Özrenk, Sr. Pre-Sales Engineer, **Brandefense**

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

André Reichow-Prehn, Managing Partner, EMEA, **Palo Alto Networks**

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

Simon Riehle, Sales Engineer, Proofpoint

Florian Rutsch, Sr. Sales Engineer Consultant CEUR, Security Division,
Cradlepoint by Ericsson

Stefan Schmugge, Director Sales Engineering, **Rubrik**

Frank Sommer, Senior Solutions Engineer, **Akamai**

Gabriel Stein, System Engineer, **SUSE**

Agenda

08:00	Breakfast & networking break
08:50	Chairman's welcome

09:00 — Beyond DORA compliance: Orchestrating digital resilience in a VUCA environment

Thomas Barkias, Principal Supervisor – Cyber Resilience, ICT, Crypto & Operational Risk, European Central Bank
- Understanding the nuanced interplay of technology, processes, and human factors in achieving resilience
- Exploring ways and challenging in orchestrating resilience in today's VUCA environment
- Beyond compliance, emphasising the need for a holistic approach that transcends mere compliance with regulations like DORA

09:20 — Cybersecurity in the age of artificial intelligence: Will the promises of today emerge as powerful threats tomorrow?

André Reichow-Prehn, Managing Partner, EMEA, Palo Alto Networks
- Cyber-threats are emerging and for years among the top three risks on any executive board and government body risk list
- Threat intelligence is a base requirement in recent regulation and best practice
- Understanding and anticipating the threat landscape and capabilities of threat actors is crucial for risk-based decision-making and investing
- The presentation will provide a recent overview about the global and regional threat landscape, describe relevant use cases of the most notorious current threat actors and also the impact of new technologies like artificial intelligence on the threat landscape

09:40 — Why identity alone is not enough for a Zero Trust strategy

Paolo Passeri, Principal Sales Engineer and Cyber Intelligence Specialist, Netskope
- 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
- Learn why the context is important to enforce a granular and effective security policy
- Discover which are the elements that must be considered, besides identity, to adopt an effective Zero Trust strategy
- Understand how the different security controls, such as data protection, threat protection, behaviour analytics, cooperate to protect the modern enterprise

10:00 — Security 3.0 – Learnings from modern medicine and longevity

Max Imbiel, CISO, Bitpanda Asset Management
- What do security and medicine have in common?
- What thoughts and best-practices can we transfer from modern medicine into modern security?
- Applying healthier and more secure ways or working

10:20 — Education Seminars | Session 1

Cradlepoint by Ericsson	**SUSE**
How 5G is going to play a crucial role, and how can we plan its adoption with an integrated Zero Trust cybersecurity approach?	**We need to talk about security in our containerised workloads**
Ivan Majdan, Regional Sales Manager CEUR, Security Division, Cradlepoint by Ericsson & **Florian Rutsch,** Sr. Sales Engineer Consultant CEUR, Security Division, Cradlepoint by Ericsson	**Gabriel Stein,** System Engineer, SUSE

11:00	Networking break

11:30 — Beyond the buzzwords, AI's double-edged sword

Francisco Z. Gaspar, Lead Cybersecurity Architect, Telefónica Germany
- Understanding the evolution of cybersecurity paradigms
- The complexities of the data dilemma
- AI's promises and pitfalls – the balancing act
- Charting the course towards a more resilient and secure future

11:50 — Why established defences like web application firewall or API gateways are not enough to protect today's APIs

Frank Sommer, Senior Solutions Engineer, Akamai
- Why are APIs increasingly used?
- What does this mean for the security department in companies?
- Why are web application firewalls and API gateways not enough?
- What is needed to secure APIs?

12:10 — Why 24 is the answer to all questions in the cybersecurity environment!

Stefan Schmugge, Director Sales Engineering, Rubrik
- Do you know the difference: resilience or resistance? How do resilience and resistance differ in data security and which is really more effective for companies?
- Are cyber-incidents really the biggest business risk? Why are cyber-risks increasingly becoming a focal point in management and what does this mean for companies?
- 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?
- How can we do it better? What strategies are there to not only minimise the risk of a cyber-attack, but also to mitigate its possible consequences?

Agenda

12:30	**Identify vulnerable assets and prioritise remediation**
	André Heller, Director Solution Architects DACH, Armis • Identify vulnerabilities across all types of connected devices, managed or unmanaged • Prioritise the vulnerabilities that pose the highest risk to your business • Build an AI-based early warning system that identifies attacks on your company before vulnerabilities (CVEs) are disclosed
12:50	**Education Seminars | Session 2**

Binalyze	**Brandefense**
Resolving incident response challenges in your SOC with automation, speed, and collaboration **Steve Jackson,** Senior Vice President of Growth, Binalyze	**Beyond the dark: A guide to secure your brand in the digital underworld** **Mahmut Kamil Özrenk,** Sr. Pre-Sales Engineer, Brandefense

13:30	Lunch & networking break
14:30	**Managing third-party breaches**
	Riccardo Riccobene, Head of CSO Security Assurance & Head of Operational Resilience, DWS • Restoration and post-recovery steps • Legal terms and conditions and resulting due diligence • Data restoration and best practice • Implementing security enhancements and lessons learnt
14:50	**Less cyber more people – putting people at the centre of your world (or cybersecurity strategy)**
	Simon Riehle, Sales Engineer, Proofpoint & **Marcel Alexander Bayer,** Named Account Manager, Proofpoint Being human-centric means placing humans at the centre of design, decision-making, and problem-solving processes. It involves understanding, empathising with, and prioritising the needs, preferences, and experiences of individuals. But how does that help us reduce our risk profile? • How can we consider the needs of each individual when we design our security strategy and deploy that next bit of tech? • How can we understand the needs of the individuals we are protecting? • How can we use it to improve our defences and mitigate risk? • How can we make it scale with limited resources? • How can we do more for less? In this session, we will share the secrets of an effective human-centric security strategy.
15:10	**How to create successful malware and defend with Zero Trust**
	Seamus Lennon, Vice President of Operations for EMEA, ThreatLocker • In a world where anyone can create successful malware or have AI generate it for them, it's important to know how malware can be successful so you can better defend • Starting from a default-deny posture, learn how adopting Zero Trust principles can keep your data safe and operations running regardless of hacking attempts by man or machine
15:30	**The expanding role of generative AI in accelerating elite SOC performance**
	Frank Lange, Technical Director, EMEA, Anomali • Today's challenges in security operations • Doing more with less: Practical security analytics use cases based on AI (demo) • The impact of AI on visibility, speed and scale in the modern SOC
15:50	Networking break
16:20	**Ethical hacking explained: Why you need ethical hackers in your organisation**
	Michele De Donno, Ethical Hacker, Sky Deutschland GmbH • Ethical hacking and penetration testing: what and why • Myths and misconceptions about ethical hacking • A glimpse into the penetration testing process • Penetration test (live demo)
16:40	**SENIOR LEADERSHIP PANEL DISCUSSION**
	Max Imbiel, CISO, Bitpanda Asset Management (Moderator); **Klaus-E. Klingner,** Information Security Officer, Assambeauty; **Ralf Mutzke,** Director Cyber Security, Aon Deutschland; **Sreedevi Jay,** Head of Cyber Threat Unit for EU, PagoNxt (A Santander Company) **Sheetal Joseph,** Director, Cybersecurity, Isar Aerospace • The role of the CISO as security regulation increases (NIS2, DORA etc.) • Compliance versus security as a true business driver • Ai – helping or hindering? • Adopting a risk-based approach to securing budgets

17:15	Closing remarks	**17:20**	Conference close

Education Seminars

Binalyze

Resolving incident response challenges in your SOC with automation, speed and collaboration

Steve Jackson, Senior Vice President of Growth, Binalyze

In an 'assume breach' world with increasing regulatory burden, Incident Response investigation capability is critical to protecting enterprise resiliency.

Attendees will learn:

- The specific challenges around operational security, SOC resources and welfare and the regulatory landscape
- How these challenges can be met head on through automation, collaboration and greater speed of investigation

Brandefense

Beyond the dark: A guide to secure your brand in the digital underworld

Mahmut Kamil Özrenk, Sr. Pre-Sales Engineer, Brandefense

In an increasingly interconnected world, the digital landscape presents both unprecedented opportunities and significant risks for brands. This presentation delves into the critical aspects of securing your brand amidst the evolving threats of the digital underworld. Join us as we go beyond the dark to illuminate the path to securing your brand in the digital age, equipping you with the knowledge and tools to protect your valuable assets against the ever-present threats of the digital underworld.

Attendees will learn:

- Credential suffering
- Ransomware groups
- Challenges

Cradlepoint by Ericsson

How 5G is going to play a crucial role, and how can we plan its adoption with an integrated Zero Trust cybersecurity approach?

Ivan Majdan, Regional Sales Manager CEUR, Security Division, Cradlepoint by Ericsson &
Florian Rutsch, Sr. Sales Engineer Consultant CEUR, Security, Cradlepoint by Ericsson

As cellular performance accelerates, 4G/5G WAN connectivity creates new opportunities for organisations to expand their business with fast, flexible and agile WWAN connections for IoT devices, vehicles, branch offices and users. So how do you plan for the adoption of 4G/5G WAN into the enterprise network? Cybersecurity is critical in a high-performance environment, especially protecting assets, sensitive data moving between remote locations, users, the Internet, SaaS and cloud applications. Learn how a cloud-based SASE solution with a zero-trust approach adapts to the cellular WAN.

SUSE

We need to talk about security in our containerised workloads

Gabriel Stein, System Engineer, SUSE

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.

What attendees will learn:

- Why are our standard tools are not enough
- Containerised workloads and security concerns
- Protecting your modern workloads