Post event report

Strategic Sponsors

BEYOND IDENTITY

deep instinct

KnowBe4 Human error. Conquered.

MANDIANT YOUR CYBERSECURITY ADVANTAGE

OneTrust PRIVACY, SECURITY & GOVERNANCE

Recorded Future®

SentinelOne™

Education Seminar Sponsors

CybelAngel

DEVO

GROUP-IB

illumio

CISCO KENNA Security

VECTRA®

Networking Sponsor

CROWDSTRIKE

Branding Sponsors

SECLORE

SOCRadar®

YogOsha

"A very good and informative event, which repeatedly handles very current and burning topics of information security, secure technical implementation and legal data protection in Germany. This is particularly well-suited for both beginners in the field of information security, who come from the technical environment of IT, for guidance, as well as for experienced colleagues in the field of information security. The networking is refreshing and varied, the vendors are carefully selected and always competent."

Data Security Officer, Bosch

"I really enjoyed the event. In addition to very interesting lectures, there were also opportunities for networking and excellent exchanges on specialist topics."

Bereichsleiter Datenschutz, Stadtsparkasse München

"I want to thank and congratulate AKJ Associates on a terrific e-Crime & Cybersecurity Congress. Your professionalism, along with the able support of all your sponsors, delivered a great event that was appreciated by all."

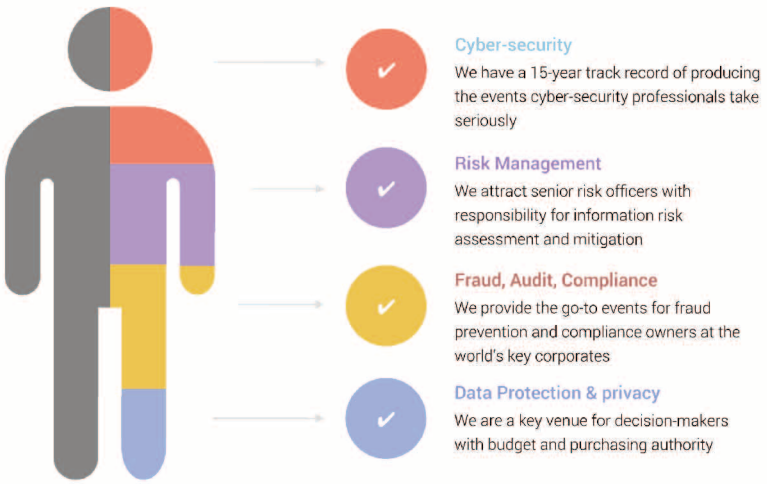
Group Information Security Officer, Citigroup

Inside this report:

Key themes

- Are we exaggerating cloud issues?
- From threat/security to risk/resilience
- What does DORA mean for you?
- Closing the cybersecurity skills gap
- Can zero trust be done?
- Is ransomware just going to keep getting worse?

Who attended?



Speakers

Maximilian Bode, Senior Sales Engineer, **Mandiant**

Kevin Boerner, Distinguished Sales Engineer EMEA, **Deep Instinct**

Matthias Canisius, Regional Sales Director CEE, **SentinelOne**

Ruben Caris, Anti Financial Crime – Liaison Office and Advanced Analytics, **HypoVereinsbank – UniCredit – Deutschland**

Camill Cebulla, Sales Director, Europe, **Group IB**

Marcquero Ermoza, Head of CyberSecurity Solution Engineering team, EMEA, **CybelAngel**

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

Alexander Goller, Senior Systems Engineer, **Illumio**

Dr. Rolf Häcker, CISO, **Landtag von Baden-Württemberg**

Marc Henauer, Head of Operation and Information Center MELANI, **National Center for Cyber Security (NCSC)**

Dr. Annegret Junker, Lead Architect, **Allianz**

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

Markus Klier, DACH Country Manager, **Devo**

Chris Meidinger, **Beyond Identity**

Dr. Annegret Junker, Lead Architect, **Allianz**

Matthias Schmauch, Regional Sales Manager, **Vectra AI**

Yao Schultz-Zheng, Former Digital Enterprise (Transformation) Architect, **BMW Group**

Rene Straube, TSA, **Cisco Kenna**

Turgut Tekkececi, Offering Specialist GRC, **OneTrust**

Thomas Wepner, Senior Corporate Security Officer, **Amadeus Group**

Jelle Wieringa, Security Awareness Advocate, EMEA, **KnowBe4**

Agenda

08:00 Registration and networking break

08:50 Chairman's welcome

09:00 **Current cyber-threats – (How) Can a 'responsible person' still sleep peacefully?**

Dr. Rolf Häcker, CISO, Landtag von Baden-Württemberg

- Current cyber-threats in the space
- Need for action-options for risk reduction
- External support for incidence response
- Conclusions

09:20 **Why legacy MFA is not good enough for modern authentication requirements**

Chris Meidinger, Beyond Identity

- A brief history of MFA
- We look into why traditional MFA was appropriate at the time but has kept up with the progress of attackers
- We detail the dangers posed by passwords and traditional MFA that requires a second device and/or push notifications
- Finally we cover off the alternative which is unphisable passwordless MFA

09:40 **Are they safe? Data, the life blood of our modern society**

Matthias Canisius, Regional Sales Director CEE, SentinelOne

- Cybersecurity is increasingly becoming a data problem
- Immense amounts of data have to be analysed and evaluated in order to derive possible steps – ideally completely autonomously – from these findings
- How can we meet this ever-increasing and complex challenge without getting buried under the masses of data?
- Do we need new ideas, processes or even technologies?
- In this presentation we will discuss new and innovative approaches that will help you solve this pressing issue

10:00 **Software architecture and software security**

Dr. Annegret Junker, Lead Architect, Allianz

- Software architecture and security architecture must work closely together
- Security architecture is more than governance – it is an enabler for successful software products
- Contribution models support collaboration
- How can successful cooperation models look like?

10:20 **Education Seminars | Session 1**

Devo **Single source of truth – the fundamental building blocks for an effective SOC** **Markus Klier,** DACH Country Manager, Devo	**Vectra AI** **MITER ATT&CK and MITER D3FEND: Understand and use** **Matthias Schmauch,** Vectra AI, Regional Sales Manager

11:00 Networking break

11:30 **EXECUTIVE PANEL DISCUSSION** **Securing your digital transformation**

Dr. Annegret Junker, Lead Architect, Allianz; **Yao Schultz-Zheng,** Former Digital Enterprise (Transformation) Architect, BMW Group

- Understanding the increasing attack surface through technological changes
- Importance of resilient infrastructure to support robust digital transformation
- Challenges faced by organisations
- Strengthening your security posture in your digital transformation journey

11:50 **Insights into key current cyber-trends and lessons learned from serious cyber-attack operations**

Maximilian Bode, Senior Sales Engineer, Mandiant

- Current trends
- Mandiant Incident Response Retainer
- Insights for security teams from the MTrends Report

12:10 **Redline and Racoon: How malware stealers cause damage and what to do about it**

Julian Kanitz, Lead Sales Engineer, DACH, Recorded Future

- Input loggers and stealer malware have enabled cybercriminals to generate easily exploitable initial access for state-sponsored threat actors and script kiddies alike
- Although proper multi-factor authentication has never been more important, it can still, unfortunately, be circumvented
- Using recent examples of successful attacks and breaches, get a close-up look at how Recorded Future tracks adversarial activity and enables you to adopt a proactive, intelligence-led security posture

12:30 **The psychology behind social engineering**

Jelle Wieringa, Security Awareness Advocate, EMEA, KnowBe4

- Ransomware attacks are becoming ever more commonplace, we'll illustrate the tricks cybercriminals use to fool you
- Understand how cybercriminals leverage the power of your own mind to make you do their bidding, psychology plays a vital role in social engineering
- We'll demonstrate how the way humans are programmed to operate is the root cause of the problem

Agenda

12:50 Education Seminars | Session 2

Cisco Kenna
Transforming vulnerability management – benefits of a risk-based approach
Rene Straube, TSA, Cisco Kenna

Illumio
How isolation stops the spread of ransomware
Alexander Goller, Senior Systems Engineer, Illumio

13:30 Lunch and networking break

14:30 Resilience and cyber-incidents

Marc Henauer, Head of Operation and Information Center MELANI, National Center for Cyber Security (NCSC)

- The current threat landscape and the increase in the attack surface (home office etc.)
- Dependencies on third parties (supply chain) with a view to security measures
- The resulting, necessary BCM or BCP for critical, IT-supported business processes

14:50 The role of the CISO & building trust: How to successfully manage the interaction?

Turgut Tekkececi, Offering Specialist GRC, OneTrust

- Explaining the definition of trust and what it means to be a trustworthy organisation
- Evolution of the CISO in driving trust initiatives and supporting trust outcomes
- Looking at examples such as ethical AI, trust in biometrics, and zero trust architecture
- Discuss successful practices in setting trust goals, implementing trust frameworks, and creating trust metrics

15:10 Speed kills malware: How 20ms puts you in the driver's seat

Kevin Boerner, Distinguished Sales Engineer EMEA, Deep Instinct

- Speed matters. Security too. Did you know that the fastest ransomware starts infiltrating and encrypting a network within 1.5 seconds? That's roughly the length of an adult's heartbeat
- Modern defence systems have to react even faster to protect you from these known and unknown attacks. Deep learning can make all the difference
- How deep learning can prevent and detect threats
- Machine learning vs. Deep learning: How deep learning can provide more speed and accuracy
- Insights into an accurate timeline of an unknown attack
- 20 milliseconds: What happens in the time in which a ransomware attack can be prevented

15:30 Education Seminars | Session 3

CybelAngel
Finding the leaky data links in your supply chains – data security beyond perimeters
Marcquero Ermoza, Head of CyberSecurity Solution Engineering team, EMEA, CybelAngel

Group IB
Christmas Hancitor Campaign: preventing Cuba's threat
Camill Cebulla, Sales Director, Europe, Group IB

16:10 Networking break

16:30 Defensive security

Francisco Z. Gaspar, Lead CyberSecurity Architect, Telefónica Germany

"He who is prudent and lies in wait for an enemy who is not, will be victorious." Sun Tzu, The Art of War

- A company is only as secure as its weakest link. Therefore, an effective defensive security must encompass and address the entire system, weak links and all, as security is a shared responsibility by the providers and consumers
- This talk will go into the foundations of defensive cybersecurity, the idea is to give the audience a different approach to security – the defensive approach

16:50 Amadeus: Security awareness – how Covid-19 and home office have helped boost security awareness

Thomas Wepner, Senior Corporate Security Officer, Amadeus Group

Covid-19 and the forced move to work from home for most of our staff presented some huge challenges to security and to security awareness. This case study shows how we adapted our awareness programme and turned the challenges into a successful new concept. The session will describe:

- The challenges presented by having almost everyone work remotely
- How turning on-site trainings into live-online sessions increased attendance and acceptance
- How you can get people to like the idea of a lot more security training

17:10 The pursuit of unfitness: Qualification gaps within cybersecurity

Ruben Caris, Anti Financial Crime – Liaison Office and Advanced Analytics at HypoVereinsbank – UniCredit – Deutschland

- An intelligence organisation: Intelligence as model
- Spacetime: the fourth dimension of cybersecurity intelligence
- Qualified or skilled? Experts you need and the organisation they deserve

17:30 Conference close

Education Seminars	
Cisco Kenna **Transforming vulnerability management – benefits of a risk-based approach** **Rene Straube,** TSA, Cisco Kenna	Organisations are overwhelmed by the total number of vulnerabilities. With limited resources, how do you prioritise the most critical vulnerabilities for remediation? In this session, we will discuss the challenges of vulnerability prioritisation and we will provide an overview of the approach Cisco Kenna is leveraging to prioritisation, exploitability characteristics and exploit prediction. • There are a plethora of options for vulnerability management tools, organisations are typically using multiple network & application scanners to understand where they are vulnerable, but the rate of identification of CVEs is far exceeding the remediation and patch capabilities of IT, leaving organisations with huge workloads, breakdowns in risk communication, and at increasing risk of exploitation • The need for prioritisation has now been widely adopted, but CVSS scoring and vendor specific threat intel are only touching the surface of the root issue: effective prioritisation requires cross-vendor collaboration of threat & exploit intelligence, data science & machine learning, and real-time risk-based analysis of likelihood of exploitation • Organisations are increasingly moving towards a central depository for all their vulnerability information, where the findings can be prioritised, deprioritised, and distributed effectively across security and IT • But what is effective prioritisation? How can we achieve 2–3% accuracy of CVE to exploitation? How can we measure the ROI and success of such an approach? What is required to meet these high standards? – we discuss the Cisco Kenna approach
CybelAngel **Finding the leaky data links in your supply chains – data security beyond perimeters** **Marcquero Ermoza,** Head of CyberSecurity Solution Engineering team, EMEA, CybelAngel	Ask yourself, where is the risk in sharing data with third parties? Is the risk the third party, or is the risk having your data leak? The real danger is the data leak! The leak being at a third party just makes it more challenging to locate. Instead of making third parties jump through long and sometimes unproductive audits, a new perspective is needed – a data risk first approach. A data risk first approach focuses on locating whatever data matches your organisation's regardless of where it appears. By focusing on which data matches, you gain visibility and protection far beyond a company's perimeter into third, fourth, and fifth parties. This increase in visibility frees cybersecurity teams from choosing which partners get monitoring. You will learn: • Why your risk is with the data, not third parties • What is a data risk first approach • How DRPS tools can assist in a data risk first approach
Devo **Single source of truth – the fundamental building blocks for an effective SOC** **Lars Wiesner,** Software Engineering Executive, Devo	How effective is your security operations and your ability to gather evidence, investigate and find source data? If unsure, you're not alone. Combating today's threats requires new approaches to how your SOC manages its data, analytics, and expertise. Join Devo as we explore innovative ways your security team can thrive in the era of massive data growth, talent shortage, and constantly evolving threats. • Cloud-based solutions scale to achieve the critical full visibility into threats, giving you a single source of truth • Analytics that use automation and machine learning uplift analysts' performance, saving your security team valuable time • Community expertise augments your tribal knowledge to quickly resolve threats, helping you bridge the industry talent gap

Education Seminars	
Group IB **Christmas Hancitor Campaign: preventing Cuba's threat** **Camill Cebulla,** Sales Director, Europe, Group IB	During the height of the pandemic, almost all countries introduced restrictions, limiting many day-to-day activities. Many aspects of public life and work were put on hold. But that didn't apply to hackers. As businesses moved to remote working there was a surge in hacker activity targeting vulnerable VPN servers and publicly available RDP services. • We uncover the attacks carried out by Hancitor operators on a European company. Revealing how we identified the attack, discovered the threat actor's infrastructure and finally prevented an incident from occurring by interrupting encryption of the organisation's systems and network • We share how Group-IB's Threat Intel & Attribution team detected an attack as it took place and kicked out the threat actors before damage was done • We reveal all the stages of hacker activity – from gaining initial access to lateral movement, methods of investigating these stages, and the hacker's tools • We also share our top recommendations that teams can immediately action to help prevent cyber-threats • Finally, and most importantly, we will share how security teams can utilise timely and accurate threat intelligence to stay ahead of threat actors to identify attacks and prevent incidents from happening
Illumio **Wie Isolation die Verbreitung von Ransomware stoppt** **Alexander Goller,** Senior Systems Engineer, Illumio	Ransomware nutzt Unternehmensnetzwerke, um sich zu verbreiten und sich seitwärts zu bewegen, bevor sie zuschlägt und im besten Fall zu Unannehmlichkeiten, großen geschäftlichen Auswirkungen oder im schlimmsten Fall sogar zu Auswirkungen auf die Gesellschaft führt. Wir werden uns ansehen, wie Sie Ihre potenziellen Risiken und Schwachstellen identifizieren, wie die Verbreitung von Ransomware funktioniert und wie Sie eine widerstandsfähigere Verteidigung gegen alle zukünftigen Bedrohungen aufbauen können. • Erfahren Sie, wie Sie die Verbreitung von Ransomware stoppen können • Identifizieren Sie potenzielle Schwachstellen in Ihrer Infrastruktur • Bauen Sie eine widerstandsfähigere Verteidigung gegen zukünftige Bedrohungen auf • Nachrichten über Ransomware reißen nicht ab und es gibt keine Woche, in der kein Ransomware-Angriff öffentlich wird
Vectra AI **MITER ATT&CK and MITER D3FEND: Understand and use** **Matthias Schmauch,** Regional Sales Manager, Vectra AI	An early opponent of security through obscurity was locksmith Alfred Charles Hobbs , who in 1851 demonstrated to the public how state-of-the-art locks could be picked. The cybersecurity industry is now increasingly shedding this secrecy, as far as patent law allows. Transparency and comparability are supposed to give the customer a serious picture of performance. In this context, one now often hears the terms MITRE ATT&CK and D3FEND, with which the American research institution MITRE demystifies cybersecurity research and makes it more comparable. In Vectra AI's seminar, you will learn: • Who is MITRE? • What do ATTACK and DEFEND involve? • How do you use this in the enterprise?