Post event report

Strategic Sponsors

corelight

CYBERSPRINT
BREAKTHROUGH SECURITY

DARKTRACE

ExtraHop

Fidelis Cybersecurity

paloalto NETWORKS

Recorded Future

SentinelOne

Edcuation Seminar Sponsors

BeyondTrust

INTSIGHTS
Defend Forward

KENNA Security

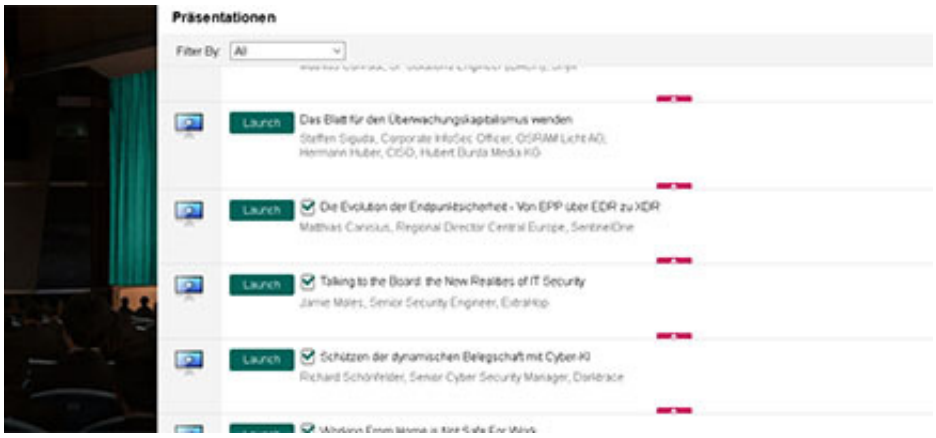
onapsis

snyk

Synack

"Thank you for the very interesting online event!"
Business Information Security Officer, CitiGroup Germany

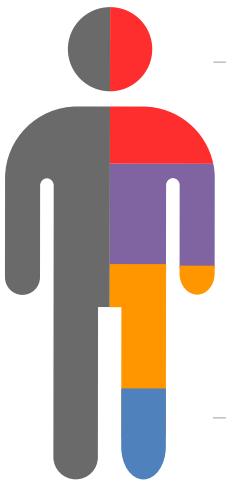
Inside this report:



Key themes

- Cybersecurity for business resilience
- Strengthening identity and access management
- Securing the citizen
- Building in security: easier said than done?
- Securing the workplace revolution
- What to do about ransomware?
- Securing digital currencies

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

Simon Brady, Managing Editor, AKJ Associates Ltd

Matthias Canisius, Regional Director Central Europe, SentinelOne

Mathias Conradt, Sr. Solutions Engineer (DACH), Snyk

Abdelkader Cornelius, Threat Intelligence Analyst, Recorded Future

Marco Di Meo, Sales Team Leader, EMEA, Darktrace

Eward Driehuis, Senior Vice President Strategy, Cybersprint

Thomas Hornung, Solutions Architect EMEA, Synack

Hermann Huber, CISO, Hubert Burda Media KG

Mohamed Ibbich, Senior Technology Consultant, BeyondTrust

Achim Kraus, Solutions Engineering CEEUR, Corelight Inc.

Chris Kubic, Chief Information Security Officer, Fidelis Cybersecurity

Andreas Lober, Partner, BEITEN BURKHARDT

Etay Maor, Chief Security Officer, IntSights

Jamie Moles, Senior Security Engineer, ExtraHop

Klaus Nötzel, CISO, EUMETSAT

Stephen Roostan, VP EMEA, Kenna Security

Stephan Rosche, Sales Director DACH Region, Synack

Ernestine Schikore, Informationssicherheitsbeauftragte CISO, University of Basel

Stefan Schinkel, Director Cortex Central Europe, Palo Alto Networks

Steffen Siguda, Corporate InfoSec Officer, OSRAM Licht AG

Peter Vahrenhorst, Detective Chief Superintendent, State Office of Criminal Investigation of North Rhine-Westphalia

Frederik Weidemann, Chief Technical Evangelist, Onapsis Inc

Marcel Zumbühl, CISO, Swiss Post

Agenda

08:00 Login and networking

08:50 Chairman's welcome

09:10 **Our challenges in IT: Attack scenarios**

Ernestine Schikore, Informationssicherheitsbeauftragte CISO, University of Basel

- Vulnerabilities: 'WannaCry' case study
- Presumption of AD: Exploitation of account rights
- Importance of central log infrastructure

09:20 **Cortex secures the future**

Stefan Schinkel, Director Cortex Central Europe, Palo Alto Networks

Security Operations Centres (SOCs) are characterised by chaos, struggling with siloed tools, manual processes, and reliant on the old premise of high-volume, low-fidelity rule-based correlation for everything from detection to investigation. This session details the building blocks of simpler, and more effective security operations and how SOCs transform to an automated proactive model by spending less time on manual reactive processes and more on hunting for unknown threats and transferring knowledge gained into future improvement.

- Simplify operations across networks, clouds and endpoints
- Trusted intelligence with automation
- Rapidly respond to threats with deep visibility, flexibility and contextual insight
- Arm your security team with integrated best-in class detection, investigation and threat intelligence

09:40 **Current pricing models for cyber-attacks**

Abdelkader Cornelius, Threat Intelligence Analyst, Recorded Future

In this presentation, you will receive live information on the current prices and requirements of active threat actors and their tools and campaigns. You will learn:

- Why ransomware attacks are so lucrative and easy
- How volatile the price structure is, and also the supply and demand dynamics
- How the prices commanded by threat actors has developed over the last two years

10:00 **International data transfer**

Andreas Lober, Partner, BEITEN BURKHARDT

- How Schrems II has nuked international data transfer
- Why transferring data to the US has become so difficult
- Why you should not forget about China and others
- How Cloud Services and SaaS are impacted
- Why the authorities say that even video conferencing is illegal

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

BeyondTrust	Snyk
Effective security: Least privilege as an important part of your PAM strategy	**Enterprise security – securing cloud-native applications at scale**
Mohamed Ibbich, Senior Technology Consultant, BeyondTrust	**Mathias Conradt,** Sr. Solutions Engineer (DACH), Snyk

10:50 Networking break

11:20 **EXECUTIVE PANEL DISCUSSION** **Turning the tide on surveillance capitalism**

On July 16th, the Court of Justice of the European Union published its eagerly awaited decision in the Schrems II case, which invalidated the framework of the US-EU data protection shield for the international transfer of data. This, of course, presents a particular problem today, given the accelerated digitisation programmes that all types of businesses are going through, particularly as a result of the current state of the world. Topics such as the close link between data privacy and data protection and their successful implementation are discussed here, among other things.

Steffen Siguda, Corporate InfoSec Officer, OSRAM Licht AG **Hermann Huber,** CISO, Hubert Burda Media KG

11:40 **The evolution of endpoint security: From EPP to EDR to XDR**

Matthias Canisius, Regional Director Central Europe, SentinelOne

- Why AV is dead and how endpoint security has developed in recent years
- What differentiates an Endpoint Protection Platform (EPP) from Endpoint Detection and Response (EDR)
- The advantages of a fully integrated XDR platform over conventional EPP and EDR solutions.

12:00 **Talking to the board: the new realities of IT security**

Jamie Moles, Senior Security Engineer, ExtraHop

- The large-scale adoption of work-from-home technologies, heightened activity on customer-facing networks, and greater use of online services has greatly increased the risk of misconfigurations and cyber-threats
- Hackers have taken advantage of these new vulnerabilities and in recent weeks, ransomware attacks have affected several major organisations
- When attacks like these make headlines, board members have one question for CISOs: how can we be sure that won't happen to us?
- Join to hear top strategies for CISOs to lead board-level conversations about risk management amidst the stark new realities of IT

Agenda

12:20 — Securing the future of work with cyber AI

Marco Di Meo, Sales Team Leader, EMEA, Darktrace

- Trends & challenges of digital collaboration
- How AI can protect your dynamic workforce
- Automated analysis and response with Cyber AI

12:40 — Education Seminars | Session 2

IntSights	Onapsis
Working from home is not safe for work	**SAP security threat landscape 2021**
Etay Maor, Chief Security Officer, IntSights	**Frederik Weidemann,** Chief Technical Evangelist, Onapsis Inc

13:10 — Lunch and networking break

14:10 — EXECUTIVE PANEL DISCUSSION — To expect the unexpected shows a thoroughly modern intellect

Oscar Wilde would probably not have chosen the life of a CISO but he was right about the way they should look at the world. The Solar Winds hack makes the security of security the issue it should always have been. Enforced digitalisation of everything from the customer interface to supply chain management makes every element of most businesses a cyber-attack surface. The IoT, better thought of as an infinite ecosystem of sensors, does the same while upending business models such as insurance. And it seems as though WFH, COVID and a continuation of on/off remote and hybrid working is with us for many more months. So, what do your fellow CISOs think 2021 will bring? And how are they planning to meet those challenges?

Ernestine Schikore, Informationssicherheitsbeauftragte CISO, University of Basel
Klaus Nötzel, CISO, EUMETSAT
Marcel Zumbühl, CISO, Swiss Post

14:30 — Present and future attack factors: the risks to Germany's internet hubs & how to protect them

Eward Driehuis, Senior Vice President Strategy, Cybersprint

- Germany's role in the international internet
- The 3 biggest risks that come with this role
- How criminals abuse these risks
- What you can do to protect your organisation

14:50 — Alarm fatigue in the SOC: 'If you lie once, you won't be believed ...'

Achim Kraus, Solutions Engineering CEEUR, Corelight Inc.

- How and what causes the signs of fatigue and consequences in the SOC?
- What can you do in order to keep pace instead of exchanging technologies?
- How do I achieve the required decision-making quality with my resources?
- The normalisation and completion of necessary data for the larger whole
- See – Decide – Act: Out-of-the-Box, but yet open, flexible, integrable?

15:10 — Education Seminars | Session 3

Kenna Security	Synack
Rethinking & solving the patching problem: A new approach	**Next generation offensive security testing**
Stephen Roostan, VP EMEA, Kenna Security	**Thomas Hornung,** Solutions Architect EMEA & **Stephan Rosche,** Sales Director DACH Region, Synack

15:40 — Networking break

16:00 — Defending enterprises from the full spectrum of cyber-threats

Chris Kubic, Chief Information Security Officer, Fidelis Cybersecurity

The threat landscape is constantly evolving and our environments are getting more complex and harder to defend. Witnessing the scale and sophistication of recent attacks disrupting our security world, what can CISOs and security operations teams do to level the playing field and defend their enterprise environments against threats originating from cybercriminals, sophisticated and stealthy nation-state attackers, insiders, 3rd party partners, and supply chains. In his presentation, Chris will outline what we can do to better protect ourselves against the full spectrum of these threats.

- Diligent patching of business critical and exposed systems
- Early detection and validation of anomalous activity
- Having a well-rehearsed plan should you be the next victim of a breach

16:20 — Spotlight on ransomware – the police perspective

Peter Vahrenhorst, Detective Chief Superintendent, State Office of Criminal Investigation of North Rhine-Westphalia

- Ransomware is still the scourge of IT systems, even or especially in times of pandemic. Why?
- Steps for effective prevention and damage reduction: how to prepare for the worst-case scenario
- Insights from the perspective of police work

16:40 — Delegates will be able to choose from the following presentations:

Cybersecurity in the age of disorder	Bug Bounty Post: Securing digital trust
Simon Brady, Managing Editor, AKJ Associates Ltd	**Marcel Zumbühl,** CISO, Swiss Post

17:00 — Closing remarks **17:05** — Networking **17:30** — Conference close

Education Seminars	
BeyondTrust **Effective security: Least privilege as an important part of your PAM strategy** **Mohamed Ibbich,** Senior Technology Consultant, BeyondTrust	It is becoming more and more difficult to find a good balance of rights distribution for employees and administrators. Users as well as IT administrators should be given sufficient authorisations to carry out their work productively, while at the same time minimising IT security risk and protecting sensitive data systems. Attackers are often one step ahead of organisations. Even those with the most comprehensive IT security systems and control mechanisms fear that an attacker could discover and exploit a vulnerability. This session explains practical tools that companies can use to implement industry-recognised best practices for endpoint privilege management and basic security controls to protect IT systems and data from the most common attacks. It contains recommendations for successfully implementing a least privilege strategy that will help you eliminate unnecessary permissions. Likewise, rights can be increased on multiple platforms and networked devices without affecting end-user productivity. This session provides information about: • Recommendations for implementing basic security controls • Best practice examples on the subject of endpoint privilege management • Tips for successfully implementing a least privilege strategy (principle of least privileges)
IntSights **Working from home is not safe for work** **Etay Maor,** Chief Security Officer, IntSights	• How threat actors leverage threat intelligence • New emerging threats for the remote workforce • What security professionals need to ask themselves to better understand their security posture
Kenna Security **Rethinking & solving the patching problem: A new approach** **Stephen Roostan,** VP EMEA, Kenna Security	This sessions explains why the area of vulnerability management offers an untapped opportunity to measurably decrease risk and deliver operational cost savings. • Strategic and tactical benefits of designing a new framework • Changing the patching mindset across all stakeholders • Leveraging existing investments with future-proof, flexible tools • Defining – and achieving – the right success metrics for your business
Onapsis **SAP security threat landscape 2021** **Frederik Weidemann,** Chief Technical Evangelist, Onapsis Inc	In the past few years, 64% of organisations' ERP systems have been breached, according to a research study by IDC. Are you aware how attackers have breached and can break into unprotected customer SAP landscapes? Attend this session to gain insights into: • What attacks on your SAP systems look like • What security challenges exist in SAP environments (e.g. S/4HANA) • Moving to the cloud with confidence – how to address security in hybrid landscapes • Ways to protect your organisation

Education Seminars	
Snyk **Enterprise security – securing cloud-native applications at scale** **Mathias Conradt,** Sr. Solutions Engineer (DACH), Snyk	Join this session to learn: • How DevSecOps is being used to secure cloud-native applications • Cloud-native architecture is improving time to capability at a reduced cost for the enterprise • Unify your dev team around a secure deployment approach with cloud-native architecture such as containers
Synack **Next generation offensive security testing** **Thomas Hornung,** Solutions Architect EMEA & **Stephan Rosche,** Sales Director DACH Region, Synack	The noise within security circles has become overwhelming, making it difficult to focus on what is real. Traditional pen testing is no longer an option so organisations are leaning on crowdsourced security testing as a proactive means of identifying sources of risk and building trust with customers, all while operating remotely. In this session you'll learn: • About a revolutionary security testing approach using teams of highly vetted, top-class security researchers who can find serious vulnerabilities in any live system often within a matter of hours • How Synack's remote security testing platform can help augment your internal teams now • Of a number of use cases and POCs performed at customers across EMEA