

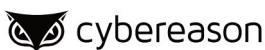
# Post event report



## Strategic Sponsors



## Education Seminar Sponsors



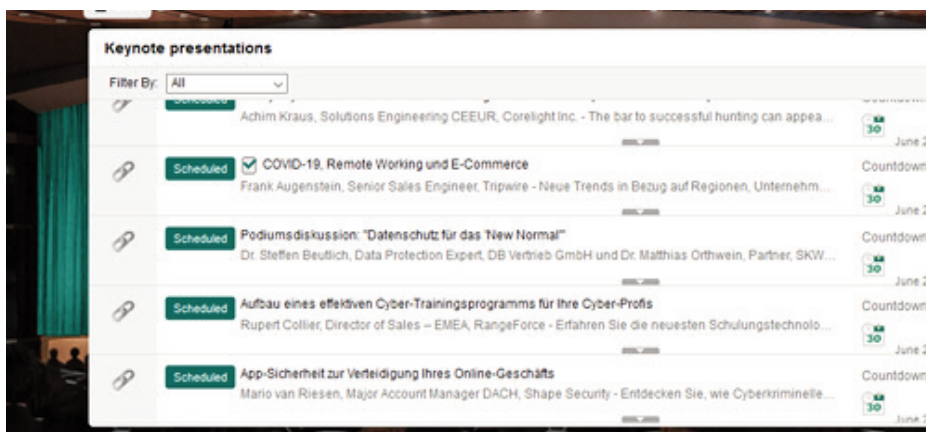
“ Despite the difficulties that the current pandemic situation brings with it, I found the event yesterday in this new virtual format to be successful, very interesting and stimulating.

I took new insights and ideas with me, which I will share with colleagues to further develop information security management. ”

IT Security Officer  
MLP

## Inside this report:

- Sponsors
- Key themes
- Who attended?
- Speakers
- Agenda
- Education Seminars



## Speakers

Frank Augenstein,  
Senior Sales Engineer,  
**Tripwire**

Israel Barak,  
Chief Information Security Officer,  
**Cybereason**

Henrik Becker, Lawyer, Kanzlei Becker

Frank Bertisch,  
Head of Group Internal Audit,  
**Coop Group**

Dr. Steffen Beutlich,  
Data Protection Expert,  
**DB Vertrieb GmbH**

Rupert Collier, Director of Sales - EMEA,  
**RangeForce**

Adam Drabik, Former CISO,  
**Opel Vauxhall Finance**

Branko Džakula, CISO, **Kaia Health**

Sergej Epp, Chief Security Officer,  
**Palo Alto Networks**

Daniel Gordon,  
Senior Solutions Engineer, DACH,  
**OneLogin**

Henning Hanke, Solutions Specialist  
Security Awareness Training, DACH,  
**Proofpoint**

Thomas Hornung,  
Solution Architect EMEA,  
**Synack**

Achim Kraus,  
Solutions Engineering CEEUR,  
**Corelight Inc.**

Dr. Matthias Orthwein, Partner,  
**SKW Schwarz Rechtsanwälte**

Stephan Rosche,  
Sales Director DACH Region,  
**Synack**

Fabian Schild, Head of Cyber Defense,  
**Deutsche Apotheker- und Ärztebank**

Andy Spencer, VP Sales Engineering,  
**Cofense**

Florian Stahl, Team Manager Security  
Method & Testing,  
**AVL**

Jan Tietze,  
Director Security Strategy EMEA,  
**SentinelOne**

Julian Totzek-Hallhuber,  
Principal Solutions Architect,  
**Veracode**

Mario van Riesen,  
Major Account Manager DACH,  
**Shape Security**

Ian Wallace, Sales Engineer DACH,  
**Cofense**

David Weber,  
Enterprise Sales Engineer DACH,  
**CrowdStrike**

## Key themes

Rethinking identity and access management

Stuck in the cloud

Performing critical security tasks remotely – how can CISOs regain control?

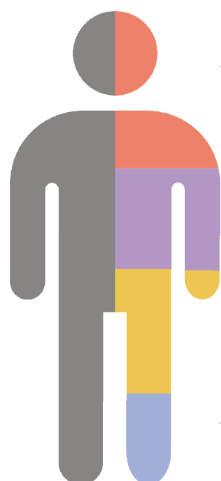
Securing the customer – are your websites up to it?

Maintaining the human firewall

Protection versus business needs

Securing and protecting remote employees

## 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

Agenda			
08:00	Login and networking		
09:05	Chairman's welcome		
09:10	<b>PANEL DISCUSSION</b> <b>Lessons from lockdown</b> <b>Frank Bertisch</b> , Head of Group Internal Audit, Coop Group; and <b>Fabian Schild</b> , Head of Cyber Defense, Deutsche Apotheker- und Ärztebank <ul style="list-style-type: none"> <li>• Practical security for the work-from-home workforce</li> <li>• Cloud and cloud security strategies in the rush to digitalisation</li> <li>• Bending the rules for the business: is security learning to be an enabler?</li> <li>• Securing the return to work: problems and solutions</li> </ul>		
09:30	<b>The threat hunting challenge: detect, prevent, respond and hunt – every second, every day</b> <b>Jan Tietze</b> , Director Security Strategy EMEA, SentinelOne <ul style="list-style-type: none"> <li>• Learn how Endpoint Detection &amp; Response (EDR) technologies pick up where antivirus technologies leave off</li> <li>• Understand why EDR should be an essential part in every endpoint security strategy</li> <li>• Learn how EDR auto-immunises the endpoints against newly discovered threats and provides rich forensic data, mitigate threats and performs network isolation</li> <li>• Demo</li> </ul>		
09:50	<b>How to keep business continuity and control costs in turbulent times</b> <b>Julian Totzek-Hallhuber</b> , Principal Solutions Architect, Veracode Join this session to learn more about: <ul style="list-style-type: none"> <li>• Leveraging the cloud so that you can begin securing your applications right away</li> <li>• How cloud-based solutions can boost collaboration and productivity for remote teams</li> <li>• The benefits of Veracode's SaaS products, including minimal to no installation</li> <li>• Scaling up, scaling down, and saving money with easy integration into your SDLC</li> </ul>		
10:10	<b>Doing more with less: surviving with limited cybersecurity resources in abnormal times</b> <b>Adam Drabik</b> , Former CISO, Opel Vauxhall Finance <ul style="list-style-type: none"> <li>• How to cope with staff shortages and hiring pauses without adversely affecting your cybersecurity strategy</li> <li>• Are your old cybersecurity processes still relevant? Reviewing and streamlining your processes for remote working</li> <li>• Adopting the necessary collaborative tools when operating remotely, on a budget</li> <li>• Outsourcing vs. in-house cybersecurity operations. What are the pros and cons of switching tactics?</li> </ul>		
10:30	<b>Education Seminars   Session 1</b> <table border="1"> <tr> <td> <b>Cofense</b>  <b>Engaging end users in phishing defence – are your teams Combat Ready?</b>  <b>Andy Spencer</b>, VP Sales Engineering, Cofense; and  <b>Ian Wallace</b>, Sales Engineer DACH, Cofense </td><td> <b>Cybereason</b>  <b>Ransomware's evolution from blunt tool to sophisticated weapon</b>  <b>Israel Barak</b>, Chief Information Security Officer, Cybereason </td></tr> </table>	<b>Cofense</b> <b>Engaging end users in phishing defence – are your teams Combat Ready?</b> <b>Andy Spencer</b> , VP Sales Engineering, Cofense; and <b>Ian Wallace</b> , Sales Engineer DACH, Cofense	<b>Cybereason</b> <b>Ransomware's evolution from blunt tool to sophisticated weapon</b> <b>Israel Barak</b> , Chief Information Security Officer, Cybereason
<b>Cofense</b> <b>Engaging end users in phishing defence – are your teams Combat Ready?</b> <b>Andy Spencer</b> , VP Sales Engineering, Cofense; and <b>Ian Wallace</b> , Sales Engineer DACH, Cofense	<b>Cybereason</b> <b>Ransomware's evolution from blunt tool to sophisticated weapon</b> <b>Israel Barak</b> , Chief Information Security Officer, Cybereason		
11:00	Networking break		
11:30	<b>Cybersecurity and the Home Office</b> <b>Florian Stahl</b> , Team Manager Security Method & Testing, AVL <ul style="list-style-type: none"> <li>• Home office cybersecurity challenges</li> <li>• Organisational measures (guidelines, employee training, ...)</li> <li>• Technical measures (VPN, encryption, secure video conference tools..)</li> </ul>		
11:50	<b>NextGen networks and security – what does it look like?</b> <b>Sergej Epp</b> , Chief Security Officer, Palo Alto Networks <ul style="list-style-type: none"> <li>• What are the lessons learned with legacy networks, connectivity, and network security?</li> <li>• Why does network security matter in times of encrypted traffic and decentralisation?</li> <li>• What are the indigents for the third generation networks?</li> <li>• What does the convergence between security and networks look like for mobile users, BYOD, branches, and connected cars?</li> </ul>		
12:10	<b>Stopping breaches faster: can you meet the 1/10/60 minute challenge?</b> <b>David Weber</b> , Enterprise Sales Engineer DACH, CrowdStrike <ul style="list-style-type: none"> <li>• 1 Minute: Time to Detection – organisations should set a goal of allowing only one minute to detect an incident or intrusion (automated)</li> <li>• 10 Minutes: Time to Investigation – the length of time it takes to find out if the incident is legitimate and determine next steps (containment, remediation, etc.)</li> <li>• 60 Minutes: Time to Remediation – the period of time needed to eject the intruder and contain the initial threat</li> </ul>		

Agenda			
12:30	<b>The human factor – your people as last line of defence</b> <b>Henning Hanke</b> , Solutions Specialist Security Awareness Training, DACH at Proofpoint <ul style="list-style-type: none"> <li>Threat landscape and threat actors 2020</li> <li>Security awareness – not just knowledge transfer but behavioural change</li> <li>Cybersecurity and the human factor = more than the sum of its parts</li> </ul>		
12:50	<b>Education Seminars   Session 2</b> <table> <tr> <td> <b>Corelight</b>  <b>Demystifying the hunt: how to assess threat hunting readiness and prepare for the next step?</b>  <b>Achim Kraus</b>, Solutions Engineering CEEUR, Corelight Inc. </td><td> <b>Tripwire</b>  <b>COVID-19, remote working and e-commerce: how are companies adapting to the evolving cybersecurity challenges?</b>  <b>Frank Augenstein</b>, Senior Sales Engineer, Tripwire </td></tr> </table>	<b>Corelight</b> <b>Demystifying the hunt: how to assess threat hunting readiness and prepare for the next step?</b> <b>Achim Kraus</b> , Solutions Engineering CEEUR, Corelight Inc.	<b>Tripwire</b> <b>COVID-19, remote working and e-commerce: how are companies adapting to the evolving cybersecurity challenges?</b> <b>Frank Augenstein</b> , Senior Sales Engineer, Tripwire
<b>Corelight</b> <b>Demystifying the hunt: how to assess threat hunting readiness and prepare for the next step?</b> <b>Achim Kraus</b> , Solutions Engineering CEEUR, Corelight Inc.	<b>Tripwire</b> <b>COVID-19, remote working and e-commerce: how are companies adapting to the evolving cybersecurity challenges?</b> <b>Frank Augenstein</b> , Senior Sales Engineer, Tripwire		
13:20	Lunch and networking break		
14:20	<b>PANEL DISCUSSION   Data protection for the new normal</b> <b>Dr. Steffen Beutlich</b> , Data Protection Expert, DB Vertrieb GmbH; and <b>Dr. Matthias Orthwein</b> , Partner, SKW Schwarz Rechtsanwälte <ul style="list-style-type: none"> <li>Protecting data, exploiting data: the business challenge of data protection</li> <li>Managing multi-country compliance</li> <li>Employee surveillance and data privacy challenges in the new normal</li> </ul>		
14:40	<b>Building an effective training programme for your cyber-pros</b> <b>Rupert Collier</b> , Director of Sales – EMEA, RangeForce <ul style="list-style-type: none"> <li>Learn cutting-edge training technologies and strategies for security team leaders</li> <li>Overcome limited budgets, time, as well as train in place requirements</li> <li>Discover the latest advances in interactive computer-based training, advanced simulation, and cyber-range exercises</li> </ul>		
15:00	<b>App security to defend your online business from automated attacks</b> <b>Mario van Riesen</b> , Major Account Manager DACH, Shape Security <ul style="list-style-type: none"> <li>Discover how cybercriminals circumvent traditional protections such as CAPTCHA and MFA</li> <li>Explore the fraud losses and security risks associated with automated application attacks</li> <li>Understand how to separate fake users from real customers without degrading the user experience</li> <li>Increase digital engagement and improve conversion rates</li> </ul>		
15:20	<b>Education Seminars   Session 3</b> <table> <tr> <td> <b>OneLogin</b>  <b>Empower your employees to work securely and efficiently from home</b>  <b>Daniel Gordon</b>, Senior Solutions Engineer, DACH, OneLogin </td><td> <b>Synack</b>  <b>Next generation offensive security testing</b>  <b>Thomas Hornung</b>, Solution Architect EMEA, Synack; and  <b>Stephan Rosche</b>, Sales Director DACH Region, Synack </td></tr> </table>	<b>OneLogin</b> <b>Empower your employees to work securely and efficiently from home</b> <b>Daniel Gordon</b> , Senior Solutions Engineer, DACH, OneLogin	<b>Synack</b> <b>Next generation offensive security testing</b> <b>Thomas Hornung</b> , Solution Architect EMEA, Synack; and <b>Stephan Rosche</b> , Sales Director DACH Region, Synack
<b>OneLogin</b> <b>Empower your employees to work securely and efficiently from home</b> <b>Daniel Gordon</b> , Senior Solutions Engineer, DACH, OneLogin	<b>Synack</b> <b>Next generation offensive security testing</b> <b>Thomas Hornung</b> , Solution Architect EMEA, Synack; and <b>Stephan Rosche</b> , Sales Director DACH Region, Synack		
15:50	Networking break		
16:10	<b>Communicating a (confirmed) data breach in the right way</b> <b>Branko Džakula</b> , CISO, Kaia Health <ul style="list-style-type: none"> <li>Overview of top threats resulting in recorded data breaches</li> <li>Where did big players fail in communication?</li> <li>How to communicate a data breach in the right way</li> <li>Crisis management – prepare for the worst case scenario</li> </ul>		
16:30	<b>Lock down = lock up?</b> <b>Henrik Becker</b> , Lawyer, Kanzlei Becker <ul style="list-style-type: none"> <li>Home office and remote working – changes from the perspective of a risk and compliance manager</li> <li>The value of personal conversations</li> <li>Detection of risks and misconduct without visual contact</li> <li>Practical recommendations</li> </ul>		
16:50	Closing remarks		
17:00	Networking		
17:30	Conference close		

## Education Seminars

**Cofense****Engaging end users in phishing defence – are your teams combat ready?**

**Andy Spencer**, VP Sales Engineering, Cofense; and  
**Ian Wallace**, Sales Engineer DACH, Cofense

As the world locked down to mitigate the risks of COVID-19, many employees are still adjusting to working from home, and companies like yours are working hard to support it. However, organisations cannot completely lock down their networks. For example, phishing emails continue to evade Secure Email Gateways, with threat actors adapting their tactics to exploit the ongoing crisis. Businesses are threatened by a surge of phish related to COVID-19 and remote work. Listen in as Cofense security experts Andy Spencer and Ian Wallace provide an in-depth review of the current phishing threat landscape, as seen through the inboxes and eyes of those on the front line – your end users, the new face of your front-line phishing defence.

**Highlights will include:**

- Insights of various phishing campaigns that evaded SEGs and reached enterprise end users, delivering credential phish and malware
- How threat actors are using trusted services, such as online business surveys and document sharing platforms, to evade SEGs
- Expert predictions of what we will continue to see through the end of Q2 and the remainder of 2020

**Corelight****Demystifying the hunt: how to assess threat hunting readiness and prepare for the next step?**

**Achim Kraus**, Solutions Engineering CEEUR, Corelight Inc.

- Many organisations want to threat hunt, but don't know where to begin, how to measure success, or how to scale an effective programme
- The bar to successful hunting can appear intimidatingly high, reachable by only the most sophisticated, well-staffed SOCs
- The reality is that one individual, with the right data and some directional guidance, can begin their hunting journey today, making immediate security contributions to their organisation
- We discuss the threat hunting maturity model based on real world examples and best practices – what works & is doable, what is hard to achieve, what's your next best move

**Cybereason****Ransomware's evolution [from blunt tool to sophisticated weapon]**

**Israel Barak**, Chief Information Security Officer, Cybereason

Though ransomware attacks dropped significantly in early 2018, they have re-emerged with a vengeance with new features that make them much more dangerous.

- In December 2019 the average ransom payout to an attacker was over \$80,000
- What once was a blunt instrument of damage is now a campaign-style piece of malware
- Learn about evolving ransomware attacks in real-world environments
- Understand how new capabilities make ransomware more sophisticated than ever

**OneLogin****Empower your employees to work securely and efficiently from home**

**Daniel Gordon**, Senior Solutions Engineer – DACH, OneLogin

Over the past couple of decades we have seen the number of employees that work from home increase dramatically. Today, due to COVID-19 quarantine policies around the globe, many companies are faced with a new paradigm – employees must work from home for an undefined period of time. This change in work brings challenges along, including controlling corporate data, managing security threats, and accessing applications in a hybrid environment.

Join Daniel Gordon, Senior Solutions Engineer – DACH, OneLogin, for his session 'Empower your employees to work securely and efficiently from home'.

**During this discussion you'll learn how to:**

- Adjust to a sudden 100% remote workforce
- Provide easy, secure access to business systems
- Give employees multiple ways to communicate effectively and efficiently
- Ensure device trust and safety flexible authentication policies



## Education Seminars

### Synack

#### Next generation offensive security testing

**Thomas Hornung**, Solution Architect EMEA, Synack; and  
**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

### Tripwire

#### COVID-19, remote working and e-commerce: how are companies adapting to the evolving cybersecurity challenges?

**Frank Augenstein**, Senior Sales Engineer, Tripwire

Security teams are at the forefront of protecting the distributed enterprise. Cybersecurity must be integrated into COVID-driven business responses such as the shift to working from home, migrating to e-commerce, and massively scaling delivery logistics. To learn more about how security professionals are dealing with the rapidly evolving environment, Tripwire has conducted some detailed research and we'd like to share some of the fascinating results in this session. Including:

- Emerging trends across regions, company size and job levels on how COVID-19 has impacted companies
- What are companies' biggest security concerns?
- What steps are being taken to reduce the impact of COVID-19 on their organisation's cybersecurity defences
- What technologies are available to assist with maintaining security in the new working environment