Post event report

Strategic Sponsors

Check Point SOFTWARE TECHNOLOGIES LTD.

CROWDSTRIKE

DARKTRACE

INTSIGHTS Democratizing Threat Intelligence™

LexisNexis RISK SOLUTIONS

Recorded Future®

SentinelOne™

Education Seminar Sponsors

BeyondTrust

CybelAngel

MENLO SECURITY

OPSWAT.

ProSoft MANAGE | SECURE | OPTIMISE IT

RELIAQUEST

Synack

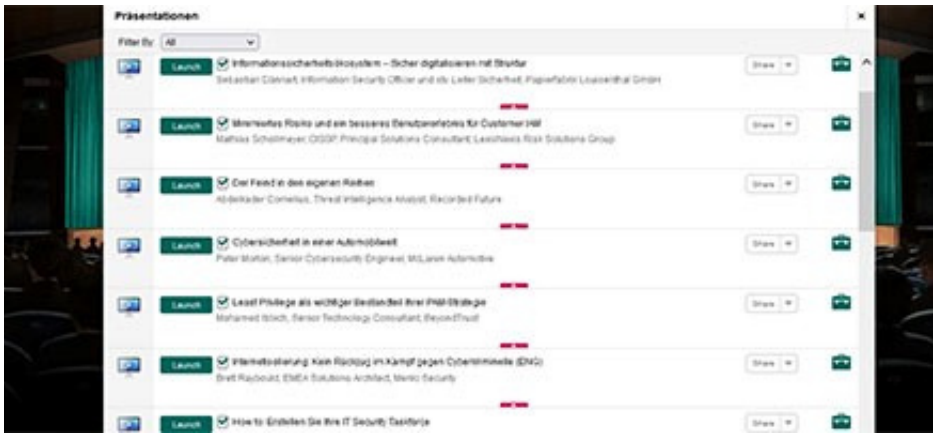
Networking Sponsors

corelight

"A very successful and professionally conducted event, very well adapted to the virtual format, with numerous information-rich lectures from practice for practice."

Corporate Information Security Expert, Merck

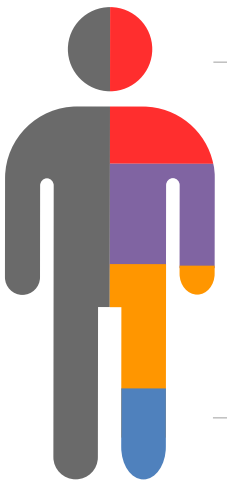
Inside this report:



Key themes

- Securing the citizen
- Building-in security: from DevOps to SecDevOps?
- Performing critical security tasks remotely - how can CISOs regain control?
- Cybersecurity for business resilience
- Securing the workplace revolution
- Stuck in the Cloud
- Security for the 5G revolution
- Securing the enterprise of sensors
- 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

Johannes Braams, Senior Cybersecurity Advisor, Royal Haskoning DHV

Matthias Canisius, Regional Director DACH, SentinelOne

Abdelkader Cornelius, Threat Intelligence Analyst, Recorded Future

Moty Cristal, CEO, NEST

Sebastian Dännart, Deputy Head of Security and Information Security Officer, Papierfabrik Louisenthal GmbH

Paul Fischoeder, Cyber Security Account Director, Darktrace

Dr. Enrico Fontan, Head of IT Operation, Repower

Kashif Husain, VP, Information Security Officer, Nomura Bank

Mohamed Ibbich, Senior Technology Consultant, BeyondTrust

Yves Jonczyk, Harmony Sales Expert, Check Point

Abdullah Kartal, Account Executive, CybelAngel

Bruno Kalhøj, former Head of Division, Security & Safety, European Central Bank

Robert Korherr, CEO, ProSoft GmbH

Gal Messinger, Global Head of Security, Signify

Peter Morton, Senior Cybersecurity Engineer, Mclaren Automotive

Joe Partlow, CTO, ReliaQuest

Udo Pittracher, Area Sales Director DACH, OPSWAT

Paul Prudhomme, Head of Threat Intelligence Advisory, IntSights

Brett Raybould, EMEA Solutions Architect, Menlo Security

Stephan Rosche, Sales Director DACH Region, Synack

Ashok Sankar, Vice President of Product Marketing, ReliaQuest

Jörg Schauff, Strategic Threat Intelligence Advisor, CrowdStrike

Mathias Schollmeyer, CISSP, Principal Solutions Consultant, LexisNexis Risk Solutions Group

Agenda

08:00 Login and networking

08:50 Chairman's welcome

09:00 **Information security ecosystem – secure digitisation with structure**

Sebastian Dännart, Deputy Head of Security and Information Security Officer, Papierfabrik Louisenthal GmbH

- How do I bring order to the jungle of security measures?
- Security by design also in digitisation – who are my stakeholders?
- Standard architectures as anchors in digitisation

09:20 **Reduced risk and improved user experience for Customer Identity Access Management**

Mathias Schollmeyer, CISSP, Principal Solutions Consultant, LexisNexis Risk Solutions Group

- Create an improved, frictionless user experience
- Control your own risk appetite
- Increase threat detection capabilities
- Replace traditional possession factors with passive authentication

09:40 **The enemy within**

Abdelkader Cornelius, Threat Intelligence Analyst, Recorded Future

Cybercrime services of all kinds are available on multiple Dark Web forums and social media channels. But did you know that you can also buy details of insiders with daily access to your critical infrastructure? In this presentation:

- get an insight into current offers from malicious insiders
- learn what it costs to buy or gain access through a dissatisfied employee
- understand which are the most affected industries
- learn how you can track this kind of threat and be notified in real time

10:00 **Cybersecurity in an automotive world**

Peter Morton, Senior Cybersecurity Engineer, Mclaren Automotive

- In-vehicle networks and their security risks: outline of a typical in-vehicle network topology
- Assessing the attack surface of a typical modern vehicle
- Examples of vehicle hacks
- How to improve vehicle security
- Incoming regulation and legislation

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

BeyondTrust	Menlo Security
Effective security: Least privilege as an important part of your PAM strategy	**Internet isolation: No surrender to cybercriminals**
Mohamed Ibbich, Senior Technology Consultant, BeyondTrust	**Brett Raybould,** EMEA Solutions Architect, Menlo Security

10:50 Refreshments and networking

11:20 **How to build your IT security taskforce**

Dr. Enrico Fontan, Head of IT Operation, Repower

- How to leverage the IT skills inside the company to create an incident response team
- Understanding IT security as mindset
- Developing the necessary IT skillset for a perfect team
- Building a skillset as a team effort

11:40 **Check Point HARMONY is revolutionising the protection of users, devices and access**

Yves Jonczyk, Harmony Sales Expert, Check Point

- Significantly more employees work from home and need to be protected right there
- Attackers are adapting to the situation and targeting remote endpoints
- IT departments are looking for consolidation and simplification due to increased complexity
- Outlook for SASE, ZTNA and Contextualised Access in VPN-less infrastructures

12:00 **Ransomware in focus: How AI stays one step ahead of attackers**

Paul Fischoeder, Cyber Security Account Director, Darktrace

- Ransomware trends and impact
- Examples of sophisticated and expensive ransomware attacks
- How self-learning AI helps companies of all industries to fight back

12:20 **A peek into the e-crime ecosystem**

Jörg Schauff, Strategic Threat Intelligence Advisor, CrowdStrike

- Services in the Deep and Dark Web
- The value chain of the criminal ecosystem
- Enhanced ransomware activities
- The value of threat intelligence for security teams

Agenda

12:40 Education Seminars | Session 2

CybelAngel

Attack on smart buildings: How IoT means that you have to re-plan your IT security strategy

Abdullah Kartal, Account Executive, CybelAngel

ReliaQuest

Tackling security in hybrid and multi-cloud environments with confidence

Joe Partlow, CTO, ReliaQuest, and **Ashok Sankar,** Vice President of Product Marketing, ReliaQuest

13:10 Lunch and networking break

14:00 How to successfully rob a bank!

Kashif Husain, VP, Information Security Officer, Nomura Bank

- The majority of crimes in our industry are initiated with cyber-attacks on people – however, our people can also be our most valuable assets
- Walkthrough of multiple 'bank robbery' scenarios to focus on a real event from 2016, where $1 billion were at stake being stolen from a bank
- How human vigilance can counteract human error

14:20 SUNBURST – chronology of a digital nightmare

Matthias Canisius, Regional Director DACH, SentinelOne

- What is known about one of the most effective cyber-attacks in recent years?
- How could it go undetected for so long despite the widespread use of threat intelligence and EPP/EDR solutions?
- How can companies protect themselves effectively against such attacks?

14:40 Selling breaches: The transfer of network access on criminal forums

Paul Prudhomme, Head of Threat Intelligence Advisory, IntSights

- Means by which criminals transfer network access to criminal buyers, such as VPNs, web shells, or RDP credentials
- Typical use cases for transferring network access to other criminals, particularly the deployment of ransomware
- Examples of targets of and prices for network access on sale on criminal forums
- Discussion of why criminals often sell their access to third parties, rather than monetising it themselves

15:00 Education Seminars | Session 3

OPSWAT & ProSoft

What do over 30 antivirus scanners and 'boiling water' have to do with the Zero Trust philosophy?

Robert Korherr, CEO, ProSoft GmbH, and
Udo Pittracher, Area Sales Director DACH, OPSWAT

Synack

Next generation defence: Using hackers to beat hackers

Stephan Rosche, Sales Director DACH Region, Synack

15:30 Refreshments and networking

16:00 Stories from the front lines: Negotiating with a ransomware criminal

Moty Cristal, CEO, NEST, and **Gal Messinger,** Global Head of Security, Signify

- Mistakes are an essential element in managing any human crisis, let alone in ransomware and cyber-extortion incidents
- Based on years of operational experience in cyber-crises, and using a variety of real life examples, this session will present the common mistakes made during ransomware crises and how to prevent them
- Hear first hand experiences in successfully negotiating with ransomware criminals

16:20 Engineering for resilience: Cybersecurity in infrastructure

Johannes Braams, Senior Cybersecurity Advisor, Royal Haskoning DHV

- What is a complex system?
- How complex is a tunnel system?
- Resilience in the lifecycle of assets
- Various approaches to designing and operating complex systems
- Risk analysis in the light of IEC 62443
- Mitigating measures

16:40 Why you're not making enough mistakes

Bruno Kalhøj, former Head of Division, Security & Safety, European Central Bank

- Research shows that people in a high-performing culture learn more effectively from their mistakes than from their successes
- What are the practical steps involved in moving from a culture of blame to one of trust and transparency?
- Case study from a central bank

17:00 Closing remarks, refreshments and 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)

CybelAngel

Attack on smart buildings: How IoT means that you have to re-plan your IT security strategy

Abdullah Kartal, Account Executive, CybelAngel

A blast furnace shut down in a German steel mill... All production lines stopped in an American brewery... Across all industries, connected buildings are becoming prime targets for cyber-attacks. Hackers are quicker than security leaders to recognise blindspots in intertwined IT/OT/IoT environments relying on third-party providers and outsourced systems. By 2023, the financial impact of cyber-physical system attacks as a result of fatal casualties will reach over $50 billion, 10 times higher than 2013 levels of data security breaches. (Source: Gartner, 2020). Good news is, your Digital Risk Protection solution can help you secure your operations against malware and ransomware attacks on smart technologies.

- Understand the risk landscape created by the increasing interconnection of IT, operational technology (OT) and building automation system environments
- Learn how to integrate third-party providers' techs and outsourced systems into your attack surface management strategy
- Discover how CybelAngel can help you bridge the gap between physical security and digital risk protection

Menlo Security

Internet isolation: No surrender to cybercriminals

Brett Raybould, EMEA Solutions Architect, Menlo Security

Despite the growing sophistication of cyber-attacks and new pressures of managing remote workers, cyber-practitioners remain defiant in their cyber-defence. No one is ready to wave a white flag. This session is designed for security professionals who are not content to maintain the cyber status quo and are exploring fundamentally different approaches such as isolation to proactively protect their users and systems.

Join this session to hear two real world case studies of organisations that have transformed risk of infection at speed and scale – outsmarting threats and promoting productivity.

What will attendees learn:

- How to eliminate risk of infection from browser-based threats
- How to protect users from credential theft via phishing attacks
- How quickly isolation's protective layer around users delivers business value

OPSWAT & ProSoft

What do over 30 antivirus scanners and 'boiling water' have to do with the Zero Trust philosophy?

Robert Korherr, CEO, ProSoft GmbH, and
Udo Pittracher, Area Sales Director DACH, OPSWAT

We believe every file poses a threat. In this seminar, Mr. Robert Korherr (CEO, ProSoft GmbH) and Mr. Udo Pittracher (Area Sales Director DACH, OPSWAT) will give an overview of how OPSWAT's core technology counteracts this threat.

- Advantages of antivirus multiscanning/sanitisation
- Different use cases for MetaDefender core technology
- File upload, removable media, e-mail, and storage-security

Education Seminars	
ReliaQuest **Tackling security in hybrid and multi-cloud environments with confidence** **Joe Partlow,** CTO, ReliaQuest, and **Ashok Sankar,** Vice President of Product Marketing, ReliaQuest	With the changing face of business demands, attack surfaces, and technology innovations, cloud computing has firmly entrenched itself as the face of digital transformation in the cybersecurity industry. As organisations mature and devise strategies to adopt and migrate to the cloud, data protection, governance and customer privacy requirements among others are dictating environments that are more than homogenous but hybrid and multi-cloud. While the cloud has many benefits, there's also hurdles to overcome to increase cloud visibility, detect common cloud attack types and different platforms to understand. Cloud adoption is more of a journey with various stages and it is important that security is baked in considering the various nuances to help detect and prevent misconfigurations and other security threats. In this session, you'll walk away with: • An overview of cloud trends and typical attack paths that you need to consider while adopting hybrid and multi-cloud strategies • Best practices to increase visibility across data that spans multiple cloud platforms (such as AWS, Microsoft Azure, and GCP) to reduce risk • Examples of how unifying existing on-premise and multi-cloud technologies enables faster threat detection and response
Synack **Next generation defence: Using hackers to beat hackers** **Stephan Rosche,** Sales Director DACH Region, Synack	Modern security architectures require continuous monitoring with regard to exploitable vulnerabilities. The size of the attack surfaces, highly professional hacking tools and methods make it difficult for any security team to make a good analysis of where to prioritise the countermeasures. In this session the participants learn: • How to quickly identify and react to risks or threats even in very agile target systems • How external ethical hackers can be efficiently integrated into vulnerability management • How crowdsourcing contributes to the cost control and reduction of security projects