

Post event report



The 8th e-Crime & Cybersecurity
Benelux Summit

6th December 2018 | Amsterdam

Strategic Sponsors



Education Seminar Sponsors



“ Thank you very much for the organisation of the event. It was excellent and I took valuable inspiration with me, as always. Presentations provided a balanced combination of technical and people perspectives to security, with some very engaging speakers. ”
Data Processing Manager,
International Criminal Court

“ As with years before: a great event to attend! Interesting conversations, inspirational speakers. ”
Security Officer & Operations Manager,
MP Objects

“ I really liked the mix of presentations. Not only from security vendors but also some showcases from business companies like Kyocera, Philips, Shell and Ahold Delhaize. ”
Senior Project Manager,
KLM

Inside this report:
Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars



Speakers

Owais Ahmed,
Chief Information Security Officer,
Kyocera Document Solutions

Richard Archdeacon, Advisory CISO,
Duo Security

Vijay Balasubramaniyan,
Co-Founder, CEO & CTO,
Pindrop

Benessa Defend, Business Security
Advisory Manager EU,
Ahold Delhaize

Rob Earley, Senior Pre-Sales Engineer,
Endace

Elisabeth Entjes, Account Manager,
Darktrace

David Janson, VP Sales, UK & Europe,
Cofense

Matt Jennings-Temple,
Digital Marketing Manager,
Ground Labs

Muhittin Hasancioglu, Former Chief
Information Security Officer,
Shell

Jacob Henricson,
Senior Risk Management Advisor,
foreseeti

Vera Krückel, Trend Researcher,
Trends Investing Equity Team,
Robeco

Sandrine Kubach,
Enterprise Account Manager,
Endace

Gal Messinger, Head of Global Security,
Philips Lighting

David Mole,
Strategic Technical Manager – EMEA,
Digital Guardian

Chris Pace, Technology Advocate,
Recorded Future

Lennart Pikaart,
Sales Director – Benelux,
BitSight

Ronald Pool, Senior Sales Engineer,
CrowdStrike

Fraz Rasool,
Head of Internal Control EMEA,
Kyocera Document Solutions

Olga Skobeleva, Solutions Engineer,
Cloudflare

Dr. Stephen Topliss, VP of Products,
ThreatMetrix

Ferdinand Uittenbogaard,
GDPR Specialist,
Ministrie van Defensie

Conrad Veerman,
Data Protection Officer,
Ministrie van Defensie

Key themes

- Cybersecurity as operational risk management
- Is acceptable cybersecurity affordable?
- Cybersecurity solutions: a problem of scalability
- Cybersecurity for the 'normal company'
- Practical solutions to the cyber-talent gap
- The merger of physical and cybersecurity
- Why threat intelligence is the key to real security
- Does anyone take third-party security seriously?

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	Breakfast networking and registration		
08:50	Conference welcome		
09:00	Cybersecurity: the investor's priority Vera Krückel , Trend Researcher, Trends Investing Equity Team, Robeco <ul style="list-style-type: none"> • Truths from one of the largest global investors and asset managers • Cybersecurity as a risk indicator for investors • Cybersecurity as an investing opportunity • Combining risk and opportunities 		
09:20	Disrupting the disrupters: how are we doing? David Janson , VP Sales, UK & Europe, Cofense <ul style="list-style-type: none"> • The latest threat and phishing attack data – and what to expect in the future • Compare industry benchmarking susceptibility and resilience to active phishing attacks • Best practices to protect your organisation against phishing 		
09:40	The importance of philosophy to establish a vigilant information security culture Owais Ahmed , Chief Information Security Officer, Kyocera Document Solutions, and Fraz Rasool , Head of Internal Control EMEA, Kyocera Document Solutions <ul style="list-style-type: none"> • How Kyocera's philosophy impacts human behaviour • Tone at the top: how everyone's responsibility for information security is given from a top-down approach • Practically measure information security performance on the basis of Kyocera's philosophy 		
10:00	Hacking exposed: lessons learnt in responding to the fight against malicious behaviour Ronald Pool , Senior Sales Engineer, CrowdStrike <ul style="list-style-type: none"> • See what advanced tactics, techniques & procedures nation-state and organised e-crime hackers have been using recently • Learn how you can detect and arm your organisation against these threats • Learn which tools you probably already have unused in your organisation to help you harden your stance against these attacks 		
10:20	Education Seminars Session 1 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;"> Cloudflare Security: the serverless future Olga Skobeleva, Solutions Engineer, Cloudflare </td> <td style="width: 50%; padding: 5px;"> ThreatMetrix Digital identities, social engineering and mule networks Dr. Stephen Topliss, VP of Products, ThreatMetrix </td> </tr> </table>	Cloudflare Security: the serverless future Olga Skobeleva , Solutions Engineer, Cloudflare	ThreatMetrix Digital identities, social engineering and mule networks Dr. Stephen Topliss , VP of Products, ThreatMetrix
Cloudflare Security: the serverless future Olga Skobeleva , Solutions Engineer, Cloudflare	ThreatMetrix Digital identities, social engineering and mule networks Dr. Stephen Topliss , VP of Products, ThreatMetrix		
11:00	Networking and refreshments break		
11:30	Intelligence-based cybersecurity Gal Messinger , Head of Global Security, Philips Lighting <ul style="list-style-type: none"> • Why do we need cyber-threat intelligence in a commercial entity? • What exactly is cyber-threat intelligence? • Where should we position it in a company? • Who should be running it? • A use case 		
11:50	Beyond security: zero trust – making the perimeter less lonely Richard Archdeacon , Advisory CISO, Duo Security <ul style="list-style-type: none"> • Concept of zero trust or the BeyondCorp model • Why a zero trust model will reduce risk • Key elements in implementing a zero trust approach 		
12:10	A new era of cyber-threats: the shift to self learning, self defending networks Elisabeth Entjes , Account Manager, Darktrace <ul style="list-style-type: none"> • Leveraging AI algorithms to defend against advanced, never-seen-before, cyber-threats • How new immune system technologies enable you to pre-empt emerging threats and reduce incident response time • How to achieve 100% visibility of your entire business including cloud, network and IoT environments • Why automation and autonomous response is enabling security teams to neutralise in-progress attacks, prioritise resources, and tangibly lower risk • Real-world examples of subtle, unknown threats that routinely bypass traditional controls 		

Agenda			
12:30	Fast and accurate issue resolution		
	<p>Sandrine Kubach, Enterprise Account Manager, Endace, and Rob Earley, Senior Pre-Sales Engineer, Endace</p> <ul style="list-style-type: none"> • The cost of network and security issues • Being prepared for a potential breach • The various approaches to breach detection • Using the right tools for the job 		
12:50	Education Seminars Session 2		
	<p>BitSight How to manage cyber-risk on a daily basis for your company and the affiliates, your suppliers and peers (Live view in the BitSight Portal) Lennart Pikaart, Sales Director – Benelux, BitSight</p>	<p>Ground Labs Standards don't bother me – all I want is your data! Matt Jennings-Temple, Digital Marketing Manager, Ground Labs</p>	
13:30	Lunch and networking		
14:30	GDPR and the Internet Of Medical Things		
	<p>Ferdinand Uittenbogaard, GDPR Specialist, Ministrie van Defensie, and Conrad Veerman, Data Protection Officer, Ministrie van Defensie</p> <ul style="list-style-type: none"> • The Internet of Things, particularly the Internet of Medical Things, can prove valuable for both employers and employees, yet there are significant risks associated with such devices • IoT brings challenges for privacy by design and GDPR • How we can make sure that organisations and employees benefit from such devices, whilst also staying safe and secure? 		
14:50	Authentication and security at the speed of conversation		
	<p>Vijay Balasubramaniyan, Co-Founder, CEO & CTO, Pindrop</p> <ul style="list-style-type: none"> • Building a voice identify platform that authenticates customers • Protecting you from fraudsters • Building new customer experiences • The emergence of the conversational economy 		
15:10	Intelligent threat intelligence: how machines are learning the language of the dark web		
	<p>Chris Pace, Technology Advocate, Recorded Future</p> <ul style="list-style-type: none"> • The impact of the threat intelligence language barrier • How machines can be taught to read and understand references to cyber-threats from the dark web and other sources • The places where humans and machines can combine to form superhuman security analysts • What predictive analytics are, and how the future is forecasting where the next threat is coming from 		
15:30	Education Seminars Session 3		
	<p>Digital Guardian How to run a successful DLP programme David Mole, Strategic Technical Manager – EMEA, Digital Guardian</p>	<p>foreseeti Threat modelling: the challenge in managing risk of both structural and technical vulnerabilities Jacob Henricson, Senior Risk Management Advisor, foreseeeti</p>	
16:10	Networking and refreshments break		
16:30	Business security advisory: from 'no' to 'know'		
	<p>Benessa Defend, Business Security Advisory Manager EU, Ahold Delhaize</p> <ul style="list-style-type: none"> • Providing business-centric, pragmatic security advice • Determining the 'just right' level of security • Ensuring that security is considered throughout the project lifecycle • Increasing automation and adapting to agile 		
16:50	A new approach to cybersecurity & risks: control your own destiny		
	<p>Muhittin Hasancioglu, Former Chief Information Security Officer, Shell</p> <ul style="list-style-type: none"> • Current reality • What is coming towards us: technology shift, digitalisation drive, new technologies, increased threat landscape • What is the step change that we need to be on? • How do we get there? 		
17:10	Final remarks	17:15	Conference close

Education Seminars	
<p>BitSight</p> <p>How to manage cyber-risk on a daily basis for your company and the affiliates, your suppliers and peers (Live view in the BitSight Portal)</p> <p>Lennart Pikaart, Sales Director – Benelux, BitSight</p>	<p>Participants will see a live view into the BitSight Portal. We will demonstrate how continuous cyber-risk monitoring works for your company and the affiliates, your suppliers and peers.</p> <p>What will attendees learn:</p> <ul style="list-style-type: none"> • How the cyber-risk rating can be improved in the easiest way; all risk vectors and the results will be demonstrated • How cyber-risk for your company and the affiliates, the suppliers and peers can be managed based on qualified events and ratings
<p>Cloudflare</p> <p>Security: the serverless future</p> <p>Olga Skobeleva, Solutions Engineer, Cloudflare</p>	<p>Does security have to come at a cost to performance and maintenance? Your security is only as strong as the weakest human link and their patience and diligence in following proper protocols. Serverless computing is the future of how complex software systems and their security will be designed and built.</p> <p>This talk will demonstrate several migration cases that Cloudflare Workers can already help with today. Some modern hosting platforms don't give you enough access to deploy certain security features. Let's say you would like to use security headers like Content Security Policy and Strict Transport Security, manage bot traffic, or do some advanced multi-factor authentication; that can be a struggle and consume many resources in your current infrastructure. With a futuristic serverless platform like Cloudflare Workers, such solutions can be deployed in seconds.</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • Security doesn't have to cost you performance or maintenance resources • Challenges of popular security implementations • Serverless computing as a security tool, eg. Cloudflare Workers • Examples: security headers, advanced multi-factor authentication, alerting, etc.
<p>Digital Guardian</p> <p>How to run a successful DLP programme</p> <p>David Mole, Strategic Technical Manager – EMEA, Digital Guardian</p>	<p>Learn about DLP Project Scope and the best DLP process, including:</p> <ul style="list-style-type: none"> • Planning and requirements phase • Deployment phase • Use case implementation phase • Transition phase <p>Learn about DLP best practices</p> <p>Learn about DLP flexible deployments</p> <p>Learn how to set up a DLP project with no upfront classification to effectively monitor and ensure data protection. See and understand who, what, where and how data flows through the enterprise out-of-the-box. This visibility and contextual intelligence can be used to confirm sensitive data (structured and/or unstructured) to permanently tag it so that it can be monitored and controlled throughout its complete lifecycle. By providing complete event visibility without predetermined rules, you can quickly assess all the ways uses access, use, and move data so that you can determine where it is most at risk.</p>

Education Seminars	
<p>foreseeti</p> <p>Threat modelling: the challenge in managing risk of both structural and technical vulnerabilities</p> <p>Jacob Henricson, Senior Risk Management Advisor, foreseeti</p>	<p>Companies today are experiencing an ever-increasing connectivity and complexity of infrastructure risk management. The underlying challenge today is that infrastructures are complex and interconnected, let alone the fact that a lot is run in the cloud. With the complexity of architectures increasing, the focus on technical vulnerabilities is not enough. Traditional vulnerability scanning offers insight on technical vulnerabilities but lacks the ability to prioritise what to focus on.</p> <p>That said, in general, there needs to be a more holistic approach to ensure that risk is managed in a proper way related to IT infrastructures. Using a combination of technical and structural vulnerabilities, being able to map large infrastructures in a scalable way, needs to be combined with a probabilistic approach in threat modelling, which enables organisations to focus on true risk instead of theoretical risk on a technical level.</p> <p>Taking this further, and being able to focus on true business risk, requires a new approach. At the Royal Institute of Technology, extensive research has been conducted in threat modelling and the probability of a certain set of parameters to be exploited to get access to an infrastructure. Join this seminar to learn the latest of research on threat modelling from both academia and the corporate world.</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • Distinction between technical and structural vulnerabilities • How to address the challenges in scaling traditional risk assessments and threat modelling of complex IT infrastructures with objective fact-based data • Using research findings to perform threat modelling on large corporate IT infrastructures • How to use threat modelling in the design process of IT infrastructures
<p>Ground Labs</p> <p>Standards don't bother me – all I want is your data!</p> <p>Matt Jennings-Temple, Digital Marketing Manager, Ground Labs</p>	<p>How a business-as-usual approach to data security and performing sensitive data discovery can aid in achieving PCI and GDPR compliance:</p> <ul style="list-style-type: none"> • Insights into how cybercriminals do not comply with global security standards, data theft is their only concern • Understanding the totality of your data helps in risk assessment for cybercrime • Data sprawl is one of the key challenges across corporate infrastructure as it presents a huge vulnerability to cybersecurity professionals
<p>ThreatMetrix</p> <p>Digital identities, social engineering and mule networks</p> <p>Dr. Stephen Topliss, VP of Products, ThreatMetrix</p>	<p>The use of digital identities in preventing fraud and enhancing customer experience in the financial industry is becoming more and more prevalent. As fraud shifts to the weakest link – the end customer – what can digital intelligence offer in combating social engineering fraud?</p> <p>What attendees will learn:</p> <ul style="list-style-type: none"> • How digital identities are used today to enhance new customer acquisition on the digital channel and protect digital banking sessions for existing customers • Specific approaches to identify the risk of social engineering based account takeover • How a targeted approach to real-time mule account detection can enhance existing fraud prevention strategies