

Post event report



The 12th e-Crime & Cybersecurity
Benelux Summit

8th December 2022 | Amsterdam

Strategic Sponsors



“ This face-to-face session was very well organised, it has been a pleasure to meet speakers & others members with direct interaction which could not be achieved in remote sessions. Topics were adequate and pointing out the world reality of cybersecurity we are in. Looking forward to the next conference. ”

IT Director, LuxAirport

“ I have always been a supporter of the e-Crime Congress, I believe it is a great platform for our industry. Many thanks for you and your companies great work to make the congress what it is today. ”

National Cyber Crime Unit UKIC
Coordinator – National Crime Agency

Education Seminar Sponsors



Networking Sponsors



Inside this report:

Sponsors

Key themes

Who attended?

Speakers

Agenda

Education Seminars



Speakers

- Marc Berns, CISO
Allianz Benelux

- Christian Borst, EMEA CTO
Vectra AI

- Robert Elferink, Sr. Manager,
Sales Engineering Benelux & Nordics
CrowdStrike

- Matthew Ellison,
Director of Sales Engineering EMEA
Corelight

- Julian Kanitz,
Lead Sales Engineer DACH
Recorded Future

- Raymond Kleijmeer,
Senior Officer Cyber Resilience
De Nederlandsche Bank

- Dr. Lydia Kostopoulos, Senior Vice
President of Emerging Tech Insights
KnowBe4

- Hanan Levin, VP Sales EMEA
Hunters

- David Lomax, Systems Engineer
Abnormal Security

- Tom McVey, Solution Architect
Menlo Security

- Rachid Mekdoud, Sales Engineer
OPSWAT

- Paul Mote, Senior Director,
Solutions Architects
Synack

- David Palmer, Business Lead for
Blockchain Technology
Vodafone

- Arash Rahmani,
Head of Information Security
Nationale-Nederlanden C&C

- Rasham Rastegarpour, Sales Engineer
ReliaQuest

- Frans Szabó, IT Lead
Rabobank

- Guus van Delft,
Bug Bounty & Crowdsourced Security
Account Executive
Intigriti

- Paul Van den Berg,
Strategic Relations & Partnerships
NCSC-NL

- Patrick Van den Branden,
Group IT Security Officer
Euroports Group

- Rick Verhagen, Cybersecurity Enterprise
Account Executive
Darktrace

- Dimitri van Zantvliet,
Chief Information Security Officer
Nederlandse Spoorwegen

Key themes

- Here comes real cybersecurity regulation
- Can zero trust be done?
- Are AI/ML solutions the answer?
- Developing the next generation of security leaders
- The pros and cons of managed services
- Building better Cloud security

Who attended?



Agenda			
08:00	Registration & networking		
08:50	Chairman's welcome		
09:00	Balancing regulation/compliance and security Paul Van den Berg , Strategic Relations & Partnerships, NCSC-NL Globally, stakeholders expect transparency on cyber-risks, and regulators are forcing organisations to act. Are CISOs and boards ready to engage in meaningful conversations? <ul style="list-style-type: none"> • The importance of acknowledging the 'material' and increasing risk • Addressing the communication gap between board and senior stakeholders • Breaking down conservative attitudes • How to engage in meaningful conversations 		
09:20	The 2022 malware and vulnerability threat landscape Julian Kanitz , Lead Sales Engineer DACH, Recorded Future The presentation examines trends in Malware use, distribution, development and high-risk vulnerabilities disclosed by major hardware and software vendors in the first half of 2022. It will cover: <ul style="list-style-type: none"> • An overview of the threat landscape of malware and vulnerabilities • Top referenced malware variants associated with cyber-attacks • Top vulnerabilities associated with cyber-attacks • Tips on how to strengthen your security posture and advisement for threat hunting teams and security operations centre teams • Outlook for the rest of 2022 based on H1 2022 observations 		
09:40	Mapping Web 3 threats Dr. Lydia Kostopoulos , Senior Vice President of Emerging Tech Insights, KnowBe4 <ul style="list-style-type: none"> • Contextualises the 4th industrial revolution and the technologies that are a part of it • Unpacks the components of Web 3 including the metaverse, internet of things, digital twins and decentralised technology • Categorises and explains the threats in the expanding cyber-terrain 		
10:00	Fireside chat: A CISO's perspective on.... Conference Chairman & Dimitri van Zantvliet , Chief Information Security Officer, Nederlandse Spoorwegen <ul style="list-style-type: none"> • How the macroeconomic downturn will affect CISOs, budgets and security • Dealing with the risks of state-sponsored cyber-attacks and spillovers • Protecting critical national infrastructure • The cyber-talent shortage – real or illusion? 		
10:20	Education Seminars Session 1 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;"> Synack Using security testing to drive change for the better Paul Mote, Senior Director, Solutions Architects, Synack </td> <td style="width: 50%; padding: 5px;"> Vectra AI Erasing surface, identity, complexity and unknowns Christian Borst, EMEA CTO, Vectra AI </td> </tr> </table>	Synack Using security testing to drive change for the better Paul Mote , Senior Director, Solutions Architects, Synack	Vectra AI Erasing surface, identity, complexity and unknowns Christian Borst , EMEA CTO, Vectra AI
Synack Using security testing to drive change for the better Paul Mote , Senior Director, Solutions Architects, Synack	Vectra AI Erasing surface, identity, complexity and unknowns Christian Borst , EMEA CTO, Vectra AI		
11:00	Networking break		
11:30	The value of strategy in information security Arash Rahmani , Head of Information Security, Nationale-Nederlanden C&C <ul style="list-style-type: none"> • Why security culture matters for third-party risk management • The strategic role of a CISO • The EU impact on third-party risk management 		
11:50	Turning the tables on cyber-attackers with a continuous AI loop approach Rick Verhagen , Cybersecurity Enterprise Account Executive, Darktrace In the face of skyrocketing cyber-risk, detecting and responding to attacks is no longer enough. Organisations must take proactive steps to prevent threats before they happen, and to recover if compromised. In this session, Darktrace unveil an ambitious new approach to security, with core engines powering AI technologies to prevent, detect, respond, and ultimately heal from attacks. Together, these engines combine to strengthen organisations' security posture in a virtuous AI feedback 'loop,' which provides powerful end-to-end, bespoke, and self-learning solutions unique to each organisation. <ul style="list-style-type: none"> • Learn how Autonomous Response knows exactly the right action to take, at the right time, to contain an in-person attack • How AI takes precise action to neutralise threats on the behalf of security teams • Use of real-world threat finds to illustrate the workings of Autonomous Response technology 		
12:10	How to address the skills shortages in a proactive manner to respond to adversaries Robert Elferink , Sr. Manager, Sales Engineering Benelux & Nordics, CrowdStrike <ul style="list-style-type: none"> • Tooling and techniques to address skills shortages • Automation and services to keep you ahead of attackers • How technology can help you become proactive and stop breaches 		

Agenda			
12:30	<p>Hunters: The SOC of the future</p> <p>Hanan Levin, VP Sales EMEA, Hunters</p> <p>Join Hunters to explore the key trends and paradigm shifts in data, detection and investigation, within the ever changing world of SOCs.</p> <ul style="list-style-type: none"> Find out how you can increase data retention whilst reducing your costs, through using built-in-detection and automation in your SOC platform 		
12:50	<p>Education Seminars Session 2</p> <table border="1"> <tr> <td> <p>Menlo Security The next class of browser-based attacks Tom McVey, Solution Architect, Menlo Security</p> </td> <td> <p>OPSWAT File upload protection: A critical gap in web app security Rachid Mekdoud, Sales Engineer, OPSWAT</p> </td> </tr> </table>	<p>Menlo Security The next class of browser-based attacks Tom McVey, Solution Architect, Menlo Security</p>	<p>OPSWAT File upload protection: A critical gap in web app security Rachid Mekdoud, Sales Engineer, OPSWAT</p>
<p>Menlo Security The next class of browser-based attacks Tom McVey, Solution Architect, Menlo Security</p>	<p>OPSWAT File upload protection: A critical gap in web app security Rachid Mekdoud, Sales Engineer, OPSWAT</p>		
13:30	Lunch break		
14:30	<p>Cyber-resilience assessments and benchmarking</p> <p>Raymond Kleijmeer, Senior Officer Cyber Resilience, De Nederlandsche Bank</p> <p>Raymond will share practical experiences on:</p> <ul style="list-style-type: none"> How to perform a self-assessment with Carnegie Mellon University's Cyber Resilience Assessment methodology Use the outcomes to make improvements Develop relevant benchmarking to enable peer comparisons 		
14:50	<p>Is network evidence really needed for security operations?</p> <p>Matthew Ellison, Director of Sales Engineering EMEA, Corelight</p> <ul style="list-style-type: none"> Do you consider network evidence a crucial part of your SOC strategy? How do you really know which alerts are the most serious? What's the best way to shift from responding to alerts to hunting for threats? Understand how to stay ahead of ever-changing attacks by using a data-first approach for detection and response. 		
15:10	<p>Defining 'ethical' hackers</p> <p>Guus van Delft, Bug Bounty & Crowdsourced Security Account Executive, Intigriti</p> <ul style="list-style-type: none"> Learn about the true meaning of ethics in hacking Walk through the thin line between criminal and lawful Discover what your company can do to reduce the grey zone to an absolute minimum 		
15:30	<p>Education Seminars Session 3</p> <table border="1"> <tr> <td> <p>Abnormal Security Key considerations for choosing the right cloud email security platform David Lomax, Systems Engineer, Abnormal Security</p> </td> <td> <p>ReliaQuest The future of security operations: Threat intelligence, automation, and data-stitching Rasham Rastegarpour, Sales Engineer, ReliaQuest</p> </td> </tr> </table>	<p>Abnormal Security Key considerations for choosing the right cloud email security platform David Lomax, Systems Engineer, Abnormal Security</p>	<p>ReliaQuest The future of security operations: Threat intelligence, automation, and data-stitching Rasham Rastegarpour, Sales Engineer, ReliaQuest</p>
<p>Abnormal Security Key considerations for choosing the right cloud email security platform David Lomax, Systems Engineer, Abnormal Security</p>	<p>ReliaQuest The future of security operations: Threat intelligence, automation, and data-stitching Rasham Rastegarpour, Sales Engineer, ReliaQuest</p>		
16:10	Networking break		
16:30	<p>How to make your company more cyber-resilient</p> <p>Patrick Van den Branden, Group IT Security Officer, Euroports Group</p> <ul style="list-style-type: none"> A pro-active and reactive approach A step-by-step process Working on 3 axes: Technical, Governance and Human The cybersecurity culture 		
16:50	<p>The metaverse opportunity</p> <p>David Palmer, Business Lead for Blockchain Technology, Vodafone</p> <ul style="list-style-type: none"> What are the key enablers for virtual and real worlds to co-exist The key challenges Security, identity, jurisdiction, copyright and ownership 		
17:10	<p>EXECUTIVE PANEL DISCUSSION Future challenges</p> <p>Marc Berns, CISO, Allianz Benelux; Arash Rahmani, Head of Information Security, Nationale-Nederlanden C&C; Frans Szabó, IT Lead, Rabobank</p> <p>Stepping back from the day-to-day necessities, what challenges in firms' digital environments cause greatest problems for the information security programme? How does the information security function mitigate and alleviate the burden on their IT and business colleagues to solve them? This panel will look at the challenges posed by:</p> <ul style="list-style-type: none"> Asset inventories (devices, applications, identity, network, data) Overall technology landscape complexity 'Digital' transformations of the business/products Testing and measuring the effectiveness of the cybersecurity control environment Incident response and problem management Ensuring the same coverage/visibility over cloud environments as on-prem Managing supply chain risk in a world less tolerant to long delays around supplier assurance (post covid) Web 3.0 and the next generation of the internet: securing new technologies and services that are inherently decentralised? 		
17:30	Conference close		

Education Seminars	
<p>Abnormal Security</p> <p>Key considerations for choosing the right cloud email security platform</p> <p>David Lomax, Systems Engineer, Abnormal Security</p>	<p>Email is both a necessary communication medium, and the most vulnerable area for an attack. Year after year, adversaries find success in abusing email to gain a foothold into an organisation – deploying malware, leaking valuable data, or stealing millions of dollars.</p> <p>Unfortunately, email threats are only growing in number. Business email compromise accounts for 35% of all losses to cybercrime, and the Verizon Data Breach Investigations Report holds that phishing remains the top entry point for breaches – a position it has held for years.</p> <p>Does that mean email is doomed, and we should give up? Quite the opposite. But the shift to cloud email requires one major thing: a shift to cloud email security.</p> <p>Attend the Abnormal Security session for answers to your most pressing questions, including:</p> <ul style="list-style-type: none"> • What are modern email threats, and how are they different from legacy attacks? • Which email threats are most concerning, and how can we defend against them in the cloud environment? • Which technical capabilities are required when protecting cloud email? • How can cloud email security platforms detect the most dangerous attacks?
<p>Menlo Security</p> <p>The next class of browser-based attacks</p> <p>Tom McVey, Solution Architect, Menlo Security</p>	<p>There are two distinct characteristics that all threat actors tend to share. First, they focus on avoiding detection by any means. Second, while some go after specific targets, many opt to aim their tactics at the vectors that will reap the greatest rewards. After all, a big pond with many fish increases everyone’s chances of success.</p> <p>Between July and December 2021, there was a 224% increase in highly evasive adaptive threats (HEAT) attacks – a class of cyber-threats targeting web browsers as the attack vector. While malware once had to be downloaded to pose a real risk, now, it’s a dynamically generated threat toolkit built in the web where employees are productive.</p> <p>In this session, you will:</p> <ul style="list-style-type: none"> • Discover the anatomy of recent browser-based attacks • Learn why network security today is broken • Experience a live demo that enables you to discover the technology approach proven to eliminate these threats
<p>OPSWAT</p> <p>File upload protection: A critical gap in web app security</p> <p>Rachid Mekdoud, Sales Engineer, OPSWAT</p>	<p>Digital transformation is a must for today’s organisations, resulting in a migration from paper-based to digital documents.</p> <p>Millions of documents are now being shared among collaborators weekly and monthly – uploaded to either a web portal, customer portal (insurance or mortgage applications) or support portal (attaching files to your support ticket).</p> <p>At the same time, an enormous amount of effort is invested into building high-availability, fault-tolerant systems and securing them.</p> <p>However, file upload remains a major attack vector and far too often is not covered by traditional web application defences.</p> <p>In this seminar, Rachid Mekdoud, Sales Engineer at OPSWAT will cover three types of risks to web applications and how to apply a Zero Trust model to both users and the files they upload and the devices from which these uploaded files originate.</p> <p>Risks from:</p> <ul style="list-style-type: none"> • Threat actors who submit malicious files to gain access to the organisation’s IT infrastructure • User who submits sensitive data in violation of an application’s terms of service • Inadvertent hosting and distributing malicious files uploaded by a threat actor

Education Seminars	
<p>ReliaQuest</p> <p>The future of security operations: Threat intelligence, automation, and data-stitching</p> <p>Rasham Rastegarpour, Sales Engineer, ReliaQuest</p>	<p>Enterprises are working to get the ROI out of their existing tools as well as accelerate their ability to detect, investigate, and respond. In attempting to accomplish these two goals, enterprises are considering a single data lake that stores their security data. There are several challenges with this approach from additional costs of data egress from cloud providers to the simple fact that the enterprise data will never be in one place. At ReliaQuest, we take a different approach using data-stitching and distributed investigations. In this talk, we will discuss the pros and cons of centralising security data and how an approach of data stitching solves those challenges.</p> <ul style="list-style-type: none"> • Security operations today • Security's 'big data' problem • Data lakes vs Data stitching • Security operations platform • Data stitching in action
<p>Synack</p> <p>Using security testing to drive change for the better</p> <p>Paul Mote, Senior Director, Solutions Architects, Synack</p>	<p>Security testing is more than a list of open vulnerabilities. It's a practice that leverages live offensive security techniques to find where true risk lies. Most organisations have very different levels of effectiveness when it comes to proactive risk identification and mitigation. Some companies might be great at fixing problems but are only average at shipping secure code the first time or with every update.</p> <p>In this session, you will learn:</p> <ul style="list-style-type: none"> • How to keep pace with digital transformation through continuous security testing • How to effectively fit security testing into your strategy • How great organisations have used security testing to make lasting, positive change – one security test at a time
<p>Vectra AI</p> <p>Erasing surface, identity, complexity and unknowns</p> <p>Christian Borst, EMEA CTO, Vectra AI</p>	<p>Threat intelligence has been a critical component to knowing threat types, methods, and profiles. As enterprises shift to cloud, security and risk leaders are facing an onslaught of unknowns. Unknown compromises, attack progressions and prioritisation challenges require more reliable, accurate, and timely insights into advanced attacks. In this session, learn how security operations need to shift their focus to be more proactive in identifying and stopping sophisticated ATP's.</p> <p>During our presentation, we will cover:</p> <ul style="list-style-type: none"> • What is threat intelligence and how it benefits your organisation and SOC team • How to analyse the data to understand the threat landscape, anticipate attackers' next moves and take prompt action to stop attacks • The importance of ongoing intelligence to prevent emerging risks and threats