Post event report

The 13th e-Crime & Cybersecurity Benelux Summit

7th December 2023 | Amsterdam

Strategic Sponsors

corelight

CROWDSTRIKE

GATEWATCHER

illumio

KnowBe4
Human error. Conquered.

rubrik

SentinelOne®

Education Seminar Sponsors

HOXHUNT

proofpoint.®

Recorded Future®

RELIAQUEST

sosafe

S-RM

> “The 13th e-Crime & Cybersecurity Congress Benelux provided excellent balance between deep tech and C-level information covering relevant topics such as AI, Zero Trust, and intrusion detection across encrypted traffic. I have been attending the e-Crime congresses for over 10 years. These congresses are a must-go-to for anyone serious about cybersecurity.”

Director IT Audit,
Liberty Global

> “Great congress to get on the most important cyber-risks, trends & techniques and to network with peers in a relaxed but professional ambiance.”

IT Risk & Security Manager,
Van Ameyde Group

Inside this report:

NIS2 puts an emphasis on governance

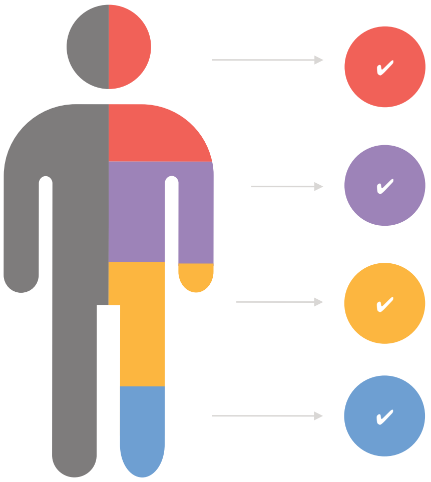
- The NIS2 Directive aims to maintain a high common level of information security across the EU. By October 17th 2024, EU member states are obliged to adopt and publish the necessary measures to comply with this directive.
- The updated NIS2 directive extends the range of organizations required to comply with its regulations beyond those already covered by the original NIS compliance directive of 2016. This expansion includes a broader range of essential services and subcontractors, as well as increased incident response obligations and more severe fines and penalties.

Arash Rahmani

Key themes

- Getting real about cyber-risk management
- Insuring the uninsurable?
- Cybersecurity as a service: the pros and cons
- Cybersecurity for SaaS/IaaS/PaaS
- Making the most of next gen tech: automation, AI and the rest
- Upskilling security teams
- Ransomware – dealing with the new normal
- Embracing digital risk management
- Here come the cybersecurity regulators
- Building better Cloud security
- Developing the next generation of security leaders
- Can zero trust be done?

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

Peter Avamale, Director, Cyber Strategy & Transformation Practice, PwC – Netherlands

Mario Beccia, Deputy CIO for Cybersecurity, NATO

Marc Berns, CISO, Allianz Benelux

Lewis Brand, Senior Sales Engineer, Recorded Future

Sjoerd de Jong, Senior Sales Engineer, SentinelOne

Trevor Dearing, Global Director of Critical Infrastructure Solutions, Illumio

Martijn Hoogesteger, Head of Cybersecurity, S-RM

Petri Kuivala, Strategic Advisor, Hoxhunt

Daniela Lourenço, CISO, Tinka B.V

Siegfried Moyo, Head of Cybersecurity EU, APAC, & LATAM, Americold Logistics

Arash Rahmani, CISO a.i., Nederlandse Zorgautoriteit

Rasham Rastegarpour, ReliaQuest

Nico Roosenboom, Systems Engineer, Corelight

Manit Sahib, Ethical Hacker

Raj Sandhu, Ethical Hacker

John Spencer, Sales Engineering, CrowdStrike

Elli Tsiala, Product Owner of Supply Chain Security, ABN AMRO Bank

Claudia van den Beld, Advisor International Cooperation, National Cyber Security Centre of the Netherlands

Bas van Erk, Director Benelux & Nordics, SoSafe

Boudewijn van Lith, Senior Manager Technical Sales, Proofpoint

Filip Verloy, Field CTO EMEA & APJ Rx, Rubrik

Jürgen Verniest, Sales Director Benelux & Nordics, Gatewatcher

Jelle Wieringa, Security Awareness Advocate, EMEA, KnowBe4

Marnie Wilking, CISO, Booking.com

Agenda

08:00	Registration and networking break
08:50	Chairman's welcome
09:00	**Collaboration is key: Balancing regulation/compliance and security** **Claudia van den Beld,** Advisor International Cooperation, National Cyber Security Centre of the Netherlands • We strive to encapsulate the current threat landscape in laws and regulations, and the need for coordination is ever more relevant. Case study: From star-gazing to law-gazing – the Observatory • We are trying to navigate this landscape through cross-border alliances which we sorely need. Case study: Choosing your cross-border partners – the Consortium • Finally, there is a great deal we can learn from each other once we appreciate the need to share information. Case study: Lowering the thresholds to heighten the insight – the Platform
09:20	**Human machine teaming: The indispensable human element of cybersecurity** **Sjoerd de Jong,** Senior Sales Engineer, SentinelOne Artificial intelligence is a pervasive part of our lives today and cybersecurity teams and adversaries alike have learned to harness the speed and power of machines to strengthen their capabilities. With machine learning becoming one of the most important tools of defence, leaders must balance the overwhelming speed and accuracy advantage of AI with the need for measured and intuitive interactions with a real-world human element. • What these trends mean for the hands-on practitioner • When velocity of innovation outpaces the capabilities of human intellect • The role of automation in the effective practice of securing our digital world
09:40	**Keeping your data incidents from becoming data breaches with Data Security Posture Management** **Filip Verloy,** Field CTO EMEA & APJ Rx, Rubrik • Data Security Posture Management (DSPM) is essential for securing data across diverse environments • DSPM enables organisations to discover, protect, and manage data assets in on-premises, cloud, and SaaS environments • Discover how by using DSPM, organisations can enforce security policies, ensure data sovereignty, and meet governance, risk, and compliance (GRC) requirements
10:00	**NIS2: Beyond compliance, a catalyst for transformation** **Arash Rahmani,** CISO a.i., Nederlandse Zorgautoriteit • The transformative opportunity of NIS2 • The strategic impact of NIS2 • The evolving role of the Chief Information Security Officer (CISO) in the age of NIS2
10:20	**Education Seminars | Session 1** **Recorded Future** **Generative AI: Amplifying attackers and defenders** **Lewis Brand,** Senior Sales Engineer, Recorded Future **SoSafe** **Hack the brain – Social engineering innovation in 2023** **Bas van Erk,** Director Benelux & Nordics, SoSafe
11:00	Networking break
11:30	**Implementing robust measures to secure the supply chain** **Siegfried Moyo,** Head of Cybersecurity EU, APAC, & LATAM, Americold Logistics • Identifying potential threats & implementing physical security measures • Conducting supplier and partner due diligence: Visibility and traceability • Business continuity planning & employee awareness • Compliance with regulations
11:50	**Living in a world of fakes** **Jelle Wieringa,** Security Awareness Advocate, EMEA, KnowBe4 Deepfakes are here, and they are here to stay. And with technology ever advancing, it is no longer a matter of simply knowing what a deepfake is. Organisations will have to actively decide how they can utilise them to grow their business, and at the same time defend against the malicious use of this technology. In this talk, we'll be looking at: • The evolving role of deepfakes in our lives • What you can do with them • How you can protect against them

Agenda

12:10	**Nowhere to hide – Key insights into adversary tradecraft 2023** **John Spencer,** Sales Engineering, CrowdStrike • Get a frontline snapshot of the current threat landscape, threat actors and their victims • Learn about the latest trends in adversary operations and tradecraft • Understand why the human factor is more relevant than ever before • Explore the 5 key steps to stay ahead of the threat actor
12:30	**NDR and NIS2: How to turn your compliance obligation into an opportunity** **Jürgen Verniest,** Sales Director Benelux & Nordics, Gatewatcher In this presentation, we will tackle: • How we allow organisations, both essential and critical, to meet the NIS2 compliance requirements by providing full network and cloud visibility • An unparalleled detection including the support of AI and ML, quick and effective response and compliancy support • Concluding NDR serves as a key tool to enable a more secure and resilient infrastructure and ensure the desired business continuity and competitive edge
12:50	**Education Seminars | Session 2** **ReliaQuest** **The future of security operations** **Rasham Rastegarpour,** ReliaQuest **S-RM** **The cyber-arms race: Staying ahead** **Martijn Hoogesteger,** Head of Cybersecurity, S-RM
13:30	Lunch break
14:30	**How to build a highly automated third-party security risk management (TPSRM) programme** **Elli Tsiala,** Product Owner of Supply Chain Security, ABN AMRO Bank • How to start your TPSRM with resources you already have • How to increase your automation and minimise onboarding effort • Lessons learned from our journey
14:50	**Using Zero Trust to improve cyber-resilience in the age of AI** **Trevor Dearing,** Global Director of Critical Infrastructure Solutions, Illumio As we transform our business models to deliver more agile services the increasing threat of AI generated attacks on critical infrastructure can potentially disrupt services causing an impact on society. Complying with any changes potentially coming with implementations of NIS2 could be complex and add cost. Taking a Zero Trust approach can simplify compliance and reduces costs. In this session, we will address the following topics: • How to identify and define risk • How to reduce the attack surface • How to contain an attack • How to respond and restore services during an attack
15:10	**Network evidence for defensible disclosure** **Nico Roosenboom,** Systems Engineer, Corelight • 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
15:30	**Education Seminars | Session 3** **Hoxhunt** **The future of the human risk reduction** **Petri Kuivala,** Strategic Advisor, Hoxhunt **Proofpoint** **Defending with an attacker's mindset** **Boudewijn van Lith,** Senior Manager Technical Sales, Proofpoint
16:10	Networking break
16:30	**CISO panel discussion** **Peter Avamale,** Director, Cyber Strategy & Transformation Practice, PwC – Netherlands, (Moderator); **Marc Berns,** CISO, Allianz Benelux; **Marnie Wilking,** CISO, Booking.com; **Mario Beccia,** Deputy CIO for Cybersecurity, NATO; **Daniela Lourenço,** CISO, Tinka B.V • Integrating cybersecurity into wider enterprise risk management frameworks • Becoming a more strategic partner to the business • Building resilience against third-party security threats • Web 3.0 and the next generation of the internet: Securing new technologies and services
17:00	**Bypassing multi-factor authentication (MFA) via phishing techniques** **Manit Sahib,** Ethical Hacker & **Raj Sandhu,** Ethical Hacker • Introduction to MFA bypass phishing techniques • Live demonstration of MFA bypass attack • Countermeasures and best practices • Conclusion of demo and presentation
17:30	Conference close

Education Seminars	
Hoxhunt **The future of the human risk reduction** **Petri Kuivala,** Strategic Advisor, Hoxhunt	Cybersecurity comes together in a holy marriage of People, Processes and Technology. CISOs needs to engage people as their force multipliers as they will not survive alone in the constantly evolving world. Join this interactive session to learn more about: • The CISO veteran & start-up coach's thoughts about the People role in the future within the cybersecurity context • Be ready with your phone having www.menti.com open to donate your ideas back into the conversation. "Hold on your chair as Texas is going bye bye….the Matrix".
Proofpoint **Defending with an attacker's mindset** **Boudewijn van Lith,** Senior Manager Technical Sales, Proofpoint	The organisation chart is the new zero-day – and today, it's publicly available on social media. • It's easier to find someone who will click a link than to find an exploit for an operating system. The attacker simply needs to know who has access to the data they want, then get creative • Most security teams don't have the same perspective that the threat actors do – they think of their attack surface in terms of VLAN and IP address, instead of the department or job title • Effective defence comes when you can anticipate your attackers' moves. By combining threat landscape insights with data on which of your users are targeted with which threats, organisations can build more effective security awareness training programmes, and users can better defend themselves from the threats they are most likely to see
Recorded Future **Generative AI: Amplifying attackers and defenders** **Lewis Brand,** Senior Sales Engineer, Recorded Future	Generative AI empowers scalable consumption and production for both attackers and defenders, ushering in a wave of surprising use cases. This presentation shifts the focus from potential malicious uses to practical takeaways. Join us to explore how generative AI can be harnessed for positive impact, providing you with actionable insights and strategies to navigate transformative possibilities. Main topics to be discussed: • Real world examples and use cases • A practical lens for defenders • Think about things differently • Recorded Future AI in action
ReliaQuest **The future of security operations** **Rasham Rastegarpour,** ReliaQuest	Security operations are changing rapidly and require a more holistic approach to security. Streamlining threat detection, investigation, and response is a good start in managing risk, but also important are utilising threat intelligence and digital risk protection, reviewing suspect employee-submitted emails via the abuse mailbox, and measuring your programme to communicate better with your stakeholders and service providers. Additionally, security operations will become more streamlined, with the automation of routine tasks and incident-response procedures becoming the norm. This session will help organisations achieve efficient and effective detection and response to security incidents. Five benefits for delegates attending the session: • How a security operations platform helps proactively detect and mitigate cybersecurity risks and support future changes in your business • The benefits of complete visibility across cloud, on-premises, and endpoint environments to mitigate security risks and enable rapid remediation • How automation at key junctures can streamline security operations, speed resolution, and reduce the risk of human error • The need for a more collaborative approach between providers and enterprises that avoids a 'black box' method and provides measurable improvements in security operations • How integration with existing security toolsets enables organisations to extract more value out of existing investments while streamlining security response

Education Seminars	
SoSafe **Hack the brain – Social engineering innovation in 2023** **Bas van Erk,** Director Benelux & Nordics, SoSafe	The human factor remains a gateway for cybercriminals as phishing and ransomware attacks continue to increase. Cases like those of Uber and Rockstar Games have also shown how cybercriminals are evolving at a rapid pace, exploiting human psychology and our emotions – and hacking our brains. But how do attackers use behavioural science specifically against us? What can we do to protect those around us? • *Emotional manipulation tactics:* Insight into how cybercriminals exploit emotions, emphasizing the need for psychological awareness in cybersecurity • *Behavioural science in attacks:* Understanding how attackers use behavioural science for effective phishing and ransomware, highlighting the importance of this knowledge in defence strategies • *Strengthening defences:* Practical strategies for enhancing resilience against social engineering, focusing on team education and recognition of sophisticated threats
SR-M **The cyber-arms race: Staying ahead** **Martijn Hoogesteger,** Head of Cybersecurity, S-RM	• Cybercriminals have had free reign for years, but organisations are better defended, driving them to develop new methods • Understand the current lay of the cybercriminal landscape • Learn about new techniques being used by ransomware groups • Hear S-RM's insights on the future of cyber-threats