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?

- 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:

- 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

- 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

- 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**

Synack	Vectra AI
Using security testing to drive change for the better	**Erasing surface, identity, complexity and unknowns**
Paul Mote, Senior Director, Solutions Architects, Synack	**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

- 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 **Fast and furious attacks: Using AI to surgically respond**

Rick Verhagen, Cybersecurity Enterprise Account Executive, Darktrace

Fast-moving cyber-attacks like ransomware can strike at any time, and security teams are often unable to react quickly enough. Join Rick Verhagen, Cybersecurity, Senior Account Executive at Darktrace, to learn how Autonomous Response uses Self-Learning AI's understanding of 'self' to take targeted action to stop in-progress attacks, without disrupting your business.

- 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

- 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

12:30 Hunters: The SOC of the future

Hanan Levin, VP Sales EMEA, Hunters

Join Hunters to explore the key trends and paradigm shifts in data, detection and investigation, within the ever changing world of SOCs.

- 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 Education Seminars | Session 2

Menlo Security **The next class of browser-based attacks** **Tom McVey,** Solution Architect, Menlo Security	**OPSWAT** **File upload protection: A critical gap in web app security** **Rachid Mekdoud,** Sales Engineer, OPSWAT

13:30 Lunch break

14:30 Cyber-resilience assessments and benchmarking

Raymond Kleijmeer, Senior Officer Cyber Resilience, De Nederlandsche Bank

Raymond will share practical experiences on:

- 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 Is network evidence really needed for security operations?

Matthew Ellison, Director of Sales Engineering EMEA, 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.

15:10 Defining 'ethical' hackers

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

- 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 Education Seminars | Session 3

Abnormal Security **Key considerations for choosing the right cloud email security platform** **David Lomax,** Systems Engineer, Abnormal Security	**ReliaQuest** **The future of security operations: Threat intelligence, automation, and data-stitching** **Rasham Rastegarpour,** Sales Engineer, ReliaQuest

16:10 Networking break

16:30 How to make your company more cyber-resilient

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

- A pro-active and reactive approach
- A step-by-step process
- Working on 3 axes: Technical, Governance and Human
- The cybersecurity culture

16:50 The metaverse opportunity

David Palmer, Business Lead for Blockchain Technology, Vodafone

- What are the key enablers for virtual and real worlds to co-exist
- The key challenges
- Security, identity, jurisdiction, copyright and ownership

17:10 EXECUTIVE PANEL DISCUSSION Future challenges

Marc Berns, CISO, Allianz Benelux; **Arash Rahmani,** Head of Information Security, Nationale-Nederlanden C&C; **Frans Szabó,** IT Lead, Rabobank

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:

- 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