Post event report

Strategic Sponsors

GROUP-IB

SOCRadar® Your Eyes Beyond

SpyCloud

TANIUM

THREATLOCKER

Education Seminar Sponsors

Abnormal

GATEWATCHER

Recorded Future®

SILVERFORT

Networking Sponsor

CybelAngel

“ Thanks for organising. It was a valuable event where we discussed important developments in the cybersecurity area. ”

Security Process Manager, ABN AMRO

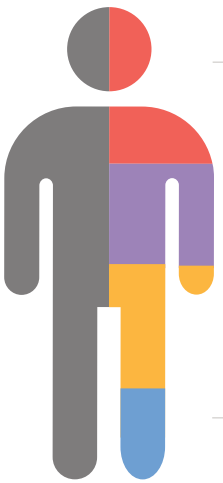
Inside this report:

Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars

Key themes

- Here come the cybersecurity regulators
- Insuring the uninsurable?
- Upskilling security teams
- Making the most of next gen tech: automation, AI and the rest
- Cybersecurity as a service: the pros and cons
- Ransomware – dealing with the new normal
- Building better Cloud security
- Cybersecurity for SaaS/IaaS/PaaS
- Embracing digital risk management
- Can zero trust be done?
- NIS2 – changing the game in cybersecurity?
- Developing the next generation of security leaders

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

Mahdi Abdulrazak, Group Information Security and Risk Officer
SHV Energy

Frank Benus, Sales Engineer
Abnormal Security

Marc Berns,
Chief Information Security Officer
Allianz Benelux

Lewis Brand, Senior Sales Engineer
Recorded Future

Lennert Branderhorst, Policy Officer
De Nederlandsche Bank (DNB)

Neill Cooper, Vice President of EMEA
SpyCloud

Martin Dimovski,
Senior DevOps/DevSecOps Engineer
ABN AMRO Bank

Andy Giles, Executive Director,
Head of Intelligence Integration
JPMorgan Chase

Roy Konings,
Head of Security Benelux & Switzerland
Ericsson

Alan Lucas, CISO
Homefashion Group

Serdar Nazlı, Solutions Engineer
SOCRadar

Fred Noordam, Regional Sales Manager
Silverfort

Manit Sahib, Ethical Hacker
The Global Fund

Mandeep Sandhu, Systems Engineering and Investigations Manager, EMEA
SpyCloud

Al Scott, Senior Sales Engineer EMEA
Silverfort

Vincent Segers,
Information Security Officer
Centrient Pharmaceuticals

Amit Kumar Sharma, Security Officer
ASR

Jukka Silomaa, Head of GRC
TomTom

Elli Tsiala, Supply Chain Security Lead
ABN AMRO Bank

Anton Ushakov, Head of Threat Intelligence and Digital Risk Protection
Group-IB

Jürgen Verniest,
Sales Director Benelux & Nordics
Gatewatcher

Thomas Zaatman,
Director of Strategic Accounts
Tanium

Agenda

08:00 Registration & breakfast networking

08:50 Chair's welcome

09:00 **Organisational resilience from policy to practice: Lessons from TomTom and experience**

Jukka Silomaa, Head of GRC, TomTom
- How to effectively implement organisational resilience strategies in cybersecurity frameworks
- Preparing for evolving cyber-threats through predictive analytics and proactive defence strategies
- Key challenges and practical insights from embedding resilience into day-to-day operations

09:20 **Future-proofing Europe: The next era of cybersecurity?**

Thomas Zaatman, Director of Strategic Accounts, Tanium
- The importance of proactive measures to protect digital assets and highlight the role of people, processes, and technology in this endeavour
- Insights into the future challenges and opportunities in cybersecurity and how organisations can effectively address them
- The growing demand for skilled cybersecurity professionals and the necessity of continuous education and training to stay ahead of cyber-threats
- The significance of implementing preventative and comprehensive strategies such as zero-trust security models to ensure compliance with regulations and standards
- The role of AI and ML in enhancing cybersecurity through real-time threat detection, predictive analysis, and automated security operations

09:40 **Iocs are not alone: Maximising outcomes from threat intelligence for preventing ransomware incidents**

Anton Ushakov, Head of Threat Intelligence and Digital Risk Protection, Group-IB

This session will delve into how threat intelligence, extending beyond traditional indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs), can help organisations mitigate ransomware risks at the earliest stages.

Key takeaways:
- How threat intelligence helps to mitigate ransomware risks
- Identifying early indicators. Monitoring for precursors like leaked credentials, compromised hosts, and initial access brokers to detect ransomware in its early stages
- Dark Web insights. How exposure of assets on the Dark Web can signal emerging attacks
- Proactive threat hunting. Shifting the perspective to the attacker to actively hunt malicious infrastructure and uncover hidden threats

10:00 **Can the AI (R)evolution help security leaders to manage complexity?**

Andy Giles, Executive Director, Head of Intelligence Integration, JPMorgan Chase
- Observations of threats using AI for fraud and malware development
- Foundations for effective AI/LLM use, focusing on the importance of a working security data model and appropriate sources
- Potential for AI application in the security risk management context to keep up with the threat
- Importance of training and AI prompt competence
- Personal reflections

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

Recorded Future	Silverfort
Generative AI: Amplifying attackers and defenders	**How non-human identities create operational and cyber-risk for organisations**
Lewis Brand, Senior Sales Engineer, Recorded Future	**Fred Noordam,** Regional Sales Manager, Silverfort & **Al Scott,** Senior Sales Engineer EMEA, Silverfort

11:00 Networking break

11:30 **Building anti-fragile security into third-party risk management and supply chain strategies**

Elli Tsiala, Supply Chain Security Lead, ABN AMRO Bank;
Roy Konings, Head of Security Benelux & Switzerland, Ericsson;
Marc Berns, Chief Information Security Officer, Allianz Benelux
- Identifying, risk assessing and screening critical vendors – a job for who?
- Defining contractual obligation: How do you enforce your security requirements, standards and data handling practices?
- Approaches to continuous vendor monitoring: Dealing with problem third parties
- Incident response planning and managing third-party breaches
- What about security vendors?

12:00 **How DevSecOps builds strong defences for cybersecurity**

Martin Dimovski, Senior DevOps/DevSecOps Engineer, ABN AMRO Bank
- DevSecOps as a foundation for cyber-resilience
- Shifting left : Embedding security left
- Enhancing collaboration between teams
- Automating threat detection and response
- Proactive threat management
- Continuous security improvement

Agenda

12:20 Education Seminars | Session 2

Abnormal Security
The AI arms race: Good AI vs. Bad AI
Frank Benus, Sales Engineer, Abnormal Security

Gatewatcher
NDR as the go-to tool to reduce the fragility in your security architecture
Jürgen Verniest, Sales Director Benelux & Nordics, Gatewatcher

13:00 Lunch & networking break

14:00 Evolving cybersecurity landscape: Key threats and future priorities

Alan Lucas, CISO, Homefashion Group
- What proactive strategies can CISOs implement to anticipate and mitigate emerging threats?
- How can organisations maintain robust cybersecurity frameworks amidst continuous technological advancements?
- How can collaboration and information sharing among cybersecurity professionals enhance threat mitigation efforts?

14:20 Inside an info stealer attack: Journey from infection to exfiltration

Serdar Nazlı, Solutions Engineer, SOCRadar
- In this session, we will take an in-depth journey through a real-world info stealer attack, from the moment of infection to the final stages of data exfiltration
- Attendees will gain insight into how these stealthy threats infiltrate environments, harvest sensitive data, and evade detection
- Through a step-by-step analysis, we will explore the tactics, techniques, and procedures (TTPs) employed by attackers and highlight how organisations can better defend against this rapidly evolving threat
- The talk emphasises detection strategies, response planning, and mitigation measures critical to protecting against info stealers

14:40 It started with a cookie: Zero Trust and the rise of session hijacking

Mandeep Sandhu, Systems Engineering and Investigations Manager, EMEA, SpyCloud;
Neill Cooper, Vice President of EMEA, SpyCloud
Learn how to go beyond traditional credential monitoring and implement continuous Zero Trust using enriched cybercrime telemetry. Attendees will learn:
- What security teams can learn from recent high-profile breaches where cybercriminals leveraged stolen session cookies in targeted attacks
- Why it's important to feed your Zero Trust policy engine with cybercrime telemetry for continuous exposure monitoring and reduced risk of session hijacking
- How cybercrime telemetry aligns with popular compliance and risk management frameworks, including DORA, NIS2, and NIST CSF
- How SpyCloud integrates with your existing security tools for automated identity exposure remediation

15:00 The ART of cyber-resilience testing

Lennert Branderhorst, Policy Officer, De Nederlandsche Bank (DNB)
- ART as a flexible framework for threat intelligence based cyber-resilience testing
- The testing process and different modules within ART
- The target user group for ART

15:20 Networking break

15:40 CISO PANEL DISCUSSION: How do we effectively manage our cybersecurity budgets?

Mahdi Abdulrazak, Group Information Security and Risk Officer, SHV Energy;
Vincent Segers, Information Security Officer, Centrient Pharmaceuticals; **Amit Kumar Sharma,** Security Officer, ASR
- How do you prioritise budget allocation and what criteria or frameworks guide your decision-making when setting spending priorities?
- How do you ensure your cybersecurity budget remains flexible enough to address unforeseen threats or emerging technologies and how do you handle unexpected costs, such as those arising from zero-day vulnerabilities or compliance changes?
- How do you measure the ROI of your cybersecurity investments, and what metrics do you use to justify budget increases to executive leadership? Are there any specific tools or technologies where you've seen the most tangible returns in terms of risk reduction or cost savings?
- What percentage of your budget do you allocate to proactive versus reactive security measures, and how do you find the right balance between the two? Have you found that increasing investment in proactive measures, like threat intelligence and automation, yields long-term cost savings?
- How do you manage budget allocation between in-house cybersecurity resources and third-party vendors or MSSPs?

16:10 LIVE DEMONSTRATION: Weaponising AI for cyber-attacks & offensive operations

Manit Sahib, Ethical Hacker, The Global Fund
- Overview & threat landscape: How AI is being leveraged in the wild for malicious activities
- Weaponising AI for offensive operations: Running AI through the cyber kill chain
- ChatGPT or [insertnamehere]GPT; What's the level of effort required to build your own AI?
- LIVE DEMO: AI in action

16:30 Chair's closing remarks

Education Seminars	
Abnormal Security **The AI arms race: Good AI vs. Bad AI** **Frank Benus,** Sales Engineer, Abnormal Security	The rapid rise of generative AI, prompted by the release of ChatGPT in late 2022, has security leaders concerned. By using this new technology, threat actors can now create highly effective attacks at scale, and few things are more vulnerable than your inboxes. Attendees will learn: • How cybercriminals are using generative AI to create their attacks • Which types of attacks are likely to grow in volume and sophistication • Why you need tools that utilise 'good' AI to protect your organisations against this 'bad' AI
Gatewatcher **NDR as the go-to tool to reduce the fragility in your security architecture** **Jürgen Verniest,** Sales Director Benelux & Nordics, Gatewatcher	In a world where uncertainty reigns, antifragility has become a key concept for building systems that not only resist but adapt to disruptions. In cybersecurity, unexpected and high-impact incidents such as zero-day exploits or advanced state-sponsored attacks, highlight how traditional security architectures often fall short. These rare but devastating threats expose vulnerabilities that static models like Zero Trust can struggle to address if improperly deployed. For Chief Information Security Officers (CISOs), who are increasingly under siege, the priority is clear: moving beyond rigid frameworks to create dynamic, antifragile ecosystems that can evolve and grow stronger in the face of an ever-changing threat landscape. This is where Network Detection and Response (NDR) solutions become indispensable. It helps CISOs to transform the limitations of Zero Trust into strengths by delivering unmatched visibility, adaptability, and rapid response capabilities. NDR technology brings antifragility to cybersecurity, helping organisations anticipate threats and grow stronger after crises, turning their networks into proactive defenders rather than passive targets. Attendees will learn: • As the number of attacks rise drastically and the attacks become increasingly sophisticated, CISOs have to deal with the concept of Shadow Risk • CISOs have to trust 100% new technologies (sometimes without regulation) while building a zero trust security architecture • CISOs have to take the right steps to provide the setting for full visibility and fast and adequate response to their SOC team
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. Attendees will learn: • Real-world examples and use cases • A practical lens for defenders • Think about things differently • Recorded Future AI in action
Silverfort **How non-human identities create operational and cyber-risk for organisations** **Fred Noordam,** Regional Sales Manager, Silverfort & **Al Scott,** Senior Sales Engineer EMEA, Silverfort	Non-human identities (NHIs) pose one of the most significant cyber-threats to an organisation as they can pose severe operational risks. In many cases, NHIs have elevated privileges, lack proper oversight, are not documented, and are often not linked to specific individuals. This makes them attractive targets for attackers, who may exploit them to gain unauthorised access, move laterally within systems, and carry out malicious activities without being detected. In our session, Silverfort will examine how organisations can reduce operational risk by understanding and implementing security controls around their NHIs. Attendees will learn: • Understand why NHIs should be a top priority for your board • Learn about how to measure and detect the level of risk NHIs pose for your organisation • Grow your knowledge of how to mitigate the risk of NHIs, before, during and after a cyber-breach