Post event report

Strategic Sponsors

censys

Integrity360
your security in mind

rubrik

TANIUM

zscaler

Education Seminar Sponsors

Abnormal

CyberProof®
A UST Company

HOXHUNT

RED SIFT

SUSE

VERACODE

Networking Sponsors

KEYSIGHT TECHNOLOGIES

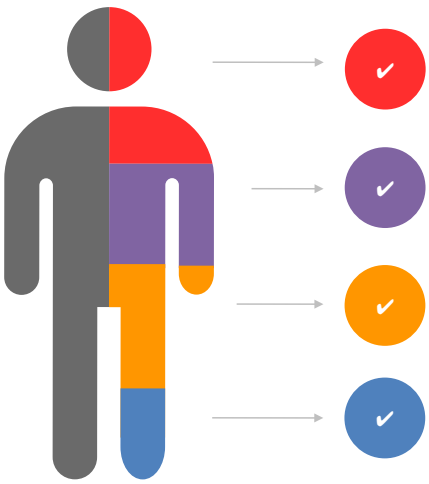
> “The conference was truly enlightening. The speakers provided practical insights into the ever-evolving landscape of digital threats, offering feasible strategies to safeguard personal and organisational data. Overall, the conference not only heightened my awareness of cybersecurity challenges but also equipped me with the knowledge and tools to better protect myself and my company in an increasingly digital world. I highly recommend this conference to anyone looking to bolster their cybersecurity knowledge.”
>
> **Security Engineer, Ericsson**

Inside this report:

Key themes

- 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
- NIS2 – changing the game in cybersecurity?
- Ransomware – dealing with the new normal
- Here come the cybersecurity regulators
- Developing the next generation of security leaders
- Embracing digital risk management
- Building better Cloud security
- 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

Thomas Berglund, Director, Technical Account Management, **Tanium**

Dominik Bieszczad, Senior Solutions Engineer, **Censys**

Simon Brady, Managing Editor & Event Chairman, **AKJ Associates**

Maxime Cartier, Head of Human Risk, **Hoxhunt**

Jonas Forsberg, Solution Architect, **SUSE**

Predrag Gaikj, CISO, **Viedoc**

Magnus Jacobson, Senior Adviser Cyber security, **Swedish Bankers' Association**

Jorge Montiel, Head of Pre-Sales, EMEA, **Red Sift**

George Mudie, Chief Technology Risk Information Officer, **H&M Group**

Christopher Schrauf, SIEM & Cybersecurity Architect, **CyberProof**

Kristoffer Sjöström, CSO & Head of Group Security & Cyber Defense, **SEB**

John Smith, CTO EMEA, **Veracode**

Amanda Spångberg, Account Manager, **Integrity360**

Dan Stead, Director, EndpointX, on behalf of **Tanium**

Eric Stenberg, Information Security Manager, **Swedbank**

Lena Stenberg Domeij, Head of Legal and Group Compliance Nordics, **Bank of China (Europe) SA**

Dimitrios Stergiou, Director of Information Security, **TapTap Send Group**

Martin Tschammer, Head of Security, **Synthesia**

James Tucker, Head of CISO, International, **Zscaler**

Filip Verloy, Field CTO EMEA & APJ, **Rubrik**

Carl Wern, Head of Group Security, **Folksam**

Steve Wills, Senior Sales Engineer, **Abnormal Security**

Teresia Willstedt, CISO, **MedMera Bank**

Agenda

08:00 Breakfast networking

08:50 Chair's welcome

09:00 **Learning from retail: Adapting to the increasing sophistication of cybercriminals and the concerns of customers**

George Mudie, Chief Technology Risk Information Officer, H&M Group

- Mitigating the rising cyber-threat landscape: Adapting your approach
- Implementing AI-powered cybersecurity solutions
- Adopting collaborative defence strategies to safeguard your organisation

09:20 **AI-powered cyber-defence: Transforming cybersecurity in the digital age**

Dominik Bieszczad, Senior Solutions Engineer, Censys

- Delve into the transformative impact of AI across three critical domains: vendors, customers, and the broader business landscape
- Intelligent threat platforms for SOCs: Learn how AI is equipping Security Operations Centres (SOCs) with smarter, more adaptive threat detection and response mechanisms
- Customer case study: Dive into a real-world application of AI in a customer's security infrastructure, detailing the challenges, solutions, and outcomes of AI integration
- Predictive end-results analysis: Discover how businesses leverage AI for predictive analytics, transforming cybersecurity from a reactive to a proactive stance

09:40 **The imbalance of cybersecurity**

Thomas Berglund, Director, Technical Account Management, Tanium, and **Dan Stead,** Director, EndpointX, on behalf of Tanium

- Capabilities before tools, moving the focus away from point solutions
- Balancing investment between capabilities, people and process and doing the basics well
- How companies have navigated their IT security journeys and any lessons learned along the way

10:00 **Third-party security: There must be a better way!**

Simon Brady, Managing Editor & Event Chairman, AKJ Associates (Moderator)
Predrag Gaikj, CISO, Viedoc
Dimitrios Stergiou, Director of Information Security, TapTap Send Group
Lena Stenberg Domeij, Head of Legal and Group Compliance Nordics, Bank of China (Europe) SA

- Can we ever really know our supply chain?
- Prioritising information gathering
- Resilience versus security
- Is it time for a complete rethink?

10:25 **Education Seminars | Session 1**

Red Sift	Veracode
Putting cyber-resilience into action	**What can we learn from 1,000,000 applications?**
Jorge Montiel, Head of Pre-Sales, EMEA, Red Sift	**John Smith,** CTO EMEA, Veracode

11:00 Networking break

11:30 **FIRESIDE CHAT** **A CSO's view...**

Kristoffer Sjöström, CSO & Head of Group Security & Cyber Defense, SEB

- AI: Balancing risks and rewards
- Security versus resilience: Aligning security priorities with organisational objectives
- Challenges of the current threat landscape

11:50 **Achieving cyber-resiliency by combining posture and recovery**

Filip Verloy, Field CTO EMEA & APJ, Rubrik

- To build a cyber-resilient organisation you need to focus both on prevention, by raising your security posture, and recovery capabilities, in the assumption that when the worst happens you are operational again as quickly as possible
- Data has the ability to both transform your business and ruin your day. As the most critical asset of any organisation, securing data is paramount
- Organisations everywhere have been on a drive to innovate and compete on the global stage, resulting in data being spread between on-premises environments, public clouds, and SaaS applications
- In order for IT and security teams to regain control over these islands of data, a new and modern approach is needed. Cyber-resiliency brings together cyber-posture and cyber-recovery to give you a safe path in dangerous times

Agenda

12:10 Education Seminars | Session 2

Abnormal Security
More attacks, more problems: 7 key elements of effective email security
Steve Wills, Senior Sales Engineer, Abnormal Security

SUSE
The importance of zero trust in Kubernetes environment
Jonas Forsberg, Solution Architect, SUSE

12:45 Lunch

13:45 Financial sector's conditions and challenges in cybersecurity and crisis preparedness

Magnus Jacobson, Senior Adviser Cyber security, Swedish Bankers' Association

- What are the driving forces behind the financial sector's work in cybersecurity crisis preparedness?
- What threats and scenarios do we need to dimension our preparedness work for?
- How should firms prepare for the many upcoming EU security and resilience regulations – DORA, NIS2, CER, CRA
- How does the financial sector work together on preparedness issues?

14:05 Cybersecurity 112

Amanda Spångberg, Account Manager, Integrity360

- Delve in the evolving world of incident response
- Statistics and trends, discuss how tactics are changing, and introduce proactive defence strategies designed to protect businesses
- The importance of preparation and fast response

14:25 Everything, everywhere, all at once

James Tucker, Head of CISO, International, Zscaler

- AI, ransomware, and nation-state attacks. These elements are all components of our threat landscape, and are shaping both our risk profile and defence strategies for the foreseeable future
- Will zero trust solve all your problems? And is AI going to increase your ransomware risk? What insights can be gained by analysing 400 billion daily transactions as seen in Zscalers Zero Trust Exchange?
- In this session, Zscaler CISO James Tucker, will provide some data-backed insights on the threats of today and the challenges we will all face in the coming year

14:45 Education Seminars | Session 3

CyberProof
Continuous threat exposure management – measure and mitigate risk in a dynamic threat landscape
Christopher Schrauf, SIEM & Cybersecurity Architect, CyberProof

Hoxhunt
How to design for any behaviour in security
Maxime Cartier, Head of Human Risk, Hoxhunt

15:20 Networking break

15:40 What to really focus on for resilience

Eric Stenberg, Information Security Manager, Swedbank

- How to break down the business needs
- What to prioritise
- Managing dependencies
- The desired results

16:00 EXECUTIVE PANEL DISCUSSION The business of being a CISO

Simon Brady, Managing Editor & Event Chairman, AKJ Associates (Moderator)
Carl Wern, Head of Group Security, Folksam
Martin Tschammer, Head of Security, Synthesia
Teresia Willstedt, CISO, MedMera Bank

- The role of the CISO as security regulation increases (NIS2, DORA etc.)
- Compliance versus security as a true business driver
- The cyber-talent shortage – real or illusion?
- CISO churn: The real causes and effects
- The future of the cybersecurity technology stack (reduction, outsourcing)
- Your biggest challenges

16:25 Chair's close **16:30** Conference close

Education Seminars	
Abnormal Security **More attacks, more problems: 7 key elements of effective email security** **Steve Wills,** Senior Sales Engineer, Abnormal Security	As long as companies use email, cybercriminals will launch email attacks. And because advanced threats exploit trusted accounts and relationships, organisations need email security that can detect even small shifts in activity and content. What attendees will learn: • Why modern and sophisticated attacks evade traditional solutions • Real-world examples of inbound email attacks and email platform attacks • The key essentials for effective cloud email security • And how to protect your organisation from the threats of today – and the future
CyberProof **Continuous threat exposure management – measure and mitigate risk in a dynamic threat landscape** **Christopher Schrauf,** SIEM & Cybersecurity Architect, CyberProof	Cyber-leaders are always measured against risks they are able to mitigate in the environment. Gathering and articulating these metrics to the management board puts them under constant pressure to do more with less. How can you gather metrics that enable them, create business cases and to get new budgets to do more? A rapidly changing threat landscape makes time a high-value commodity. The only way security practitioners can effectively handle the dynamic relationship between the threat landscape and defensive strategies is through the smart use of automation and orchestration with unbiased, evidence-based and continuous validation of the multiple tools and technologies deployed in an enterprise environment. What attendees will learn: • What are the factors to generate an organisation threat profile? • How to compare your defensive capabilities against the adversarial TTPs that are most likely to affect your organisation • How to prioritise and optimise your defences and reduce threat exposure in a manner that is both efficient and effective
Hoxhunt **How to design for any behaviour in security** **Maxime Cartier,** Head of Human Risk, Hoxhunt	Are there any risky behaviours you wish people in your organisation would just stop doing? Or secure actions you hope they would take more often? Cybersecurity risk largely stems from people and their actions, with the human element accounting for around 80% of breaches. Therefore, the best way to reduce risk is to change behaviours. What attendees will learn: • A new model to design for any behaviour (model referenced by 1,000+ academic publications) • How to apply the model to cybersecurity, with walkthrough of real-life examples such as reporting security incidents or using approved cloud platforms • Effective strategies for implementing learned skills into tackling human risk in your organisation, summarised in a physical handout given to participants.
Red Sift **Putting cyber-resilience into action** **Jorge Montiel,** Head of Pre-Sales, EMEA, Red Sift	Cybersecurity is no longer just a concern for large corporations or government agencies; it's a fundamental aspect of doing business for organisations of all sizes. With the increasing frequency and sophistication of cyber-threats, every organisation must prioritise cybersecurity to protect its assets, data, and reputation. Failure to invest in cybersecurity measures can have severe consequences, including financial losses, damage to brand reputation, and legal liabilities. What attendees will learn: • Automate threat detection, streamline incident response, and enhance overall cyber-resilience • Protect against phishing and BEC attacks • Integrate AI-driven tools for real-time monitoring and analysis to proactively identify and address potential security vulnerabilities • Transition from project-based approaches to continuous processes to combat evolving threats

Education Seminars	
SUSE **The importance of zero trust in Kubernetes environment** **Jonas Forsberg,** Solution Architect, SUSE	Beyond CVE scanning: Unveiling the crucial role of runtime security in Kubernetes clusters. What attendees will learn: • Today's challenges with container security • What to consider with CVE scanning • Why runtime security is important • What to consider with runtime security
Veracode **What can we learn from 1,000,000 applications?** **John Smith,** CTO EMEA, Veracode	Generative AI is already having a big impact on the way that software is being developed. AI assistance is allowing code to be produced faster and in greater volume than ever but it is not delivering more secure code. Generative AI models have been trained using existing code with all of the same flaws and weaknesses that plague software. Meanwhile organisations are already drowning in security debt, so the influx of new vulnerable code could be the straw that breaks the camel's back. What attendees will learn: • Review recent research into AI code generation and software security • Gain insight into where we are today and how we can plot a course to more secure software portfolios