Post event report

Strategic Sponsors

Akamai

CLOUDFLARE

proofpoint.

rubrik

SILVERFORT

SOCRadar®

THREATLOCKER

UTOPIA

Education Seminar Sponsors

CROWDSTRIKE

CyberProof®
A UST Company

netskope

Recorded Future®

SpyCloud

SUSE

“ First of all, thank you for an amazing Congress. I was there for the first time and found it both very informative and entertaining. The overall mood and feel was great! And in all fairness, can’t complain about the food either. ”
Global IT Security Manager, Birgma

“ A great format for networking with peers with top-class presentations from industry leaders. It was a day well spent. ”
IT Security Officer, PSI Paul Scherrer Institut

“ Thank you for organising a very interesting event. I learnt about some interesting developments in the cyber-world and had a great time networking. I will be coming if the event is held in Zurich next year. ”
Senior Cybersecurity Engineer, Tecan Group Ltd

“ The Event was like every year an important event for me to see new technologies and to network with possible partners. Thank you. ”
Cyber Security Engineer, AMAG Group

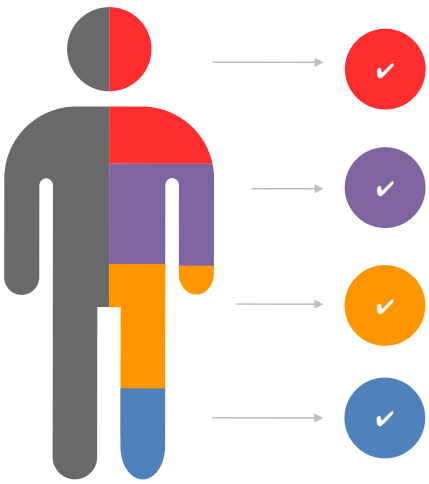
“ I just want to say thank you to you and to everyone in front and behind the scenes which organised this interesting forum. Also, my thank goes to the speakers, be it the panelist or the vendor representatives. It was very insightful. ”
Director, UBS Group

Inside this report:

Key themes

- The rise and rise of effective cybersecurity regulation
- Insuring the uninsurable?
- Cybersecurity as a service: the pros and cons
- Getting real about cyber risk management
- Cybersecurity for SaaS/IaaS/PaaS
- Making the most of next gen tech: automation, AI and the rest
- Developing the next generation of security leaders
- Securing digital currencies and DLT
- From smart machines to smart cities - securing the IoT
- Keeping citizens safe
- Reining in BigTech
- Upskilling security teams

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

Gary Adams, Solutions Consulting Manager, **Rubrik**

Matt Baird, Lead Solutions Architect, **CyberProof**, a UST company

Frank Barthel, Manager Solutions Engineering DACH, **Netskope**

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

Jan Camenisch, CTO, **DFINITY Foundation**

Alga Condoleo, Attorney, **Condoleo Law**

Dr. Shahriar Daneshjoo, VP Sales – EMEA Central, **Silverfort**

Guillaume de Benoit, Head of Information Security Operations, **Caisse des Médecins**

Joël Giger, Intelligence Consultant, **Recorded Future**

Philipp Grabher, CISO, **Canton Zurich**

Stephan Habegger, Enterprise Sales Executive, **Akamai**

Klaus Haller, Senior IT Security Architect, **AXA**

Dominic Haussmann, Specialist Solutions Engineer – Zero Trust, **Cloudflare**

Alfonso Hermosillo, Senior Solutions Engineer, **SpyCloud**

Richard Kearney, CISO, **Octapharma**

Tom Kretzschmar, Sales Engineer, **Proofpoint**

Juan Carlos Lopez Ruggiero, CISO, **Enotrac**

Ali Marwani, Senior Solutions Engineer, **SOCRadar**

Christophe Monigadon, CISO, **Visana Services AG**

Hélène Mourgue d'Algue, Chief Information Officer (CIO) and Head of Information Systems & Digital Technology, **City of Bienne**

Dieter Reuter, Solutions Engineer – NeuVector, **SUSE**

Manit Sahib, Ethical Hacker, **The Global Fund**

Dr Michel Verde, Attorney at Law, **Lustenberger + Partners**

Philipp Wachinger, Sales Engineer, **CrowdStrike**

Sandro Waelchli, CISO, **Bank Avera**

Agenda

08:00 Breakfast & networking break

08:50 Chairman's welcome

09:00 **Why third-party risk management is much more important than you think**

Guillaume de Benoit, Head of Information Security Operations, Caisse des Médecins
- Outlining the purpose, scope, and principles of your third-party risk management programme
- Establishing detailed SOPs for each stage of the third-party lifecycle
- Developing strategies for avoiding, transferring, mitigating or accepting risk
- Implementation and monitoring

09:20 **Knowing how an attacker thinks puts you one step ahead!**

Dominic Haussmann, Specialist Solutions Engineer – Zero Trust, Cloudflare
- Learn how to get on top of the different risks, and develop a holistic approach to fighting cybercriminals
- Understanding and mitigating SaaS security risks
- Developing a holistic cybersecurity strategy
- Addressing security gaps in the era of digital transformation with SaaS

09:40 **What's the chef doing in the treasure chamber?**

Stephan Habegger, Enterprise Sales Executive, Akamai
- Network segmentation and a lack of visibility in one's own data centre has long been an issue that causes annoyance and headaches in companies. For a long time, firewalls and vLANs were the inevitable approach to creating zones and thus meeting the urgent need for segmentation. As part of the digital transformation, new data centre infrastructures are being created and new applications are being developed. These and other factors require a fast and flexible procedure. The options of the past are no longer up to these requirements, as they are too rigid, complicated and inflexible.
- Let's explore how software-based segmentation enhances visibility and flexibility, while simplifying complexity for greater ease of use
- In this presentation, you'll discover why entrusting the keys to the treasure chamber to the chef is a bad idea, and how this relates to securing your IT assets

10:00 **Adapting your security strategy with the rise of SaaS solutions**

Hélène Mourgue d'Algue, Chief Information Officer (CIO) and Head of Information Systems & Digital Technology, City of Bienne
- Identifying the legal framework: Understanding the relevant laws and regulations for your information security and determining the necessary measures for compliance
- Understanding the shared responsibility model: Clarifying the division of security responsibilities between your organisation and the provider
- Managing interfaces: Address the security aspects of interfaces and integrations with the SaaS solution
- Integration into security monitoring: Ensure that the SaaS solution is fully integrated into your existing security monitoring systems for comprehensive oversight

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

Netskope	Recorded Future
Why identity alone is not enough for a Zero Trust strategy	**Take a proactive approach to ransomware mitigation!**
Frank Barthel, Manager Solutions Engineering DACH, Netskope	**Joël Giger,** Intelligence Consultant, Recorded Future

11:00 Networking break

11:30 **Encryption in the Cloud: Safeguard or expensive security theatre?**

Klaus Haller, Senior IT Security Architect, AXA
- Discover where clouds and workloads in the cloud apply encryption
- Uncover the power of diverse encryption approaches in mitigating real-life risks
- Understand how post-quantum impacts our cloud workloads

11:50 **Cyber-attacks are here to stay. Are you?**

Gary Adams, Solutions Consulting Manager, Rubrik
- What's the buzz about cyber-resiliency, and why does it matter in today's digital jungle?
- How fast can your business spring back after a cyber-attack?

12:10 **UTOPIA: Technology for creating private and sovereign clouds that are immune to cyber-attacks**

Jan Camenisch, CTO, DFINITY Foundation
- Governments and enterprises are under constant pressure to fortify their infrastructure against the imminent threat of cybercrime, often spending significant resources and labour in order to achieve a sense of security that may still fall short
- In light of this, it seems high-time to rethink the overall approach to systems infrastructure and explore how security can be more efficiently integrated into the very DNA of its architecture. Luckily, there is a better path forward: networks designed as distributed compute platforms
- This keynote explores UTOPIA networks as a unique approach to sovereign cloud infrastructure

Agenda

12:30 — **How to protect people and defend data in the age of Generative AI**

Tom Kretzschmar, Sales Engineer, Proofpoint

- As Generative AI tools continue to evolve, both cybercriminals and your employees are using them in ways that can pose risks to your organisation. Bad actors are creating more sophisticated social engineering schemes and deep fakes, and your internal users are potentially sharing sensitive corporate data
- In this dynamic and evolving environment, how can security teams best protect people and defend data?
- Top trends in the cyber-threat landscape
- Proactive actions to protect your people against human-targeted threats
- Best practices to defend data in the new age of GenAI

12:50 — **Education Seminars | Session 2**

SpyCloud	SUSE
It started with a cookie: Zero Trust & the rise of session hijacking	**We need to talk about security in our containerised workloads**
Alfonso Hermosillo, Senior Solutions Engineer, SpyCloud	**Dieter Reuter,** Solutions Engineer – NeuVector, SUSE

13:30 — Lunch & networking break

14:30 — **EXECUTIVE PANEL DISCUSSION** — **Legal requirements for Swiss organisations within the European and Swiss regulatory frameworks**

Juan Carlos Lopez Ruggiero, CISO, Enotrac (Moderator); **Philipp Grabher,** CISO, Canton Zurich; **Alga Condoleo,** Attorney, Condoleo Law; **Dr Michel Verde,** Attorney at Law, Lustenberger + Partners

- Mandatory legal steps for Swiss organisations
- Key regulatory frameworks
- Critical compliance requirements
- Impact of emerging technologies on future regulatory frameworks
- How can CISOs guard against their own liability? Is insurance a consideration?

15:00 — **Protecting service accounts – are safeguarding non-human identities with high privileges a luxury or a critical necessity?**

Dr. Shahriar Daneshjoo, VP Sales – EMEA Central, Silverfort

- Why Machine-to-Machine (M2M) accounts, also known as service or non-human accounts, are so difficult to protect
- How to automatically discover, monitor and protect every service account in your environment
- Why the visibility and protection of service accounts have become indispensable elements of a comprehensive cybersecurity strategy
- Which approaches currently exist to mitigate this risk and their limitations

15:20 — **From risk management to ransomware mitigation: Enhancing supply chain security with SOCRadar**

Ali Marwani, Senior Solutions Engineer, SOCRadar

- Comprehensive third-party risk management
- Proactive monitoring and response
- Enhancing internal security protocols and employee awareness
- Mitigating ransomware threats

15:40 — **Education Seminars | Session 3**

CrowdStrike	CyberProof
Hunting threats and adversaries: News and best practices from the front lines of cyber-defence	**The attacker's POV: How to build the right continuous threat exposure management (CTEM) programme to reduce risk**
Philipp Wachinger, Sales Engineer, CrowdStrike	**Matt Baird,** Lead Solutions Architect, CyberProof, a UST company

16:20 — Networking break

16:40 — **CISO daily challenges**

Simon Brady, Managing Editor & Event Chairman, AKJ Associates (Moderator); **Sandro Waelchli,** CISO, Bank Avera; **Hélène Mourgue d'Algue,** Chief Information Officer (CIO) and Head of Information Systems & Digital Technology, City of Bienne; **Christophe Monigadon,** CISO, Visana Services AG; **Richard Kearney,** CISO, Octapharma

- What are your biggest challenges in the day-to-day battle of protecting your customers and organisation? What threats worry you the most?
- Security versus resilience: aligning security priorities with organisational objectives. How do you prioritise, and do you feel supported and heard when airing concerns?
- How do you assess and prepare for the threat of state-sponsored cyber-attacks targeting your organisation? What strategies do you have in place to ensure cloud security and manage associated risks?
- In the event of a significant cyber-incident, what are the key components of your incident response strategy, and how do you ensure that your organisation can quickly recover and continue operations?
- With the regulatory environment continually evolving, and with new data protection laws and cybersecurity regulations being introduced, how do you ensure your organisation remains compliant with both local and international regulations, and what challenges does this bring?
- What are the primary advantages you see in integrating AI into your organisation's cybersecurity framework, and how have these benefits manifested so far?
- What challenges have you encountered while implementing AI-driven cybersecurity solutions, and how have you addressed these obstacles?

17:10 — **LIVE DEMONSTRATION: Weaponising AI – The Deep Fake Central Banking Heist**

Manit Sahib, Ethical Hacker, The Global Fund

- Overview: How AI is being weaponised in the wild for malicious activities
- Use-cases: How to weaponise AI for your own offensive operations
- Weaponising AI for cyber-attacks: [The Deep Fake Central Banking Heist]
- Exploring how APAC was compromised for $25m with AI and deep fakes
- Live demonstration: How easy is it to create a deep fake to steal gold, print money and disrupt the global economy?

17:30 — Chair's closing remarks — **17:35** — End of conference

Education Seminars

CrowdStrike

Hunting threats and adversaries: News and best practices from the front lines of cyber-defence

Philipp Wachinger, Sales Engineer, CrowdStrike

Attendees will learn:

- Find out about significant adversary activity and their preferred targets and attack vectors in the last 12 months
- Learn about and from real incidents observed by CrowdStrike's Counter-Adversary-Operations Team
- Take away practical insights in how you can protect against modern adversaries and their TTPs
- Never forget the five key steps to be prepared

CyberProof

The attacker's POV: How to build the right continuous threat exposure management (CTEM) programme to reduce risk

Matt Baird, Lead Solutions Architect, CyberProof, a UST company

Today's cybersecurity leaders are under constant pressure to demonstrate their ability to manage risks effectively. With threats constantly evolving, companies need dynamic strategies to mitigate risks, especially in the cloud. This session will explore how CISOs can use Cyber Threat Exposure Management (CTEM) to stay ahead of threats and maintain strong security by analysing attack methods and threat actor behaviour.

The only way security practitioners can effectively manage the ever-changing threat landscape and maximise defensive strategies is by leveraging automation, orchestration, and continuous, evidence-based validation of the tools and technologies deployed in their enterprise environment. Effective threat management must be an ongoing, continuous, and integrated service, not just a one-time analysis or isolated mitigation effort.

Attendees will learn:

- Generating an effective organisational threat profile
- Identifying the threat actors and adversarial TTPs that pose the greatest risk to your organisation
- Understanding the business and security risks of threat exposure
- Gathering meaningful metrics to develop the business case for enhanced cybersecurity
- Developing a threat management programme that is continuous, efficient, and proactive

Netskope

Why identity alone is not enough for a Zero Trust strategy

Frank Barthel, Manager Solutions Engineering DACH, Netskope

The new reality of living in a hyperconnected online world requires a new approach to security, where multiple elements must be taken into account, besides simply blocking/allowing access to a specific service or the user identity to enforcing granular permissions.

Attendees will learn:

- Learn why the context is important to enforce a granular and effective security policy
- Discover which are the elements that must be considered, besides identity, to adopt an effective Zero Trust strategy
- Understand how the different security controls, such as data protection, threat protection, behaviour analytics, cooperate to protect the modern enterprise

Recorded Future

Take a proactive approach to ransomware mitigation!

Joël Giger, Intelligence Consultant, Recorded Future

With its staggering rise in attacks and its devastating consequences, ransomware is no longer just a security problem; it is now a business problem and needs a proactive approach.

Attendees will learn:

- Recent trends in ransomware activity across region
- How intelligence can help prevent or mitigate ransomware attacks
- How monitoring ransomware leak sites can provide an early warning of potential data leakage
- Why a holistic approach is required to meet the challenges

SpyCloud **It started with a cookie: Zero Trust & the rise of session hijacking** **Alfonso Hermosillo,** Senior Solutions Engineer, 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
SUSE **We need to talk about security in our containerised workloads** **Dieter Reuter,** Solutions Engineer – NeuVector, SUSE	Securing your container workloads with modern security tools that gives you peace of mind. Let's talk also about Zero Trust and why it is so important. Attendees will learn: • Why our are standard tools are not enough • Containerised workloads and security concerns • Protecting your modern workloads