Post event report

The 2nd e-Crime & Cybersecurity Switzerland

21st September 2023 | Zurich

Strategic Sponsors

CLOUDFLARE

Ontinue

proofpoint.

SentinelOne

Education Seminar Sponsors

CROWDSTRIKE

eb-Qual

netskope

Recorded Future

RELIAQUEST

SECLORE

SUSE

Branding Sponsors

MENLO SECURITY

SpyCloud

> “ The conference was incredibly valuable and dynamic. The diversity in sessions, catering to both CISOs and the business aspects, along with practical operational segments, was commendable. The sponsor presentations were also impressively executed. ”

Group IT Security Operator, Alpiq

> “ The plenary sessions and Education Seminars were very informative, as was the opportunity to network. I learned and was able to refresh my knowledge, the organisation was of very good quality. ”

Market Support & Solutions Expert | Fraud & Risk, Nestlé

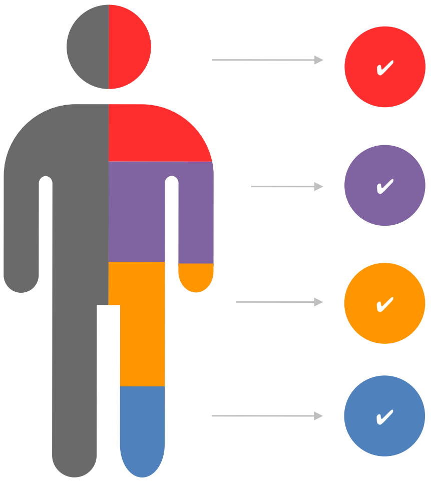
Inside this report:

Sponsors
Key themes
Who attended?
Speakers
Agenda
Education Seminars

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
- The rise and rise of effective cybersecurity regulation
- Keeping citizens safe
- From smart machines to smart cities - securing the IoT
- Reining in BigTech
- Developing the next generation of security leaders
- Securing digital currencies and DLT

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

Monika Atanasova, Global Head of Cyber TPRM, **Raiffeisen Group – Switzerland**

Rebecca Gibergues, Regional Director, France & Southern Europe, **FS-ISAC**

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

Javier Gonzalez, Senior Information Security Analyst, **Roche**

Philipp Grabher, CISO, **Canton Zurich**

Andreas Grzess, **ReliaQuest**

Theus Hossmann, Director of Data Science, **Ontinue**

Tom Kretzschmar, PreSales Engineer, **Proofpoint**

Nevena Lazarevic, Security Technology Specialist, **Microsoft**

Juan Carlos Lopez Ruggiero, CISO, **Bouygues Energies & Services**

Holger Moenius, NeuVector Sales Executive DACH, Benelux, Nordics & South, **SUSE**

Paolo Passeri, Principal Sales Engineer and Cyber Intelligence Specialist, **Netskope**

Dominik Raub, CISO, Crypto Finance AGMark Impini, Head of Information Security, **Swissquote**

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

Manit Sahib, Ethical Hacker, Contracted to **Global Fund**

Raj Sandhu, Ethical Hacker, Contracted to **World Health Organisation**

Jeff Schiemann, CISO, **SEBA Bank AG**

Jasbir Singh, Partner and Managing Director Europe, **Seclore Technologies**

Philipp Wachinger, Sales Engineer, **CrowdStrike**

Sammie Walden, Banking Expert DACH, **Cloudflare**

Fabian Wuest, Head of Security, **Bank CIC**

Thomas Wüst, Sales Lead Switzerland, **SentinelOne**

Marcel Zumbühl, CISO, **Swiss Post**

Agenda

08:00	Registration and networking break
08:50	Chairman's welcome
09:00	**Feeling secure or being secure? That is the question**
	Philipp Grabher, CISO, Canton Zurich • What do we understand when speaking about Security Theatre? • How can we address Security Theatre in our organisations? • Three concrete use-cases
09:20	**The new cyber-threat landscape Switzerland**
	Sammie Walden, Banking Expert DACH, Cloudflare • Cyber-threat landscape international and Switzerland • Why employee security training falls short • What can you do today to shut down one of the biggest attack vendors?
09:40	**What is the key to successfully engage on cybersecurity with executive and supervisory boards?**
	Marcel Zumbühl, CISO, Swiss Post • As CISO you meet with executive and supervisory boards, what do these boards expect from you? • How do you prepare to make these encounters a win for the cybersecurity of your company?
10:00	**Education Seminars | Session 1**
	Netskope **Understanding the cloud-native threat landscape** **Paolo Passeri,** Principal Sales Engineer and Cyber Intelligence Specialist, Netskope
	Seclore Technologies **Know, protect and control your data** **Jasbir Singh,** Partner and Managing Director Europe, Seclore Technologies
10:40	Networking break
11:10	**EXECUTIVE PANEL DISCUSSION** **CISO panel discussion**
	Juan Carlos Lopez Ruggiero, CISO, Bouygues Energies & Services, (Moderator); **Fabian Wuest,** Head of Security, Bank CIC; **Philipp Grabher,** CISO, Canton Zurich; **Rebecca Gibergues,** Regional Director, France & Southern Europe, FS-ISAC; **Javier Gonzalez,** Senior Information Security Analyst, Roche • Learning from a recent cyber-attack on Swiss federal agencies and state-linked companies • Third-parties risks and threats for Switzerland • Overcoming the skills shortage in the Swiss market • Are CISOs under budget pressure? Is there pressure to outsource?
11:40	**Generative AI: What will change with the rise of GPT in cybersecurity?**
	Theus Hossmann, Director of Data Science, Ontinue, and **Nevena Lazarevic,** Security Technology Specialist, Microsoft • The impact of generative AI like GPT on security operations • Innovative use-cases beyond detection of malicious activity • The inevitable prospect of attackers using AI
12:00	**Break the attack chain: Strengthening defences and safeguarding people and data**
	Tom Kretzschmar, PreSales Engineer, Proofpoint • People are the primary targets of today's advanced attacks. But most organisations aren't centering their security strategy around their people • It is critical to align protection with risks targeting users throughout the attack chain – from initial compromise to lateral movement to impact • In this session, you will get an overview of the evolving threat landscape and proactive strategies you can implement to protect your organisation and break the attack chain at every stage

Agenda

12:20	**Education Seminars | Session 2**	
	Recorded Future **Unspoken words with immense criminal potential** **Joël Giger,** Intelligence Consultant, Recorded Future	SUSE **Importance of Zero Trust security in Kubernetes environments** **Holger Moenius,** NeuVector Sales Executive DACH, Benelux, Nordics & South, SUSE, and **Dieter Reuter,** Solutions Engineer, NeuVector, SUSE
13:00	Lunch and networking break	
14:00	**Shaping the future of Cyber TPRM by unlocking the potential of automation & digitalisation – lessons learned & best practices, case study**	
	Monika Atanasova, Global Head of Cyber TPRM, Raiffeisen Group – Switzerland • Main aspects of the Cyber TPRM programme • Security assessments workflow automation • Comprehensive Cyber TPRM profiling • Reporting: KPIs/KRIs cyber-risk cockpit • AI & threat intelligence	
14:20	**Human-machine teaming – AI in cybersecurity: Why the human element will always be indispensable in cybersecurity**	
	Thomas Wüst, Sales Lead Switzerland, SentinelOne • What the current AI 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	
14:40	**Bypassing multi-factor authentication (MFA) via phishing techniques**	
	Raj Sandhu, Ethical Hacker, Contracted to World Health Organisation, and **Manit Sahib,** Ethical Hacker, Contracted to Global Fund • Introduction to MFA bypass phishing techniques • Live demonstration of MFA bypass attack • Countermeasures and best practices • Conclusion of demo and presentation	
15:00	**Education Seminars | Session 3**	
	CrowdStrike **Nowhere to hide – key insights into adversary tradecraft 2023** **Philipp Wachinger,** Sales Engineer, CrowdStrike	ReliaQuest **The future of security operations** **Andreas Grzess,** ReliaQuest
15:40	Networking break	
16:10	**EXECUTIVE PANEL DISCUSSION** **Crypto CISOs open questions**	
	Jeff Schiemann, CISO, SEBA Bank AG (Moderator); **Dominik Raub,** CISO, Crypto Finance AG **Mark Impini,** Head of Information Security, Swissquote • What is the impact of crypto fraud and crime? • What is our focus for the next 6–9 months? • What is 'a day in the life' of a crypto CISO like?	
16:40	Chairman's closing remarks	
16:50	Conference close	

Education Seminars	
CrowdStrike **Nowhere to hide – key insights into adversary tradecraft 2023** **Philipp Wachinger,** Sales Engineer, CrowdStrike	Your ability to defeat advanced cyber-threats rests almost entirely on your understanding of the problem. And the problem isn't malware – it's the adversaries. While technologies and security products that organisations rely on are evolving, they struggle to keep up with the alarming pace at which adversary tooling and tradecraft is evolving. In all incidents observed by CrowdStrike's specialist teams, adversaries looked for ways to broaden their reach, optimise their tradecraft and deepen their impact on targets. To gain access, the intrusion attempts often started with an identity compromise or the exploitation of vulnerable software. In addition, adversaries have been quick to learn how to take advantage of common misconfigurations in public cloud services. To stop these adversaries, it is imperative that security teams understand how they operate. • 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 five key steps to stay ahead of the threat actor
Netskope **Understanding the cloud-native threat landscape** **Paolo Passeri,** Principal Sales Engineer and Cyber Intelligence Specialist, Netskope	The consolidated adoption of cloud services and the distribution of the workforce have led to a new paradigm in the threat landscape. Threat actors are capitalising on the fact that users access their data from any location and any device, even the personal ones, and also on the fact that they have progressively replaced human interactions with digital interactions. The attackers are launching evasive campaigns that exploit the trust on cloud services and collaboration tools, but they are also dusting off more traditional techniques such as sophisticated social engineering and SEO poisoning campaigns that exploit the unconditional trust on search engines and online tools in general. Join this session to: • Understand what are cloud-native threats and why they are more evasive than traditional web-based threats • Understand the most common attack techniques • Gain a comprehensive view of the current threat landscape • Learn how to mitigate the risks with a security culture and a cloud-delivered security model
Recorded Future **Unspoken words with immense criminal potential** **Joël Giger,** Intelligence Consultant, Recorded Future	The recent boom in artificial intelligence capability has led to the creation of beautiful art and writing of essays within seconds, but threat actors have not stood idly by. In this session, you will learn about: • The rise of Voice-Cloning-as-a-Service offerings, a new form of commodified cybercrime • Current use cases, future potential and possible impact for your organisation • Not all is lost – old mitigation techniques work against new threats, at least for now
ReliaQuest **The future of security operations** **Andreas Grzess,** 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

Seclore Technologies **Know, protect and control your data** **Jasbir Singh,** Partner and Managing Director Europe, Seclore Technologies	In the fast-paced digital age, safeguarding digital assets has become more crucial than ever. This education seminar delves into the key topics essential for effective data protection. Jasbir Singh introduces an approach that revolves around understanding the data landscape within an organisation: The key to establishing a robust security framework and compliance includes to set labels to the documents, track and visualise the usage but always to protect & control confidential information. By understanding the value of data, classifying it, and implementing usage controls based on classification labels, organisations can stay one step ahead of cyber-threats and safeguard their digital assets effectively. A safeguard that goes beyond the security perimeter of an organisation, allowing usage control updates and even remote revocation of shared data at any time. The seminar will also outline why classification can act as a first layer of security and the importance of dynamic watermarks to deter or detect data leakage. In this session, you will learn: • Why we need data-centric security in today's landscape • How to know, protect and control sensitive information • Example: An integration of data-centric security into the M365 landscape
SUSE **Importance of Zero Trust security in Kubernetes environments** **Holger Moenius,** NeuVector Sales Executive DACH, Benelux, Nordics & South, SUSE, and **Dieter Reuter,** Solutions Engineer, NeuVector, SUSE	Deep network visibility is the most critical part of run-time container security. In traditional perimeter-based security, administrators deploy firewalls to quarantine or block attacks before they reach the workload. Inspecting container network traffic reveals how an application communicates with other applications and it's the only place that can stop attacks before they reach the application or workload. SUSE NeuVector is the only 100% open source Zero Trust container security platform with continuous audits throughout the full lifecycle. • Perform deep packet inspection (DPI) • Real-time protection with the industry's only container firewall • Monitor 'east-west' and 'north-south' container traffic • Capture packets for debugging and threat investigation