

Post event report



The 1st e-Crime & Cybersecurity
Switzerland

28th September 2022 | Zurich

Strategic Sponsors

DARKTRACE



KnowBe4
Human error. Conquered.

MANDIANT
YOUR CYBERSECURITY ADVANTAGE



Education Seminar Sponsors



**Counter
Craft**



SECLORE



Networking Sponsors



“ The 1st e-Crime event in Zurich provided useful insights on new available products in the security area and the format was meeting my expectations. ”

Chief Security Officer, LGT Group

“ e-Crime Congress Switzerland was a valuable experience. In a handful of hours I collected many relevant updates and hits about the evolving cybersecurity scenario and I had the opportunity to network with many peers. The discrete presence of brands relevant to the segment also allowed for contacts to be developed. ”

Director Global IT Infrastructure and Security, Burckhardt Compression AG

“ I think you raised the bar this year in terms of presenters, topics and open panels. I enjoyed the presentations and found a lot of useful information during the day. Did a lot of networking especially with the vendors, which seemed to be perfectly aligned with current security needs, so I have already booked a follow up meeting with a few of them. Overall, a great event and great organisation; looking forward to next year's conference. ”

Head of Information Security and Risk Management, Qliro

Inside this report:

Sponsors

Key themes

Who attended?

Speakers

Agenda

Education Seminars



Speakers

Andrea Arquint, Senior Solutions Engineer, **F5 Switzerland GmbH**

Simon Brady, Managing Editor, **AKJ Associates**

Albert Brauchli, Country Manager, **Mandiant Switzerland**

Olivier Busolini, Chief Information Security Officer, **Sygnum Bank**

Conrado Crespo, Senior Sales Engineer, **CounterCraft**

Michele Federici, Head of IT Security, **Dialectic AG**

Captain Patrick Ghion, Head Regional **Cyber Competence Center for Western Switzerland (RC3)**

Marcel Gill, Account Director, **Darktrace**

Philipp Grabher, Chief Information Security Officer, **Canton of Zurich**

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

Florian Hartmann, Senior Sales Engineer, **CrowdStrike**

Julian Kanitz, Lead Sales Engineer, DACH, **Recorded Future**

Achim Kraus, Technical Solution Architect, **Gatewatcher**

Wade Lance, Field CISO, **Synack**

Javvad Malik, Lead Security Awareness Advocate, **KnowBe4**

Aneta Podsiadla, Data Protection & Compliance Officer, **Vorwerk**

Dr. Dominik Raub, Chief Information Security Officer, **Crypto Finance AG**

Brett Raybould, EMEA Solutions Architect, **Menlo Security**

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

Alain Salesse, Senior Sales Engineer, **Cofense**

Tom Schmidt, Partner, **EY**

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

Philippe Vuilleumier, Chief Security Officer, **Swisscom**

Ralf Winzer, Group Information Security Officer/ Group Data Protection Officer, **Zehnder Group International AG**

Manuel Wolf, Security Expert, Alps, **SentinelOne**

Marcel Wuestner, Account Director, **Darktrace**

Key themes

Are we exaggerating cloud issues?

Is ransomware just going to keep getting worse?

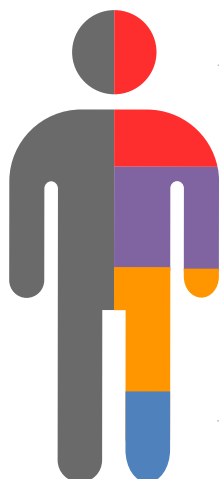
Can zero trust be done?

What does DORA mean for you?

Closing the cybersecurity skills gap

From threat/security to risk/resilience

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

Agenda			
08:00	Registration & networking		
08:50	Chairperson's welcome		
09:00	Securing the digital citizen: A public sector view Philipp Grabher , Chief Information Security Officer, Canton of Zurich <ul style="list-style-type: none"> • Cybersecurity strategy for the Canton of Zurich • Supporting and inter-sector cooperation: raising awareness • The big three areas – what to focus on 		
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: <ul style="list-style-type: none"> • 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	Debunking common myths about XDR Manuel Wolf , Security Expert, Alps, SentinelOne <ul style="list-style-type: none"> • What is XDR and why should I consider the technology in my enterprise security stack? • What should I expect from vendors who claim to have built the perfect mousetrap? • What is reality, and what is just hype? • This session is intended to debunk a few common myths that continue to muddy the water for security teams 		
10:00	The vulnerability vector: An opportunity for the hacker and a challenge for the CISO Juan Carlos López Ruggiero , CISO, Bouygues Energies & Services <ul style="list-style-type: none"> • Malicious actors are so much better organised (and financed) than company CISOs • How do we survive the threats and stay one step ahead? • What works and what doesn't when facing the challenges in an ever changing scenario? 		
10:20	Education Seminars Session 1 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 60%; padding: 5px;"> Seclore Technologies Data-centric security for data protection Every digital asset Everywhere Jasbir Singh, Partner and Managing Director Europe, Seclore Technologies </td> <td style="width: 40%; padding: 5px;"> Synack Staying secure in the midst of the talent crisis Wade Lance, Field CISO, Synack </td> </tr> </table>	Seclore Technologies Data-centric security for data protection Every digital asset Everywhere Jasbir Singh , Partner and Managing Director Europe, Seclore Technologies	Synack Staying secure in the midst of the talent crisis Wade Lance , Field CISO, Synack
Seclore Technologies Data-centric security for data protection Every digital asset Everywhere Jasbir Singh , Partner and Managing Director Europe, Seclore Technologies	Synack Staying secure in the midst of the talent crisis Wade Lance , Field CISO, Synack		
11:00	Networking break		
11:30	EXECUTIVE PANEL DISCUSSION Balancing regulation/compliance and security Tom Schmidt , Partner, EY (Moderator); Aneta Podsiadla , Data Protection & Compliance Officer, Vorwerk; Juan Carlos Lopez Ruggiero , Chief Information Security Officer, Bouygues Energies & Services; Ralf Winzer , Group Information Security Officer/ Group Data Protection Officer, Zehnder Group International AG; Olivier Busolini , CISO, Sygnum Bank; Dr. Dominik Raub , Chief Information Security Officer, Crypto Finance AG <ul style="list-style-type: none"> • How do new resilience regulations help in the battle against cybercriminals (NIS2 and DORA) and the impacts of the coming complete revamp of the FINMA 2008/21 circular for Swiss banks? • Does cybersecurity fit naturally into the three lines of defence model? • Third-party dependency 		
11:50	Distributed cloud services: Uniform security controls for distributed infrastructures Andrea Arquint , Senior Solutions Engineer, F5 Switzerland GmbH <ul style="list-style-type: none"> • Distributed cloud -> the infrastructure should become completely transparent, allowing customers to move seamlessly between environments • An overlay that helps improve the quality of each individual cloud, with a single, central system that interconnects them all • Spend less time fiddling with infrastructure • Release new applications faster • Reduce annual expenses • Do not limit the ability of innovators to use best-of-breed services 		

Agenda			
12:10	How AI can think like an attacker Marcel Gill , Account Director and Marcel Wuestner , Account Director, Darktrace <ul style="list-style-type: none"> In the face of skyrocketing cyber-risk, detecting and responding to attacks is no longer enough Organisations must take proactive steps to prevent threats before they happen, and to recover if compromised Darktrace unveils an ambitious new approach to security, with core engines powering AI technologies to prevent, detect, respond, and ultimately heal from attacks Together, these engines combine to strengthen organisations' security posture in a virtuous AI feedback 'loop,' which provides powerful end-to-end, bespoke, and self-learning solutions unique to each organisation 		
12:30	It's more than phishing – how to supercharge your security awareness programme Javvad Malik , Lead Security Awareness Advocate, KnowBe4 <ul style="list-style-type: none"> Why you need to brand the security department the right way The psychological approach to getting your message across Practical advice on building a strong security culture 		
12:50	Education Seminars Session 2 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;"> Cofense Combatting the latest phishing threats – why an adaptive layered defence is the ONLY offence for Swiss organisations Alain Salesse, Senior Sales Engineer, Cofense </td> <td style="width: 50%; padding: 5px;"> CounterCraft Adversary driven threat intelligence: Understand how cyber-deception will help your organisation make intelligent business-driven decisions Conrado Crespo, Senior Sales Engineer, CounterCraft </td> </tr> </table>	Cofense Combatting the latest phishing threats – why an adaptive layered defence is the ONLY offence for Swiss organisations Alain Salesse , Senior Sales Engineer, Cofense	CounterCraft Adversary driven threat intelligence: Understand how cyber-deception will help your organisation make intelligent business-driven decisions Conrado Crespo , Senior Sales Engineer, CounterCraft
Cofense Combatting the latest phishing threats – why an adaptive layered defence is the ONLY offence for Swiss organisations Alain Salesse , Senior Sales Engineer, Cofense	CounterCraft Adversary driven threat intelligence: Understand how cyber-deception will help your organisation make intelligent business-driven decisions Conrado Crespo , Senior Sales Engineer, CounterCraft		
13:30	Lunch & networking break		
14:30	The cloud security journey Olivier Busolini , Chief Information Security Officer, Sygnum Bank <ul style="list-style-type: none"> The implicit choices of starting a cloud(s) journey The key cloud security risks to evaluate The most important security principles and measures when running workloads in cloud(s) The implications of the shared responsibility model of data protection 		
14:50	Activating cyber-threat intelligence Albert Brauchli , Country Manager, Mandiant Switzerland Mandiant responders are on the frontlines every day, investigating and analysing the latest attacks and threats, and understanding how best to respond to and mitigate them. Everything we learn is passed on to our customers through our various services, giving them a much needed advantage in a constantly evolving threat landscape. <ul style="list-style-type: none"> Mandiant identified trends Cyber-threat intelligence provides tactical, operational and strategic support Cyber-threat profile Defender's advantage 		
15:10	Getting out of the terminological confusion around security concepts: What is really new and relevant? Achim Kraus , Technical Solution Architect, GATEWATCHER <ul style="list-style-type: none"> Security operations: Latest terminologies (SIEM, SOAR, NDR; EDR, XDR, MDR...) – so what ? Zero Trust & attack surface: 'Threat hunting' – way before detection Team efficiency will come from integration of data and automation Where to start: Levels of maturity and deployment 		
15:30	Education Seminars Session 3 <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; padding: 5px;"> CrowdStrike Understanding the true threats to identity against the modern threat actor Florian Hartmann, Senior Sales Engineer, CrowdStrike </td> <td style="width: 50%; padding: 5px;"> Menlo Security The next class of browser-based attacks Brett Raybould, EMEA Solutions Architect, Menlo Security </td> </tr> </table>	CrowdStrike Understanding the true threats to identity against the modern threat actor Florian Hartmann , Senior Sales Engineer, CrowdStrike	Menlo Security The next class of browser-based attacks Brett Raybould , EMEA Solutions Architect, Menlo Security
CrowdStrike Understanding the true threats to identity against the modern threat actor Florian Hartmann , Senior Sales Engineer, CrowdStrike	Menlo Security The next class of browser-based attacks Brett Raybould , EMEA Solutions Architect, Menlo Security		
16:10	Networking break		
16:30	Securing client assets – in the context of escalating cyber-threat Dr. Dominik Raub , Chief Information Security Officer, Crypto Finance AG <ul style="list-style-type: none"> Blockchain vs classical assets from a cyber-threat exposure perspective Information security threat landscape and securing client assets as central protection goals for a blockchain asset company Using secure hardware and sound security architecture to mitigate risks and secure client assets Residual risks to client assets and further recommended defences 		
16:50	SENIOR LEADERSHIP PANEL What's on the horizon? Simon Brady , Managing Editor, AKJ Associates (Moderator); Philippe Vuilleumier , Chief Security Officer, Swisscom; Captain Patrick Ghion , Head Regional Cyber Competence Center for Western Switzerland (RC3); Klaus Haller , Senior Security Architect, AXA; Michele Federici , Head of IT Security, Dialectic AG <ul style="list-style-type: none"> What's on the horizon, and how to we ensure security in a complex ecosystem? How do we ensure customer trust and strive to make society more cyber-immune? How do we protect artificial intelligence in the future? How do we cope with the fact that computing power will put our current encryption mechanisms at risk, etc.? 		
17:30	Conference close		

Education Seminars	
<p>Cofense</p> <p>Combatting the latest phishing threats – why an adaptive layered defence is the ONLY offence for Swiss organisations</p> <p>Alain Salsesse, Senior Sales Engineer, Cofense</p>	<ul style="list-style-type: none"> • <i>What is an adaptive security architecture and what are the objectives?</i> –With so much focus on cyber-attack prevention, many security teams have adopted an incident response mindset versus one that assumes systems are compromised and require continuous monitoring and remediation. We’ll walk you through the benefits and objectives of implementing an adaptive security architecture and risk framework. • <i>The current situation in email and phishing security</i> –We’ll share some of the latest insights from the industry and what we’re seeing through our unique combination of artificial, human, and high-fidelity intelligence. • <i>Implementing adaptive security architecture and risk framework with Cofense</i> –We’ll talk through how to classify your existing and potential email security investments to increase your security posture while reducing costs, vendors, and configuration complexity.
<p>CounterCraft</p> <p>Adversary driven threat intelligence: Understand how cyber-deception will help your organisation make intelligent business-driven decisions</p> <p>Conrado Crespo, Senior Sales Engineer, CounterCraft</p>	<p>Join this session to find out more on:</p> <ul style="list-style-type: none"> • Limited value in generic intelligence: why is the traditional threat intelligence broken? • Can deception technology really provide actionable intelligence? How does it work? • What are the risks involved in adopting this approach? • Am I mature (from a security operations perspective) enough to leverage this approach?
<p>CrowdStrike</p> <p>Understanding the true threats to identity against the modern threat actor</p> <p>Florian Hartmann, Senior Sales Engineer, CrowdStrike</p>	<p>Modern adversaries no longer break in, they login. An attacker with compromised credentials has free reign to move about an organisation and carefully plan their attack before they strike.</p> <p>In more than 80% of modern attacks, threat actors are using valid credentials. It’s not zero days or phishing that should be your concern from attackers, it’s that they already have the keys to your kingdom.</p> <p>Join us to further understand:</p> <ul style="list-style-type: none"> • The history of identity and identity architecture • The identity threat landscape • Identity attack techniques by e-crime and nation-state actors • Best practices for solving the identity problem
<p>Menlo Security</p> <p>The next class of browser-based attacks</p> <p>Brett Raybould, EMEA Solutions Architect, Menlo Security</p>	<p>There are two distinct characteristics that all threat actors tend to share. First, they focus on avoiding detection by any means. Second, while some go after specific targets, many opt to aim their tactics at the vectors that will reap the greatest rewards. After all, a small pond with many fish increases everyone’s chances of success.</p> <p>Between July and December 2021, there was a 224% increase in highly evasive adaptive threats (HEAT) attacks – a class of cyber-threats targeting web browsers as the attack vector. While malware once had to be downloaded to pose a real risk, now, it’s a dynamically generated threat toolkit built in the web where employees are productive.</p> <p>In this session, you will:</p> <ul style="list-style-type: none"> • Discover the anatomy of recent browser-based attacks • Learn why network security today is broken • Experience a live demo that enables you to discover the technology approach proven to eliminate these threats

<p>Seclore Technologies</p> <p>Data-Centric security for data protection Every digital asset Everywhere</p> <p>Jasbir Singh, Partner and Managing Director Europe, Seclore Technologies</p>	<p>IT environments digital borders have shifted significantly over the last years. WFH, BYOD, Cloud, collaboration plus evolving hacker tactics and new compliance regulations are causing a lot of pressure on organisations. What should the boundaries of your IT environment look like today, with evolving technology and remote workforces?</p> <p>Jasbir Singh will discuss the challenges of traditional security solutions in a world of disappearing borders and how data-centric-security can address these challenges in a centralised and transparent way.</p> <p>We will explore:</p> <ul style="list-style-type: none"> • How to protect your organisation against insider threats • How to ensure secure collaboration • Mitigating third-party risk by protecting your data everywhere • Data-centric security as a cornerstone to staying compliant
<p>Synack</p> <p>Staying secure in the midst of the talent crisis</p> <p>Wade Lance, Field CISO, Synack</p>	<p>The worldwide cyber-talent shortage is real and growing. Just in the US there are 1 million people employed as cybersecurity professionals, but over 700,000 unfilled job postings and that number is growing at an alarming rate. Globally, the gap is at least 2.7 million. Initiatives are underway to address the shortage spanning government, industry groups, and the private sector, however the short-term cybersecurity implications are alarming. The lack of skilled practitioners extends beyond the issue of headcount – deficiencies exist in capability, diversity, morale and more. But effective and innovative solutions can bridge the talent gap and address both near term and longer term needs.</p> <p>In this session, we will discuss:</p> <ul style="list-style-type: none"> • Current options to increase the cyber-talent capacity required to meet organisations' current and future security needs • Broadening the diversity of available security skill sets to cover the full scope of vulnerabilities for on-premise, cloud, networking, hosts, mobile, applications, etc. • The challenges, and importance, of establishing a continuous testing practice to keep pace with the continuous application development and deployment methodologies • The advantages of leveraging a global researcher community as part of your security operations • The importance of standard testing frameworks and operational transparency in leveraging untapped and available security talent