SWITZERLAND

Connect | Educate | Inspire | Secure

www.isc2chapter-switzerland.ch

#csc2018ch

Chapter Security Conference 2018

Friday 28th September 8:30 – 18:00 @ Auditorium, Technopark Zurich

08:30 - 09:00	Registration & Welcoming Coffee
09:00 - 09:10	John Alexakis, President, (ISC)2 Chapter Switzerland Welcome & Opening Remarks
	Morning Session. Topics: Banks, Cloud
09:10 – 10:00	Alain Beuchat, Chief Information Security Officer, UBS Keynote – S1: Cyber Risk Management The focus of the presentation will be on the management of cyber risk at an international bank. The first step is to develop a common understanding of what cyber risk means for the organization. Cyber security frameworks are essential to define the holistic approach to cyber risk but there is also a need to have a deep understanding of how cyber-attacks work. Lastly the risk management approach is discussed with a focus on the key elements to address the risk.
10:00 – 10:30	Ilias Raftopoulos, Enterprise Security Architect, Credit Suisse S2: Credit Suisse journey through the clouds If you want a tough engineering problem, take a 162-year-old bank and try to connect it to today's modern cloud services. In this talk we will be following Credit Suisse's IT cloud transformation, with emphasis on the security and compliance implications. Moreover, we will go through the challenges a financial organization has to face in order to become a technology company.
10:30 – 11:00	Mauro Verderosa, IT Security Specialist & CEO at PSYND S3: Implementing your IAM over the Cloud In the latest years companies are migrating their systems on premise to cloud solutions. Before this transformation takes place, it's needed to run a deep analysis to be sure that processes and internal policies are respected. Moreover, the security is playing a key factor because, without the needed protection, business confidential information could be wrongly exposed to Internet generating a data loss that could compromise the business of a company. Discover what measures should be implemented to enforce the access control in the cloud and what are the key points that should be considered before developing a secure infrastructure.
11:00 – 11:20	Coffee Break

	Midday session. Topics: GDPR, IoT/Mobile
11:20 – 12:10	**Daniela Fábián Masoch, Attorney at Law & Privacy Professional, Fabian Privacy Legal GmbH** **S4: GDPR the first 100 days** The EU General Data Protection Regulation (GDPR) entered into force on May 25, 2018. The new law has gained very high attention, not only in the EU but worldwide. Many enterprises have worked intensively over the past 2 or more years on preparing for GDPR compliance. While companies have put their energy into developing their privacy programs and on managing the external facing aspects, such as the website privacy notice, cookies policy and the establishment of contracts and safeguards with third parties, we now see the focus on internal aspects and in particular in the practical implementation of accountability and the privacy program. At the same time, companies with more advanced programs struggle with the question how to apply the privacy principles in connection with the digital revolution, including technologies such as Internet of Things, Artificial Intelligence and Machine Learning, and finally Blockchain.
12:10 – 13:00	**Romuald Szkudlarek, Senior Cyber Security Architect, Schneider Electric** **S5: A perspective on mobile security in IoT and how OWASP can help** OWASP is strongly committed to application security as a whole, and since a long time has recognized the importance of mobile security, be it as a standalone service or as part of a larger ecosystem. After introducing the context of mobile security in IoT, we'll dive into the kind of resources OWASP can provide in this domain, the tools and processes that support their use and will explicit the value they can bring in all domains of application to IoT security through real live examples. Although this presentation may contain some technical elements, it is not technically oriented and all types of audience with any type of background is welcome (IT, development, project management, ...). Also, no particular experience on IoT / mobile technologies is required.
13:00 – 13:40	**Networking Lunch**

	Afternoon session. Topics: Blockchain, Quantum
13:40 – 14:30	**Daniel Fischmann, Lead Security Auditor, ChainSecurity** **S6: Blockchain Security** The increasing importance of blockchain and especially smart contract applications seems ubiquitous. Individuals, companies and organizations are getting actively involved in a still young field with a only recently strong focus on formal security. The presentation gives an overview on the development of blockchains and smart contracts and afterwards moves on to discuss unique attack vectors on smart contract applications. In the process, case studies of successful attacks will be shown, as well as manual methods and state-of-the-art research tools presented, which can help to mitigate these.
14:30 – 15:00	**Andreas Curiger, CTO/CSO, Securosys SA** **S7: Blockchain systems, it's all about trust** Blockchain systems are often touted to be "trustless" and hence implying to offer improved resilience against certain attacks compared to conventional, centralized IT architectures. In this talk we are going to investigate the role of trust in blockchain-based systems and show that the term "trustless" is quite misleading. As in conventional systems, a "trust anchor" is required, which essentially needs to adequately protect identities, addresses, and their handling in deployed systems.
15:00 – 15:40	**Kelly Richdale, Executive VP Quantum Safe Security, ID Quantique** **S8: Quantum Proofing your Organisation** Governments and enterprises are being forced to seriously re-assess their security in the forthcoming quantum era, as quantum computing moves from hype to reality. Today's most commonly used public key cryptographic primitives will be rendered vulnerable by quantum algorithms, breaking the security of everything from PKI to blockchain. NIST and other government bodies have recommended to move to new quantum safe cryptographic primitives. In this talk Kelly Richdale will give an update on the current status of quantum computing, and advise on different methods for achieving quantum safe security in the oncoming post-quantum era.
15:40 – 16:00	**Coffee Break**

	Final session. Topics: Business Risk Intelligence, Small budget
16:00 – 16:50	**Maurits Lucas, Director of Strategic Accounts, Flashpoint** **S9: Best Practices for Building a Successful BRI Program** Abstract: Business Risk Intelligence (BRI) enables organizations to shift away from "whack-a-mole" tactics and toward a more strategic, integrative approach that addresses not just individual threats but overall risk. Flashpoint's Maurits Lucas will explain why BRI is often considered the more strategic and cross-functional counterpart to cyber threat intelligence (CTI), and how BRI surpasses CTI's limited applications to inform decision-making, improve preparation, and mitigate a broad spectrum of cyber and physical risks. The presentation will discuss considerations for building a successful BRI program, and provide practical application through the recent developments in threats against SMS two-factor authentication. Topics covered will include: • Business Risk Intelligence (BRI): What is it, and why is it important? • BRI vs. CTI • Practical considerations for building a successful BRI program • Recent developments in threats against SMS two-factor authentication • How can BRI help organizations proactively bolster their security postures, and inform all business functions (not just cyber teams) to mitigate risk?
16:50 – 17:20	**Florian Schnettelker, IT Consultant, Avacone AG** **S10: Cybersecurity for healthcare facilities - How to ensure good cybersecurity with limited budget** Healthcare facilities are more and more under attack. Even Ransomware like WannaCry could have dramatic effects on healthcare facilities, due to different reasons like: tight budgets, knowledge gap, valuable information, cyber-physical systems and that they are part of the critical infrastructure of every country. Due to a tight budget for IT and cybersecurity in general, it is a challenging exercise to implement cost-effective cybersecurity mitigation. In this talk we will look on why healthcare facilities are so vulnerable and interesting for cyber-attacks. In addition, we will also look a little bit on how to mitigate some risks with low budget solutions, like to use raspberry pi as network monitoring equipment.
17:20 – 18:00	**Networking Reception – Apéro with beers and soft drinks**