

PERSONAL INVITATION to 28th

swiss**ciso**summit



Multi-Cloud: New Security Challenges

9th May 2023, Airport Hotel Radisson Blu, Zurich
(upon requests, virtual participation will be organized)

Sponsorships:

DETECON
CONSULTING

Platinum



Gold



Lucerne University of
Applied Sciences and Arts
**HOCHSCHULE
LUZERN
SWITCH**

Silver



Partner:

satw it's all about
technology

Contents

1

Introduction *Page 3*

2

Summary *Page 4*

3

Keynote Ia, Ib
and Roundtable I *Page 5*

4

Keynote II and
Roundtable II *Page 7*

5

Information *Page 8*

6

Registration *Page 10*

7

Sponsorships &
Partner *Page 11*

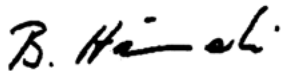
1

Introduction

Dear CISO,

You are kindly invited to the 28th Swiss CISO Summit – a series of moderated round-table discussions for sharing information security practices and strategies among senior professionals.

Please be informed that we have only a limited number of places. Therefore we kindly ask you to confirm your attendance as soon as possible.



Prof. Dr. Bernhard M. Hämmerli



Multi-Cloud: New Security Challenges

Date 9th May 2023

Time 12:00 Lunch and 13:00 Summit starts / approx. 19:00 Summit ends

Location Airport Hotel Radisson Blu, Zurich, Switzerland
Please contact Prof. Dr. Hämmerli for virtual participation.

Keynote 1 **Novel SOC challenges in EDR for multi-cloud environments**

Mark A. Barwinski, Global Head of Cyber Operation
CDIO Cyber & Information Services, UBS AG

Keynote 1b **Moving IT Security Products from on-prem to the cloud – yes or no?**

Manuel Fluri, Global Head of Network Security Engineering, Credit Suisse

Keynote 2 **Cloud Security Guardrails and Encryption Models**

Andrew Hutchison, Technical Program Manager, Information Security Engineering, Google

**Key
Benefits**

- Experience industry best practices in the Swiss market
- Participate actively in moderated high-level peer exchange
- Understand drivers for security, gain competence and experience in discussing strategic issues
- Design, develop and manage effective information security strategies for your own organisation
- Receive an exclusive consolidated end of summit report detailing all the major themes discussed for re-use in your organization

Join the Swiss CISO Summit and benefit from the peer exchange!

Summary

2

Multi-Cloud: New Security Challenges

Multi-Cloud security

Cloud is a non-stoppable development and transformation of IT infrastructure: the trend is paramount and does not depend on whether we like it or not: it is a fact. For example, regarding security, we need to understand many details to secure the cloud: We understand many concepts today for single-cloud solutions. But by today, any company uses many applications in the cloud, software-as-a-service (SaaS), as well as data storage and cloud servers which run our corporate applications. As a result, the infrastructure landscape has developed to be powerful but more complex.

At the other end, we run our endpoints in the companies and urgently need endpoint security & resilience and Endpoint Detection and Response (EDR). These concepts are promising, but their interaction with multi-cloud environments is not obvious. An exchange based on experience should make what works and needs more attention transparent.

Regulation is another issue. Is Richard Clarke, counselor for cyber security to US presidents for two decades, right, when he states in a Słotwińska computer world interview: "the Swiss Cloud is just a business model, and does not inhibit US access to the servers"? And,

of course, we have a relevant Swiss community that wants the cloud data center in Switzerland because of regulations. So our debate may result in a better understanding of the arguments of both sides: global geographic spread vs. in-country focused data residency.

Mark Barwinski will explain how SOC requirements change with EDR and multi-clouds. We must know a lot behind the scenes, such that the expected advantages of a multi-cloud SOC are to be achieved.

Manuel Fluri will share his experience with security products in the multi-cloud context. In short: it is not as expected that products can be moved from on-prem to the cloud, and the performance remains. It will be interesting to follow his experience.

Andrew Hutchison will explain what encryption and key management options customers will have to be the only ones who can access and decrypt the cloud data.

With this setup, we want to contribute to this novel multi-cloud era and exchange best practices and experiences within the security community.

3

Keynote 1a

Keynote 1a

Novel SOC challenges in EDR for multi-cloud environments

As organizations continue migration to the cloud, many seek to insulate against risks and vendor lock-in by leveraging multi-cloud environments. Implementing an EDR strategy in a multi-cloud environment presents unique challenges in cybersecurity. These include complexity, visibility, integration, resource consumption, compliance, and training. Implementing a consistent EDR strategy across all endpoints is difficult with different cloud providers, tools, and technologies. Comprehensive visibility is crucial to detect and mitigate cyber threats accurately. Integrating EDR solutions with different cloud providers' security

offerings and other security tools is critical to achieving a comprehensive security posture. Compliance with different cloud providers' regulations and standards is also essential. Finally, specialized skills and knowledge are required to operate and maintain EDR solutions in multi-cloud environments. Organizations must carefully evaluate their multi-cloud environments and select EDR solutions that integrate seamlessly with each cloud provider's security offerings, provide comprehensive visibility, meet all relevant compliance requirements, and provide comprehensive training to staff.



Mark Barwinski is the Global Head of Cyber Operations at UBS AG, where he oversees the Security Operations Center's strategy and transformation and the development of cyber capabilities. He previously held leadership positions as Global Head of Cybersecurity Protection and Detection at Siemens (Germany) and Interim CISO and Cyber Security Director at PwC Switzerland, leading hunt, incident response, and threat intelligence services. Mark began his cyber career at the National Security Agency (NSA), contributing 12 years in various technical and leadership roles, including developing offensive capabilities for NSA's hacking team – Tailored Access Operations (TAO). His previous roles have taken him to hotspots in Central and South America, Europe, and Afghanistan. Before coming to Switzerland in 2016, Mark represented NSA Cyber activities at Canada's intelligence agencies in Ottawa, coordinating and supporting joint cyber operations and BOTNET takedowns. Today, he focuses on assisting organizations in achieving their transformative strategies and is a guest lecturer and speaker at various Swiss universities and supervisory boards.

Keynote 1b and Roundtable I

Keynote 1b

Moving IT Security Products from on-prem to Cloud – yes or no?

To get an answer to the above question IT Management need to understand a couple of issues to be able to make an informed decision:

- Cloud Risks: What are the general information security risks associated with cloud services, and how do these apply to moving security products to the cloud?
- A self-assessment of the organization: What kind of company are we? What is our security strategy? What is the maturity of internal security skills?
- Assess the vendor: What is the core business of the vendor? How mature are they in IT Security? How does their maturity compare to yours?

Getting answers to the above questions enables an IT organization to make appropriate decisions, thus laying the foundation for a successful adoption or transformation project.

Roundtable Session I

Issues in selected security key issues for successfully moving to the cloud: know and understand pitfalls.

The implementation and operation of onsite data center security are, concerning complexity, far easier

than multi-cloud security concepts. How should a cloud service customer deal with different contracts and the vast amount of "built-in security solutions"? How can these cloud security solutions be integrated into and complement a customer's existing IT (security) ecosystem? How should one deal with duplicated controls? Should they be seen as a chance, maintained or avoided, and reduced to a single control product within the ecosystem? And how to provide compliance for authorities? Endpoint Detection and Response (EDR) is another tricky point for a paramount broad variety of endpoint products in a multi-homed cloud environment: How to deal with these issues? And finally: How to deal with the organizational aspects? How to find a person with sufficient capabilities for these tasks? How should these teams be placed in the organization (part of the cloud team, part of security teams, or separate security teams)? How should an organization collaborate with Cloud Service Providers?

Evaluation of security products and solutions for one cloud and the multi-cloud ecosystem has its pitfalls: The deployment may bring up surprises, and in some cases, products and solutions do not master the complexity. Moreover, a stringent test concept may serve to experience unwanted surprises. We share the experience in this respect at the tables and elaborate on the most important points to consider.

In the session, we will discuss the balance of security and detection and response investments and look at which components may be outsourced. What is a good CISO strategy?



Manuel Fluri is the global Head of Network Security Engineering at Credit Suisse and is currently based in Switzerland. His team is responsible for all Network Security products, designs, and standards and their development within the bank. In addition, he is also the Head of Network Security Solution Architecture ad interims. Before this current role, he owned one of the Network Security services. In addition, he worked as the Global Network Security Service Delivery Manager, managing the entire network security project portfolio. Before joining Credit Suisse, Manuel held various IT roles at HINT and Alstom Switzerland & Singapore. His technical experience includes forensic analytics for malware incidents, Network and Network Security engineering, and operation. He holds a master's in Information Security from the Norwegian University of Science and Technology (NTNU).

4

Keynote II and Roundtable II

Keynote II

Cloud Security Guardrails and Encryption Models

Creating a secure cloud environment and establishing a landing zone from which to provide services is important in adopting cloud services. Security guardrails and encryption models are building blocks supporting landing zone establishment and provision of secure services.

This talk will consider cloud security concepts and options. Examples of how different security requirements can be met in Google Cloud will be reviewed. Several security elements and services are available to ensure increased control over how and under what circumstances the cloud service provider may work in the customer area.

Encryption at rest, in transit, and while processing provides further customer assurance and options for data confidentiality and integrity. Various encryption key models- from default key management services to hardware-based options and even external key management- can also be used depending on the particular use case and requirement.

Roundtable Session II

How to define cloud security targets, and what are the most important security measures?

We will elaborate on single- and multi-cloud security requirements and risk analysis, focusing on the most important points that must be considered.

The security measures which enable one to reach the defined security targets are manifold and may be contractual, legal act, encryption, and identity-based limitations.

A closer look at encryption applying the NIST model results in different encryption options for data at rest, in transit, and during processing: which tools are best in which situation. And key management is paramount for overall security, both in normal operation and to switch keys or encryption algorithms whenever needed. Appropriate preparation of both ends, customers and cloud provider, must be performed in relaxed times.

The central takeaway will be knowledge about the borderlines of cloud security and sharing state-of-the-art experience and knowledge.



Andrew Hutchison works at Google in Zurich as a technical program manager in information security engineering. He was previously a cloud security specialist in Google Cloud, advising customers on secure cloud adoption. Andrew was previously with T-Systems in various roles, including international program executive for cyber security and General Manager / Vice President of the Telecommunications Business in South Africa. Before joining T-Systems, Andrew co-founded an IT consulting and training company, which was acquired by a South African IT group, and he has also been on the faculty of the Computer Science Department at the University of Cape Town (UCT), where he remains an Adjunct Professor. Andrew received a Ph.D. in Computer Science (Information Security) from Zurich University while working at the IBM Zürich Research Laboratory in Rüschlikon. He is a Google Cloud-certified professional cloud security engineer.

Information

5

What is the Swiss CISO Summit?

The Swiss CISO Summit facilitates the exchange of current security challenges and opportunities between security executives, managers, and thought leaders in Switzerland. Each summit addresses a current hot topic. The strategic dialog and the subsequent discussions are inspired by a keynote speech from well-recognised national and international speakers. The moderated and guided discussions in groups of 8-10 members share views, experiences and strategies. An excerpt of the discussions will be written down in the result paper for the participants.

Participation is by invitation only.

How Swiss CISO Summit maintains confidentiality?

The Swiss CISO Summit is provided as a closed-door event (please contact Bernhard Hämmerli for participation). This exclusive CISO Executive programme is created for information security and risk executives providing them with an environment for achieving new ways of thinking and ensuring success in protecting their organisations.

The summits are held strictly under the Chatham House Rules which is the ruleset to treat the shared information with full discretion, and for providing secrecy against non-group persons.

Why should I join the Swiss CISO Summit?

The Swiss CISO Summit has a unique concept of creating trusted circles amongst executives, managers and thought leaders. Meeting peers in an advanced business location, having time to network amongst

each other and to touch current issues which are unique opportunities for sharing experiences, and for receiving advice far beyond the discussion at the table.

- Extensive networking opportunities with peers and experts on an ongoing basis
- Meet with other leading executives to share successes, failures, obstacles, and challenges
- Learn about current strategies on managing security threats and to prepare for the future
- Make new connections and equip yourself with information on recent projects and achievements

What makes the difference?

The Swiss CISO Summit has many and diverse benefits for the invited experts. The participants are the focal point of the summit and the meeting is not intended for providers to present solutions or products. Sales are strictly prohibited to the good of an open and free CISO information exchange.

What is the history behind the Swiss CISO Summit?

The Swiss CISO Summit has been run successfully since 2001 under the name «Risk and Security Exchange» and from 2004 - 2009 when it was known as „Swiss Security Exchange“. Then with the financial turmoil the summit came to a halt. From 2009 onwards, the same successful format was adopted in Norway where it ran under the name „Sikkerhetstoppmøte“. All this experience gained by Prof. Dr. Hämmerli is put into the organisation of the Swiss CISO Summit.

5

Information



Who prepares and facilitates the Swiss CISO summit?

An organising committee under the lead of Prof. Dr. Bernhard M. Hämmerli is responsible for the invitation, preparation and guidance of the discussions. He is an internationally well recognised expert with 25 years of experience in information security in governments, industry and academia. He led the Cyber Security activities of the Swiss Academy of Engineering Sciences SATW from 2012 – 2017.

Prof. Dr. Hämmerli is a founding member of the Information Security Society Switzerland and he built up the first Information Security master programme in Lucerne in 1996, respectively 1999, and since 2017 he is head of the new BSc Information & Cyber Security at Hochschule Luzern/Informatik. Additionally, he teaches at the Norwegian University of Science and Technology Norway www.ntnu.no, in the technology and management track of the Information Security master programme.

Prof. Dr. Hämmerli is supported by Katarzyna Kuhn for administrative purposes.

Agenda (generalised)

- 12:00 Start with a small lunch
- 12:45 Networking Session
- 13:15 Welcome and introduction
- 13.30 Keynote from experts or members
- 14:00 Roundtable session I
- 15:00 Exchange between the groups and wrap-up of roundtable I
- 15:10 Break
- 15:40 Keynote from experts or members
- 16:10 Roundtable session II
- 17:05 Exchange between the groups and wrap-up of the roundtable II
- 17:15 Summary note
- 17:30 Cocktail and aperitif
- 19:00 End

The meeting is held three times per year.

Registration

6

Join Swiss CISO Summit

Participation is by invitation only. We accept proposals for new participants. The number of participants is limited to 40 per summit in order to maintain an atmosphere of trustful information sharing.

Single summit CHF 450.- per participant

Three summits CHF 1'000.- per participant (25 % discount for booking three consecutive summits – not three participants at the 25th summit)

Cancellation Policy

Cancellations of registrations are free of charge only if received no later than seven days before the summit. Cancellations received beyond this point will incur 100 % of the admission fee. In any case a delegate may be sent at no additional cost. More information is found at www.ciso-summit.ch. Content responsibility for the summits lies with Prof. Dr. Bernhard M. Hämmerli.

Register by just replying to the invitation email with all your details or by following these steps:

Step 1: Fill out & save the form

Step 2: Select Send button > email opens (info@ciso-summit.ch)

Step 3: Attach the PDF file

Registration

Register by just replying to the invitation email with all your details – or by filling out this form and mailing it to info@ciso-summit.ch.

Three consecutive summits for CHF 1'000.–

3 Summits, Summit 28 (09.05. 2023), 29 (24.10.2023), 30 (30.01.2024)

28th Swiss CISO Summit:

09.05.2023: CHF 450.– for all forms of participation

First Name _____ Surname _____

Organisation _____

Street / No. _____ ZIP / City _____

Phone _____ Email _____

Signature _____ Date _____

7

Sponsorships & Partner

Platinum Sponsor

Detecon



Detecon Consulting is one of the world's leading management consulting companies for integrated management and technology consultancy. Detecon (Schweiz) AG is located in Zurich and bundles Financial Management as well as ICT Management competences among its roughly 150 employees. The main focus lies on the requirements of CFOs and CIOs in nearly all industry sectors. Globally, more than 6000 projects have been implemented successfully. The international spirit and the openness are reflected not only in the number and origin of our clients from over 160 countries but also in our employees that are recruited from 30 different nations.

Gold Sponsor

PricewaterhouseCoopers



At PwC, our purpose is to build trust in society and solve important problems. PwC looks at cyber security as one of the biggest challenges to solve in today's times and provides a full stack of cyber security consulting services. PwC's Cyber security practice comprises deep information security, forensic technology, business and technology resilience, Cybercrime response, technology risk and controls, project and program management and operations specialists to help clients address Cyber risks through the whole lifecycle from strategy to execution and operations.

Silver Sponsor

SWITCH FOUNDATION



The foundation "SWITCH" was founded in 1987 under private law by the Swiss Confederation and the university cantons and is an integral part of the Swiss-academic community. Based on our core competencies network, security and identity management, SWITCH offers collaboratively developed ICT solutions that empower users in and beyond the academic world to achieve leading edge results in a globally competitive environment. SWITCH's Computer Emergency Response Team (SWITCH-CERT) is one of the most experienced CERT and besides the government CERT MELANI, one of two National CERTs in Switzerland.

Silver Sponsor

Armed Forces Command Support Organisation (AFCSO)
Führungsunterstützungsbasis (FUB)

With its services in ICT and electronic operations, the Armed Forces Command Support Organisation (AFCSO) ensures that the armed forces can accomplish their missions. It guarantees the command and control of the armed forces under all conditions.

Silver Sponsor

SWISS POST



Swiss Post is part of the critical infrastructure of Switzerland. On top of its logistics and transport services, Swiss Post offers a variety of digitalized services in other industries ao. electronic voting, eHealth and secure eMail. The ICT department holds certificates on ISO 27001, 22031 and 20000. Information Security is an integral part of all activities of Swiss Post Group. As a first mover in the Paris Call for Security and Trust in Cyberspace, Swiss Post Group fosters expertise sharing on security in trusted environments both nationally and internationally.



Sponsorships & Partner

Silver Sponsor **HSLU**

Lucerne University of Applied Sciences and Arts



Lucerne School of Computer Science and Information Technology provides most comprehensive range of IT study programs within Switzerland. The Lucerne School of Computer Science and Information Technology offers bachelor's and master's degree programs, applied research and development, and continuing education programs in Computer Science, Information Technology and Business Information Technology. Newly developed (past 5 years) and innovative study programs are: Information & Cyber Security, Artificial Intelligence and Machine Learning, Digital Ideation, and International IT Management.

Silver Sponsor **Palo Alto**



Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

Partner **SATW**



SATW is recognized as the Swiss organization for the communication of independent, objective, and comprehensive information about trends in technology – as a basis for the forming of well-founded opinions – and as an effective institution for the promotion of engineering sciences and new technologies in Switzerland. SATW identifies technological developments of relevance to industry and informs politicians and society about the significance and consequences of such developments.

swisscisosummit

More information is found at www.ciso-summit.ch

Sponsorships:

DETECON
CONSULTING

Platinum

pwc

Gold



Lucerne University of
Applied Sciences and Arts
**HOCHSCHULE
LUZERN
SWITCH**

Silver

paloalto
NETWORKS
SWISS POST

Partner:

satw it's all about
technology