PERSONAL INVITATION to 25th

swissciso summit

Zero Trust: What does it mean, and how to implement it?

17th May 2022, Zunfthaus zur Schmiden, Zurich
(upon requests, virtual participation will be organized)

Sponsorships:

DETECON CONSULTING — Platinum

pwc — Gold

FUB | Lucerne University of Applied Sciences and Arts HOCHSCHULE LUZERN | SWITCH — Silver

paloalto NETWORKS | SWISS POST

Partner:

satw it's all about technology

Contents

1 Introduction

Dear CISO,

You are kindly invited to the 25th 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

Zero Trust: What does it mean, and how to implement it?	
Date	17th May 2022
Time	12:00 Lunch and 13:00 Summit starts / approx. 19:00 Summit ends
Location	Zunfthaus zur Schmiden Marktgasse 20, 8001 Zurich, Switzerland Please contact Prof. Dr. Hämmerli for virtual participation.
Keynote 1	**Zero Trust: Is Multi-Factor Authentication the security solution to everything?** Christian Ledergerber, Enterprise Security Executive at Microsoft Switzerland GmbH
Keynote 2	**Building the Zero Trust Enterprise: The Role of the SOC** Amitabh Singh, Field CTO EMEA at Palo Alto Networks
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

In light of ever-increasing and more rewarding criminal activities, "Zero Trust" promises a solution. But what does it mean, and how to implement it?

Zero Trust is perceived as a practical approach in today's cloud-first world. But what does it take to move from a Zero Trust strategy to active implementation? Gartner recommends as best practices for building a Zero Trust foundation the following measures:

- Create a secure, standard federated identity management system
- Apply adaptive access for more granular resource and access control
- Roll out user-to-application segmentation (Zero Trust Network Access (ZTNA))

Today, a cloud-first strategy can be considered default and promotes building software directly in the cloud rather than building on-premises and migrating to the cloud. The goal is to create software faster and reduce the overhead associated with on-premises resources and cloud migration.

Platform advantages of a Cloud-First approach are flexibility, less overhead, more resources available without investments i.e. cost-effective upgrades, Improved recovery abilities, support options from the cloud provider, faster release cycles, and an integrated option for collaboration. And the business advantages embrace innovation, new business models, new composition and design of applications.

A central role in the cloud and Zero Trust plays secure identities: with two and more factors, we can nail down the acting identity and make them responsible for their actions.

The Zero-Trust-Modell (NIST 800-207) applies the following principles:

- Permanent control: access must be controlled at any time for any resources.
- Limitation of impact: by segregation, the impact of a compromise is limited. Later movement is not possible.
- Automated context detection and reaction: behavioral data are analyzed, and the contexts of all information technologies (Identity, End-device, Workload, etc.) are gathered and processed such that targeted responses are enabled.

These nice "promises" are compelling. First, however, we need to reflect on how to implement Zero Trust, which steps must be taken, and whether the security gain justifies investments and work effort. The more fine-grained we implement access control, the more work must be invested in the design and implementation of access control: What is the CISO's experience? Where to cut the refinement of access control to limited efforts? And by when is the second line of defense (SOC) the better option?

We want to have an open exchange for creating a sharp picture of prerequisites for the success of implementing Zero Trust and having resilience success in defending our system against new forms of attack.

3 Keynote I and Roundtable I

Keynote I

Zero Trust: Is Multi-Factor Authentication the security solution for everything?

Multi-Factor Authentication (MFA) can be seen as one of the most effective security measures to protect corporate assets, and one of the fundamental security controls organizations consider on the Zero Trust journey. However, is Multi-Factor Authentication the security solution for everything?
This keynote will elaborate and deep dive on how MFA can help you secure your environment and protect your assets. It will start with a discussion on how MFA can play a major role on the Zero Trust journey. However, is MFA the unassailable solution overall?

The following topics will be covered:

- The evolvement of MFA and challenges within organizations.
- MFA vs. Passwords – on which you should focus.
- The difference between MFA and intelligent MFA is part of an enhanced Conditional Access configuration.
- What you should consider while enforcing CA.

More and more organizations are moving towards Zero Trust, and therefore it's time to reflect and consider some lessons learned to avoid pitfalls.

Roundtable Session I

Multi-factor authentication (MFA): how to implement MFA for better security without aggravating users?

Many employees get more and more the feeling of fulfilling duties against application portals, with many authentications in a large variety of corporate applications. And finally, employee satisfaction suffers, even when we enjoy greater corporate security.

In the discussion, we elaborate

- how to reduce the number of electronic identities as much as possible with reasonable effort,
- how to design the number of actors when doing authentication to be secure enough but still not overstretching the patience of employees, and
- how to implement access management such that the standard workflow is still flowing with ease.

The intention is that participants will get a picture of what other CISOs are preparing for and get insights on Switzerland's diversity of handling MFA's and access management in the frame of Zero Trust.

Christian Ledergerber has been Enterprise Security Executive at Microsoft Switzerland for one year. In his role, he is responsible for managing customer relationships with CxO, technical decision-makers, and CISOs regarding security, compliance, and identity. He is focused on insurance and health insurance customers with HQ in Switzerland. One of his main priorities is helping customers build the bridge between their asks and technology. Be it in Microsoft 365 or a public, hybrid, or multi-cloud setup.

Christian gathered different experiences during his time as a cybersecurity consultant within the financial service sector, working for a big-four company.

Keynote II and Roundtable II

4

Keynote II

Building the Zero Trust Enterprise: The Role of the SOC

One of the essential truths of Zero Trust is to "never trust, always verify." However, how do we know the policies and subsequent trust decisions we are making are the right ones? How do we continuously monitor and validate those decisions? Most threat prevention tools must decide, in real-time, whether to permit or block user access, endpoint files, and an innumerable set of other events and actions. The Security Operations Center (SOC) operates at a different level – using analytics, AI, automation, and human analysis – and this allows the SOC to reevaluate past trusted decisions. When building a Zero Trust enterprise, the main role of the SOC is to provide an additional layer of verification to reduce risk further.

At the same time, many organizations are working to modernize their approach to the SOC due to an overwhelming number of alerts, crippling manual processes, and a lack of skilled personnel. While the SOC is an essential element of Zero Trust, organizations should consider incorporating innovations like automation, analytics, and machine learning to increase SOC efficiency.

Roundtable Session II

Zero Trust second line of defense: How to align security operation center SOC to handle additional tasks efficiently?

Snowden gave us references to what most security experts knew before: we can apply as much security technology and principles as we want, but the systems will never reach the level of 100% security. That's why we need to detect and respond.
Automation is key when sorting out indicators of compromise, making conclusions, and preparing immediate reactions.

Discussion points are:

- What is the right balance between MFA, access management (AM), and detection & reaction capacity?
- Which are the important use cases for MFA and AM a SOC must be prepared for in respect to detection and response?
- How to train the analytics and AI to do the best job? Which parameters can be tuned in the SOC organization?
- Which inter-organization exchange networks do we need for the best success?
- And how do we manage the continuous improvement while optimizing SOC services?

Amitabh Singh is Field CTO EMEA for Palo Alto Networks. He was CISO and CDO for Swisscard and has worked with companies like IBM, HSBC, and GE. He has been managing and consulting on Security and Data Privacy for fortune 100 companies in Europe at C level. He is a guest lecturer at University of St. Gallen and Hochschule Luzern. He is also the regional Ambassador of Switzerland for Global Business Blockchain Council (a WEF and Richard Branson promoted think tank).
He is a speaker of repute and has been keynote speaker at various conferences. He is a trusted advisor to boards and companies.

Amitabh is an Engineer from Indian Institute of Technology and an MBA from Faculty of Management Studies, New Delhi.

5 Information

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.

Information 5

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.

6 Registration

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

PRINT RESET SEND

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 25 (17.05.2022), 26 (25.10.2022), 27 (31.01. 2023)

☐ **25th Swiss CISO Summit:**
17.05.2022: CHF 450.– for all forms of participation

First Name _____ **Surname** _____

Organisation _____

Street / No. _____ **ZIP / City** _____

Phone _____ **Email** _____

Signature _____ ***Date*** _____

Sponsorships & Partner

7

Platinum Sponsor	**Detecon**
DETECON CONSULTING	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**
pwc	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**
SWITCH	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)**
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	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.

7 Sponsorships & Partner

Silver Sponsor	**HSLU**
Lucerne University of Applied Sciences and Arts HOCHSCHULE LUZERN	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**
paloalto NETWORKS	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 it's all about technology	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.

swissciso summit

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

Sponsorships:

DETECON CONSULTING

Platinum

pwc

Gold

FUB

Lucerne University of Applied Sciences and Arts
HOCHSCHULE LUZERN
SWITCH

Silver

paloalto NETWORKS

SWISS POST

Partner:

satw it's all about technology