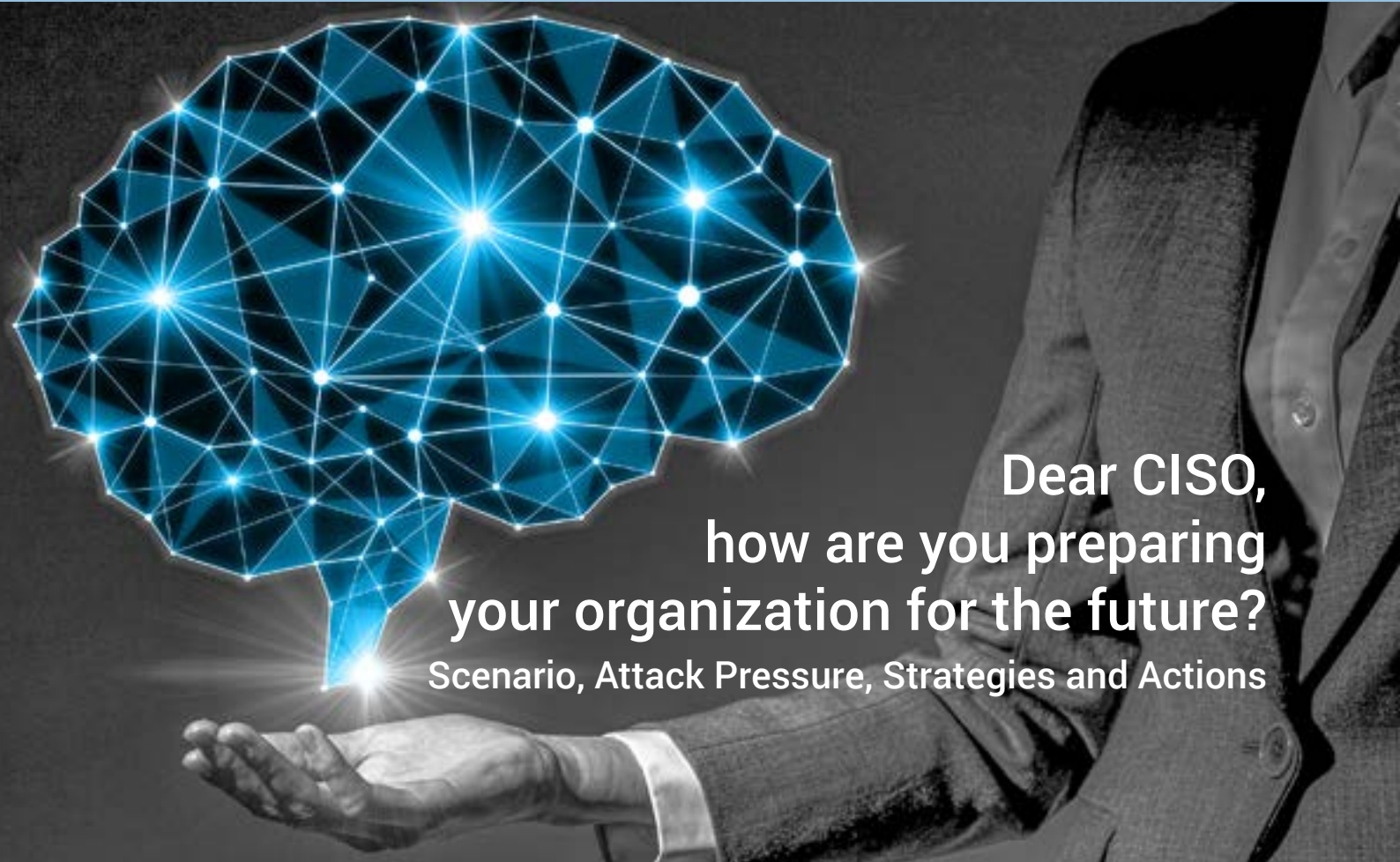


Personal Invitation to 24th
swisscisco summit



Dear CISO,
how are you preparing
your organization for the future?
Scenario, Attack Pressure, Strategies and Actions

25th January & 1 February 2022
online

Sponsorships:

DETECON
CONSULTING



Lucerne University of
Applied Sciences and Arts
**HOCHSCHULE
LUZERN**
Information Technology
FIT Zentralschweiz



Partner:

satw it's all about
technology

Platinum

Gold

Silver

Contents

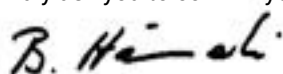
1	Introduction	Page 3
2	Summary	Page 4
3	Keynote I and Roundtable I	Page 5
4	Keynote II and Roundtable II	Page 6
5	Information	Page 7 – 8
6	Registration	Page 9
7	Sponsorships & Partner	Page 10 – 11

Introduction

Dear CISO,

You are kindly invited to the 24th 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



Dear CISO, how are you preparing your organization for the future?

online only (corona regulation)

Summit 25th January / 1st February online

Time 13:00 join the online session,
summit starts 13:15 and ends 15:30 on both dates

Keynote 1 **Are we fit for the future? A personal view on future challenges to master as CISO**
Alain Beuchat, CISO Banque Lombard Odier

Keynote 2 **Cyber-risks as a threat to critical infrastructures:
Standards, strategies, and alignment to upcoming security needs**
Daniel Caduff, Secretariat for the ICT-Division at the Federal Office
for National Economic Supply

- 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!

2

Summary

Against the background of ever-increasing and more rewarding criminal activities: Dear CISO, how are you preparing your organization for the future? Scenario, Attack Pressure, Strategies, and Actions

In 2020 Germany suffered losses of 220 billion Euro related to cyber security incidents, according to the association Bitcom. Scaling this down to Switzerland will result in more than 22 billion CHF, more than four times the Swiss military budget. Hackers are rewarded with good money, and they re-invest the money in better technology for attacking. This dream budget of hackers is not available in the counterpart, the CISO offices, which must defend their IT infrastructures. How to communicate the new conditions towards executive offices and get them aware that early investment into the security office might be better than sponsoring hackers later?

The pressure towards hackers to get caught is relatively small, especially if they operate from countries with no contracts with Switzerland regarding law enforcement and countries not cooperating with other law enforcement agencies. The hacking business has better profitability rates than drug and other criminal businesses. Hackers realized that the ransom works better when attacking critical infrastructure. Of course, they need more and new knowledge when attacking SCADA and ICS, but investments will pay back soon, as e. g. the colonial pipeline case demonstrated.

The Corona home office period displaces secure corporate working spaces to warm and beautiful homes. However, the security measures are not on the same level, and through diverse family interaction in the same net will the attack surface grow. In other words, hackers have easier access.

Innovation of technology is not to stop: Internet of things, cloud shift, choices of networks (4G, 5G, fiber, DSL), cellphones which have enormous computing and storage capacity, and the new generation of software open up for further attacks.

Against this background, we will discuss how security should be shaped in the following strategic period:

- What are the intentions of the top executives in respect to security? To which function should CISO report? And how should CISO deal with the new pressure of the management, which wants more reporting, more reliable security, and more control over the security function?
- Which strategies must be followed to succeed with security in the next period?
- How to reorganize security and security offices for counter-fighting attacks in the new area?
- Which actions are most urgent to be taken?
- How to speed up the implementation of security measures for new technologies the company has procured?

Against this background, we want to have an open exchange stimulating each other to have a better picture of preparedness and a greater awareness of the many options to deal with the new and more challenging situation.

Keynote I and Roundtable I

Jan 25, 2022:

Keynote I

Are we fit for the future? A personal view on future challenges to master as CISO:

The developments in cyber security are accelerating. Not all happenings are necessarily new, but theoretical matters in the past are now a reality. The presentation will illustrate some of the cyber security challenges that are awaiting CISO and provide a basis for discussing approaches to address them:

- The time between the publication of new vulnerabilities and their exploitation has dramatically diminished
- The financial incentive for hackers is becoming such that any organization may become a target in the future
- Technology empowers organizations to fight cybercrime more effectively but makes them more dependent on third parties, i. e. third parties are now part of our perimeter.
- The need for cyber security specialists is increasing, and the market is already dry
- CISOs are becoming more and more part of the executive management and have better opportunities to shape the organization and make it more cyber resilient

Roundtable Session I

How to reach cyber resilience with the new opportunities in the new context?

Companies are more and more under pressure to defend against hackers with an enormous budget. Switzerland's loss due to cyber incidents is estimated to 22 billion CHF, more than five times the defense budget. Executives want to know how well the company is protected and welcome CISO in the executive team.

In the discussion, we elaborate

- on threats of hackers, with a huge budget,
- on organizational security structures ready for the future,
- prioritization of measures and applied security technologies in the new context,
- on the dependence of third parties (SW, HW, Services) as well as
- on how to enlarge and educate the security personnel.

The intention is that participants will get a picture of what other CISOs are preparing for and a holistic view of Switzerland's diversity of preparedness in the upcoming area.



Alain Beuchat is the chief information security officer at Lombard Odier. He is responsible for defining the information security strategy and implementing the security program to protect the bank and its clients against cyber threats.

Alain has gathered extensive experience in the field of information security as the CISO of a multinational financial institute and as the head of a Swiss IT advisory practice at one of a major international consulting firm. Alain chairs the Cyber Security expert group at the Swiss Banking Association and contribute to various cyber security initiatives e. g. in the context of the SATW.



Keynote II and Roundtable II Feb 1, 2022:

Keynote II

Cyber-risks as a threat to critical infrastructures: Standards, Strategies, and alignment to upcoming security needs

Digitization is increasingly permeating all areas of life. Information technology and telecommunications (ICT) have thus become an indispensable resource for the well-functioning of critical infrastructures. For example, without ICT, the supply of food, energy, and medicines can no longer be guaranteed. Neither can the functionality of hospitals or emergency services.

Newer, harder, and targeted attacks create a new risk landscape for Switzerland. New risks are analyzed as part of the National Strategy for the Protection of Switzerland against Cyber Risks NCS, and measures to improve resilience in the following area are developed.

The presentation will include the current strategy, show which upcoming risks are of particular importance, and which measures should be prepared to address these new risks.

Roundtable Session II

What can CISO's learn from ICS security: standards, strategies, and measures?

The fact is that Corona speeded up digitization all over Switzerland.

Some trends became a reality as e. g:

- evermore spreading out of Internet of things
- Cloud shift of data, services, and hardware even when not directly wanted or induced
- shift to third party security services

The question we address in addition:

- Can we change towards being able to act and be secure?
- SCADA and ICS are fully networked with the internet, even when fine-grained segmentation is applied. So how do these two technologies harmonize, one with 20 years minimum lifetime and internet with a few seconds to hours for the next change?
- What is the right budget for security against new risks, new and stronger wave of hacking, and the new pace of technology, which must be faster than corporate budget processes?



Daniel Caduff is the Deputy Head of Secretariat for the ICT-Division at the Federal Office for National Economic Supply FONES. He is a member of the steering committee for the Swiss National Cybersecurity Strategy NCS and the „industrial Resources and Communications Services Group IRCSG“ within NATO's „Partnership for Peace“.

Together with his team, Daniel develops ICT-Minimum-Standards to address the specific Cybersecurity-needs of critical infrastructure providers to strengthen the resilience of Switzerland's supply chain of critical goods and services.

Daniel is a Digital Native with a strong „can-do“ attitude and a regular contributor to national and international Cybersecurity-Events, like the NIST-Conference in Baltimore and the OSCE-Cybersecurity-Conference in Bratislava or the annual MERIDIAN-Conference, among others.



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



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

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 24th 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 24 (25.1. / 1.2. 22), 25 (17.05.2022), 26 (25.10.2022),

24th Swiss CISO Summit: 25.1. & 1.2. 2022: CHF 400.- (online)

First Name _____ Surname _____

Organisation _____

Street / No. _____ ZIP / City _____

Phone _____ Email _____

Signature _____ Date _____

Sponsorships

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



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

**HOCHSCHULE
LUZERN**

Information Technology
FH Zentralschweiz

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



Gold



Lucerne University of Applied Sciences and Arts
**HOCHSCHULE
LUZERN**
Information Technology
FIT Zentralschweiz

SWITCH



Silver

Partner:

satw it's all about technology