

PERSONAL INVITATION to 26<sup>th</sup>



## Vulnerability Management: How to recognize vulnerabilities and threats and defend successfully against?

25th October 2022, Kursaal Berne (as part of the Swiss Cyber Storm conference)  
(upon requests, virtual participation will be organized)

*Free Tickets for Swiss Cyber Storm for all CISO Participants*

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 I and  
Roundtable I

*Page 5*

4

Keynote II and  
Roundtable II

*Page 6*

5

Information

*Page 7*

6

Registration

*Page 9*

7

Sponsorships &  
Partner

*Page 10*

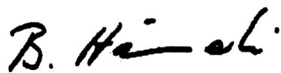
# 1

## Introduction

Dear CISO,

You are kindly invited to the 26<sup>th</sup> 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



### Vulnerability Management: How to recognize vulnerabilities & threats and defend successfully against them?

**Date** 25<sup>th</sup> October 2022

**Time** 12:15 Lunch and 13:15 Summit starts / approx. 19:00 Summit ends  
8:45–12:15 and 16:15– 17:30, you are invited to attend the Swiss Cyber Storm presentations.

**Location** Kursaal Bern, Kornhausstrasse 3, 3013 Bern, Switzerland  
Please contact Prof. Dr. Hämmerli for virtual participation.

**Keynote** **Next Generation Vulnerability Management: Which maturity level do you need to be successful?**  
Holger Scriba, Head Platform Security Services at SIX Group

- 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

## **Vulnerability Management: How to recognize vulnerabilities & threats and defend successfully against them?**

At first glance, vulnerability management does not look very attractive. However, for many enterprises, engaging with the processes around vulnerability and asset management is very beneficial. It lowers the attack surface relevantly.

Before starting with vulnerability management, the processes of the organizations must be mature and well defined: This means that patch management, lifecycle management, and adjunct processes are established on a high maturity level. In addition, it includes the perception turnaround from patch management for fewer errors to patch management as a strategic security activity.

It is a well-recognized fact that asset management will never be 100% perfect, but approaching a state of "near perfect" is highly desirable. It includes hardware, software (applications), middleware, firmware, and services like encryption (note: remember SSL heart bleed). In addition, the link between assets and responsibilities is of critical importance, where a group or a person may be responsible for an asset entity or an asset entity group.

Two levels of automation we face today: the automation of software production with DevOps and DevOpsSec, which is not relevant for this context. But the automation and orchestration of vulnerability scanners are highly relevant. Main processes must be

efficient and automated; meanwhile, zero-day-exploits must be followed and evaluated still hand-picked. Those two approaches must be connected and tuned to each other.

Another issue is the gravity of CVSS rating depending on the respective security zone they show up: The rating may differ from the systematic rating because of enhanced or diminished business impact. The number of false positives, i.e. of false alarm is paramount. Unless this number is sufficiently low, these systems bring no value for the company.

Finally, the everyday day routine, including the human factor within groups and between groups, plays a major role in the success of the next generation of vulnerability management.

# 3

## Keynote and Roundtable

### Next Generation Vulnerability Management: Which maturity level do you need, to be successful?

Massive exploitation of vulnerabilities has reminded many companies of the huge risk IT vulnerabilities pose and has prompted them to take firm, proactive action to manage them.

Holger Scriba will share insights on how the NextGen Vulnerability Management set-up is designed within SIX Group, how to leverage an orchestration tool to connect and aggregate various vulnerability scanner sources, and what challenges have been encountered.



**Holger Scriba** has now been working at the SIX Group since 2016. In his role as Head of Platform Security Services, he is primarily responsible for the vulnerability, hardening practice, and Splunk, which is used as operational monitoring.

He originally studied economics at the University of Zurich but remained loyal to IT in a variety of roles, with a detour into controlling. Due to his activities as strategic management support and project manager, it is easy for him to respond to different stakeholders, be it application managers or C-level executives.

# Roundtable

# 4

## Roundtable Session I

Which maturity level of surrounding processes as e. g. patch-& lifecycle-management, is needed for successful vulnerability management?

The maturity level of processes is critical to the mission of vulnerability management. It means, that the surrounding processes must be analyzed and optimized:

How works patch management today, which needs are covered, how far automated the process is, and what is the potential of optimization?

Which lifecycles are controlled today: Hardware, Application, Middleware, Firmware, and services. Are termination dates available, and what are the precautions for early replacement in case of relevant deficiencies?

What is the level of orchestration by today: Are these processes integrated into a landscape with assigned responsibilities?

The intention is that participants will get a picture what other CISOs are preparing for and get insights on Switzerland's diversity of patch management and lifecycle management.

## Roundtable Session II

Stringent asset-management: How to assign responsibilities for each component (HW, SW, Middleware, and OS)?

As the last SSL vulnerability demonstrated, most organizations do not know in which software modules as SSL are used and in which version. If the organization knew, the upgrade of the SSL would not be that difficult. But if the organization must first find out in which module the SSL is active and how is responsible for the software, the time span to fix grows enormously.

Discussion points are:

- To which granularity should asset management be performed?
- How to update the asset database?
- How to define the responsible experts for the asset components? And how to resolve conflicts when several experts need to work together?
- How to optimize the human aspect in collaboration in this field?
- Are there any shortcuts, which could be exchanged?

## 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](http://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, not for Swiss Cyber Storm)

- 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 25<sup>th</sup> 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](http://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](mailto: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](mailto:info@ciso-summit.ch).

Three consecutive summits for CHF 1'000.–

3 Summits, Summit #26 (25.10.2022), 27 (31.01.2023), 28 (09.05.2023)

26th Swiss CISO Summit, including free entrance to Swiss Cyber Storm:

25.10.2022: CHF 450.– for all forms of participation

First Name \_\_\_\_\_ Surname \_\_\_\_\_

Organisation \_\_\_\_\_

Street / No. \_\_\_\_\_ ZIP / City \_\_\_\_\_

Phone \_\_\_\_\_ Email \_\_\_\_\_

Signature \_\_\_\_\_ Date \_\_\_\_\_

# 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.

## 7

## Sponsorships &amp; 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



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](http://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](http://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