

PERSONAL INVITATION to 29<sup>th</sup>

swiss**ciso**summit



## Red Teaming Exercises – What are your experiences, and how we can convert good SOC teams into excellent teams?

24th October 2023, in Person, Kursaal Bern  
(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*

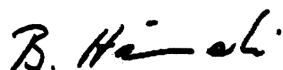
## 1

# Introduction

Dear CISO,

You are kindly invited to the 29<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



## Red Teaming Exercises – What are your experiences, and how we can convert good SOC teams into excellent teams?

**Date** 24th October 2023, co-located with Swiss Cyberstorm

**Time** 9:00–19:00 hrs with Cyberstorm visit, CISO Summit only: 12:15 hrs to 19:00 hrs

**Location** Kursaal Bern  
Please contact Prof. Dr. Hämmerli for virtual participation.

**Keynote 1a** **Between SOC Services and internal operation: How to reach maximum IT resilience and most effective defence?**

Christophe Monigadon, Cybersecurity Expert, National Cyber Security Centre (NCSC) Switzerland

**Keynote 1b** **How a vendor runs its SecOps - tales from the CISO.**

Marco Eggerling, CISO EMEA, Check Point

**Keynote 2** **10 years of running adversary simulations: Key learnings from a red teamer's perspective.**

Patrick Schmid, Head of Security Testing & Architecture, Redguard

### 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

## **Red Teaming Exercises – What are your experiences, and how we can convert good SOC teams into excellent teams?**

In an era where cyber threats loom large over organizations, the role of Security Operation Centers (SOCs) has never been more vital. The urgency is clear – it's not a matter of if you'll be targeted, but when. Statistics tell us that the average cyberattack inflicts a staggering CHF 4 million in damage in Switzerland alone. Imagine what this sum could achieve if you proactively secured your digital infrastructure.

Establishing their own SOC is a daunting challenge for many small and medium-sized enterprises (SMEs). This is where fully managed SOC service providers offer comprehensive monitoring and incident response capabilities. Outsourcing SOC functions allows SMEs to access professional-grade security services without breaking the bank. However, rigorous training and exercises are imperative in this evolving landscape to ensure seamless cooperation between companies.

On the other hand, larger corporations often choose to build their in-house SOCs, establish collaborative networks with peers, and acquire real-time threat intelligence feeds. While these strategies offer unparalleled control, they demand a more sophisticated approach to training and development.

Learning from the collective experiences of SOC experts is paramount in optimizing SOC services. The pace of SOC advancements necessitates swift adaptation. Our upcoming round table presents an exceptional opportunity to share insights, explore red and purple teaming exercises, and uncover the benefits of these simulations.

We also aim to delve into change and transformation processes, discussing strategies to elevate SOC maturity and identifying the prerequisites for transforming proficient SOC teams into exemplary units.

# 3

## Keynote Ia

### Keynote Ia

#### Between SOC Services and internal operation: How to reach maximum IT resilience and most effective defense?

Achieving maximum resilience and optimal protection requires a strategic alignment between SOC services and internal operations. The desired goals can be attained through this synchronization across key domains. By fostering collaboration and integration, organizations can ensure smooth information sharing, incident response coordination, and alignment of security objectives. This synergy enables proactive

threat intelligence, comprehensive monitoring and detection, efficient incident response, and continuous improvement. The combined efforts of SOC services and internal operations in these critical domains lay the foundation for robust defense capabilities and the highest level of resilience against evolving threats.



**Christophe Monigadon** is a cybersecurity expert currently employed at NCSC-CH (National Cyber Security Center). In his previous roles as CISO, he played a key role in specifying and procuring managed security services for his employers.

With his extensive experience and expertise, Christophe firmly believes that humans are not the weakest link in cybersecurity. He recognizes the importance of implementing robust security measures, raising awareness, and providing comprehensive training to turn individuals into resilient defenders against cyber threats.

# Keynote 1b and Roundtable I

## Keynote 1b

"How a vendor runs its SecOps – tales from the CISO "

Running SecOps for a technology vendor is often perceived as black magic. This is why we will look at how we run our SOC and do things, look at what monitor capabilities are employed and how we make use of them also in the context of AI.

Check Point's homegrown development efforts often flow into commercial products, which is why we will look at how evolution in infosec triggers our own maturity as well as that of our client's security programs. Also, we will consider MFA-fatigue as an issue and how we deal with this. Finally, we will see how data models are used in our SOC and which efforts have been put into making them useful for the SIEM use cases and look at what lies ahead.

## Roundtable Session I

Discussion on: "How to convert good SOC teams into excellent teams?"

After the two keynote speeches, we extend a formal invitation to our upcoming discussion round. This forum aims to systematically explore the journey from capable to exceptional Security Operations Center (SOC) teams. Our dialogue will cover essential aspects of achieving SOC excellence, including the latest tools that empower advanced SOC teams, streamlining processes for swift and efficient responses, and the seamless integration of security practices into your organization's IT framework.

Furthermore, we will delve into the comprehensive path toward SOC maturity, examining the necessary phases and strategic steps to elevate the quality of your SOC services. Team development will also take center stage as we discuss various education and training options to enhance your SOC staff's skills and expertise. This session promises to be a valuable exchange of insights, experiences, and best practices. Whether you lead a SOC team, oversee cybersecurity strategy, or aspire to stay at the forefront of security, this session offers significant opportunities for learning and networking.



**Marco Eggerling** is CISO EMEA for Check Point. Before being appointed, he served in a similar role at Splunk, where he spent two years of his 25-year-long career.

Marco started in cryptography and forensics and worked for leading security vendors and big4 consulting firms. He studied computer science in the US and earned an MA in International Business Management and LL.M. in IT law along the way.

# 4

## Keynote II and Roundtable II

### Keynote II

10 years of running adversary simulations: Key learnings from a red teamer's perspective

Adversary simulations like red or purple team exercises can enhance already established blue teams and their detection and response capabilities by offering fresh insights and helping them break through their detection bubble with new ideas. However, running these simulations successfully usually comes with a few potential pitfalls. From years of conducting adversary simulations at different companies, we share our key learnings from a red teamer's perspective so you may circumvent some pitfalls when you perform your own simulations.

### Roundtable Session II

Discussion 2 on "Red Teaming Exercise, Testing and Verification of SOC Services"

A famous proverb, "The proof of the pudding is eating it," describes that the ultimate test is the reality check. The discussion on how to test the SOC and its diverse components will lead us from architectural via cultural to organizational and technical issues. Specific use cases are usually dealt with and could be used on purple-teaming exercises to create learning and optimization points. Is this a cost-effective training instrument? Or is it preferred to visit a cyber range and train the employees there? What other options are available? We expect a variety of rate options for this discussion.



As Head of Security Testing & Architecture, **Patrick Schmid** is responsible for the offensive service area of Redguard AG, with a total of 25 security testers distributed across four teams. Patrick specializes in putting enterprise networks and their core systems and services to the test.

He combines 15 years of experience in IT and information security, holds a bachelor's degree in computer science from FHNW and a master's degree in information security from NTNU as well as several professional certifications in the area of offensive security. In addition, he lectures in the field of penetration testing at HSLU as well as a regular guest lecturer at ETH. He is involved as an exam expert for interdisciplinary practical work (IPA) for prospective computer scientists EFZ.

# 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](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)

- 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 29<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 29 (24.10.2023), 30 (30.01.2024), 31 (14.05.2024)

### 29<sup>th</sup> Swiss CISO Summit, including free entrance to Cyber Storm:

24.10.2023: CHF 450.– for all forms of participation

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

Organisation \_\_\_\_\_

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

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

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

## 7

## Sponsorships &amp; 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

**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.

# swisscisorummit

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



Partner:

**satw** it's all about  
technology