PERSONAL INVITATION to 33rd

swissciso summit

Operational Resilience: The role of the cyber regulatory landscape of today and in the future: How to act now?

28th January 2025, Zunfthaus zur Schmiden, Zurich
(upon requests, virtual participation will be organized)

Sponsorships:

DETECON

Platinum

pwc

Gold

Lucerne University of Applied Sciences and Arts
HOCHSCHULE
LUZERN

SWITCH

SWISS POST

Silver

Partner:

satw it's all about technology

Contents

1 Introduction

Dear CISO,

You are kindly invited to the 33rd 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

Operational Resilience: The role of the cyber regulatory landscape of today and in the future: How to act now?

Date	28th January 2025, zur Schmiden, Zurich
Time	12:00 to 19:00h
Location	Zunfthaus zur Schmiden, Marktgasse 20, 8001 Zurich
Keynote 1	**Operational Resilience: Making Julius Baer Cyber resilient and robust** Lucas Welton, Head Security Transformation & Reporting, Bank Julius Baer
Keynote 2	**NIS2, CRA, AI Act, Data Act, RED, ERJU, Product Liability Directive:** **What we can learn from cybersecurity regulatory compliance in the EU rail industry.** Gabriela Bogk, Group CISO Stadler Rail
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

Operational Resilience: The role of the cyber regulatory landscape of today and in the future: How to act now?

Operational Resilience means running an IT environment that is secured according to the best standards and planning to return as fast as possible to normal operation after events and incidents. This is important for all IT systems but is a condition “sine qua non” for critical infrastructure. Policymakers and creators of frameworks have understood the urgency of operational resilience and started regulation: DORA for the finance sector, NIS 2 for critical infrastructure, European Cyber Resilience Act (CRA) for software and hardware products, Critical Entities Resilience Directive (CER) for ensuring essential services for the maintenance of vital societal functions, AI Act, Data Act, Product Liability Directive. The security community must now apply the regulations and define what they mean to their corporate environment. Typically, elements like Vulnerability Management, Incident Reporting, and Supply Chain Issues (SOBM and VEX) require strict compliance procedures, including audit (internal and external) security testing (Pentest, red teaming) and certification.

The most relevant regulatory challenges are:

- DORA, Incident reporting in the finance sector: Financial Supervisory Authorities, Sectorial Specialized Authorities, and Cybersecurity Authorities.
- European Cyber Resilience Act (CRA) Challenges: Which are the best tools to support conformity procedure, and which composition applies to regulation, standards, and certification? The goal is to simplify the interplay between these elements. Serves composition as a key concept to support a Supply Chain of Trust?
- NIS2 Challenges: Differences and Complexity: NIS2 has been adopted by around 5 Member States (MS), and most other MS have developed public draft. Many MS have included more sectors than required from NIS2.
- Many nations center themselves around security frameworks like e.g., ISO 27001/27002, NIST SP 800-53, IEC 62443, and NIST Cybersecurity Framework for implementing NIS2. Compliance with NSI2 is typically examined with questionnaires. Experts recommend making the questionnaires like those of CSA and Minimum Viable Product.

We are proud to have two speakers, *Lucas Welton from Julius Baer*, who implemented operational resilience, and *Gabriela Bogk from Stadler Rail*, who is in the process of adopting Stadler Rail to compliance with several EU regulations, including NIS2 and CRA, and CER. We will profit from their experience and learn about processes and their steps when approaching compliance.

As usual, we will run two rounds of discussions:

- Discussion Round 1: **Operational Resilience: Which threat model should we base on, and which technologies lead to the best results?**
- Discussion Round 2: **NIS2, CRA, Product Liability Directive, etc.: How to navigate in the jungle and set priorities right?**

3 KEYNOTE I AND ROUNDTABLE I

Keynote I: Operational Resilience: Making Julius Baer Cyber resilient and robust

In today's increasingly dynamic and interconnected world, the financial industry faces unprecedented challenges from sophisticated cyber threats. Operational resilience has merged as a cornerstone for ensuring business continuity and safeguarding stakeholder trust. This session explores Julius Baer's holistic approach to achieving operational and cyber resilience by embedding cybersecurity practices within its overarching risk management framework.

Key focus areas include proactive threat identification, advanced monitoring systems, and the development of adaptive incident response strategies to mitigate risks and minimize potential disruptions effectively. The presentation will also delve into Julius Baer's commitment to leveraging cutting-edge technologies, fostering collaboration with industry partners, and implementing a forward-looking security roadmap that addresses emerging threats and regulatory requirements.

Participants will gain valuable insights into how Julius Baer strengthens its defenses, maintains operational stability, and sets the foundation for a secure, robust, and sustainable future in an ever-evolving digital landscape.

Lucas Welton was born and raised in Switzerland and holds a degree from the University of Zurich in Social Sciences. After working at IBM for seven years and getting to experience cyberspace, he continued his career at PwC Switzerland as a cybersecurity consultant with various assignments aboard especially in Singapore. Lucas joined Bank Julius Baer in November of 2020 and oversees building up, automating, and improving the information security reporting across the bank, in addition to leading key security roadmap projects, including cyber resiliency. Lucas supports the business and information security team with various smaller cybersecurity assignments with a strong focus on innovation.

Roundtable I: Operational Resilience: Which threat model should we base on, and which technologies lead to the best results?

KEYNOTE II AND ROUNDTABLE II

Keynote II:
NIS2, CRA, AI Act, Data Act, RED, ERJU, Product Liability Directive: What we can learn from cybersecurity regulatory compliance in the EU rail industry.

The last decades have seen a major shift. What once seemed like a period of eternal peace in Europe after the end of the Cold War has turned into a situation in which the threat of a hot war has become a reality for which the European countries must prepare. At the same time, computers and telecommunication systems have found their way into every nook and cranny of the modern economy and society. This is the recipe for a perfect storm: on the one hand, highly sophisticated and motivated attackers; on the other hand, all our modern critical infrastructure is vulnerable to cyber-attacks. It is no wonder that the EU has taken steps to protect their citizens and economies by introducing several directives addressing cyber security and resilience in critical infrastructure and essential entities supporting them.

Quite a few directives have to be implemented into national law with their regulations on top. This talk will give insight into how Stadler, a decentralized organization spanning two dozen countries, tackles this maze of laws, regulations, technical standards, and resulting customer demands.

Gabriela Bogk had the fortune to have access to computers when growing up in East Berlin, so she's now looking back at 40 years of experience, with very early exposure to reverse engineering and information security. Her professional career started 30 years ago, taking her from administrating the first website used for advertisement in Germany, real-time programming, 3D graphics, and signal processing to embedded development. She pivoted to information security as a profession more than 20 years ago, first as a consultant, doing pen testing, cryptanalysis, reverse engineering, and incident response, later in governance roles such as Principal Security Architect for Nokia, as well as in a CISO role at Volkswagen for two years, and, for five years now, Stadler. Gabriela has been an expert witness to the German Bundesverfassungsgericht and at hearings of the Bundestag.

Roundtable II:
NIS2, CRA, Product Liability Directive, etc.: How to navigate in the jungle and set priorities right?

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 31st 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 33 (28.01.2025), 34 (14.05.2025), 35 (28.10.2025)

□ **33rd Swiss CISO Summit**
28.1.2025: 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

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) Cyber Command**

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.

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.

swisscisosummit

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

Sponsorships:

DETECON

Platinum

pwc

Gold

Lucerne University of Applied Sciences and Arts HOCHSCHULE LUZERN

SWITCH

SWISS POST

Silver

Partner:

satw it's all about technology