

PERSONAL INVITATION TO 11TH SWISS CISO SUMMIT

Detection of Threats and APT:

Which approaches perform in corporations, and how to communicate incidents?

18 October, 2017



PERSONAL INVITATION

Dear CISO,

You are kindly invited to the 11th Swiss CISO Summit – a series of moderated round-table discussions for sharing information security practices and strategies among senior professionals.

Due to there being only a limited number of places, we kindly ask you to confirm your attendance as soon as possible.



Prof. Dr. Bernhard M. Hämmerli

Detection of Threats and APT: Which approaches perform in corporations, and how to communicate incidents? October 18, 2017

TIME: 12:00 pm

PLACE: KKL: Kunst- und Kongresszentrum Luzern, Europaplatz 1, 6002 Luzern
(3 walking minutes from Lucerne train station, parking available)

Free Entrance to Swiss Cyberstorm (9-12:30h and evening party / dinner)

KEYNOTES: Addressing General Threats and APT: Experience with an all-in-one approach
Stefan Lueders, CISO CERN

Communication throughout incidents and crisis

Juan Carlos Lopez Ruggiero, CSO EMEA DXC Technology, before Chief Risk Officer at Royal Philips

Key benefits:

- Experience industry best practices in the Swiss market
- Actively participate 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 organisation

Join the Swiss CISO Summit and benefit from the peer exchange!

Detection of Threats and APT:

Which approaches perform in corporations, and how to communicate incidents?

October 18, 2017

KEYNOTE I

Addressing General Threats and APT: Experience with an all-in-one approach

Like any other enterprise, university and organization, CERN is under permanent cyber-attack: automatic scans, script-kiddies, white hats, hackers, but also through advanced persistent threat (APT) actors trying to infiltrate the organization. Given CERN's academic environment, however, CERN cyber-security must be well balanced with CERN's academic mandate and the free and open operation of its assets. This presentation shall outline CERN's computing environment, the identified cyber-risks associated with it, and the various measures implemented and deployed in order to prevent, protect and detect any kind of cyber-attack.



Stefan Lüders, PhD, graduated from the Swiss Federal Institute of Technology in Zurich and joined CERN in 2002. 2009 on-going, he is heading the CERN Computer Security Incident Response Team as CERN's Computer Security Officer with the mandate to coordinate all aspects of CERN's computer security - office computing security, computer centre security, GRID computing security and control system security - whilst taking into account CERN's operational needs. Dr. Lüders has presented on computer security and control system cyber-security topics at many different occasions to international bodies, governments, and companies, and has published several articles.

KEYNOTE II

Communication throughout incidents and crisis

The communication concept in security incidents and crisis management is a subject that involves three disciplines with common elements: Security, Risk and Compliance. By identifying how to communicate, it means knowing how to handle it. The speaker will bring up communication processes and notions used in case of incidents and crises and share some "do and don't's" from real environments with an eye on the imminent GDPR regulation.

Three basic aspects of the speech are:

- The Incident must stay underground.
- The Incident can be communicated internally, but to a limited group (still secret).
- The Incident must be brought to media.



Juan Carlos Lopez Ruggiero is global Risk and Security Executive with 20+ years' experience in implementing complex IT solutions in Risk Management, Cyber Security, Regulatory Compliance and Quality Management across multiple countries and industries. He lead IT organizations in implementing COSO, COBIT, ERM, ISO 27001, 6SIGMA, ISO 31000 and CMMI tenets, Lean Manufacturing strategies, and metric-based management. Having been the global CISO and Chief Risk Officer for Royal Philips, Juan Carlos is currently the CSO for DXC Technology in Switzerland and GDPR Lead for the EMEA region. He owns a degree in Law and speaks at least 7 languages fluently.

Detection of Threats and APT:

Which approaches perform in corporations, and how to communicate incidents?

October 18, 2017

ROUND-TABLE SESSION I

Balancing investments into regular information security and APT defence: sharing good practices

Every enterprise has open regular information and IT security issues, and it is not possible to cover all risks at short hand. With this background, many CISO state that addressing APT is no option, as long as basic security issues remain unsolved. We will discuss, which strategies in detecting and mitigating APT are successful: all-in-one approach, provider with APT specific skills, self-install APT detection tools, or increasing log period to two or more years? The CISO will exchange their view and share their experience in these issues.

Exchange between the groups: A delegate from each group will present major findings to the audience.

ROUND-TABLE SESSION II

Sharing communication concepts of internal and external incident and crisis communication

After detecting potential incidents in the first phase, verification is needed to be sure that there's a real incident. At this stage, very few employees only are involved with strict rules to keep it secret. The longer the incident is analyzed and the more people are involved, the secrecy requirements become higher. An internal limited communication will be necessary. Eventually, a decision must be taken: Is this a board issue? Do the authorities (e.g. in case of GDPR relevant issues) have to be informed, do the media and shareholders have to be informed? We discuss the secrecy and communication concepts, and share the success and the open question in this respect. The goal is to elaborate on industry best practice, and learn about the variety in different sectors.

Exchange between the groups (as in session I) and wrap-up of the event.

NEXT SUMMIT JANUARY 30, 2018

Introduction to the 12th Swiss CISO Summit

Tentative topic: Internet of Things (IoT), Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) security: CISO's responsibility in context with other organizational units

Date and place: January 30, 2018: Zunfthaus zur Schmiden, Zurich

PRELIMINARY OUTLOOK ON THE FOLLOWING SUMMIT

13th Swiss CISO Summit

Tentative topic: Insider Threats: How to manage insider threats with monitoring, processes and technologies?

Date and place: Airport Zurich, TBD May 2018

PARTICIPATION

Join Swiss CISO Summit

Participation is by invitation only. We accept proposals for new participants. The number of participants is limited to max. 40 per summit because the effectiveness of trust circles and sharing are limited in larger groups.

Single summit CHF 450.– per participant

Three summits CHF 1'000.– per participant (25% discount for booking three consecutive summits)

Cancellation Policy

Cancellations of registration are free of charge but 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, however, 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

REGISTRATION

Register by just replying to the invitation email with all your details – or by filling out this form and mailing it

Three consecutive summits for CHF 1'000.– 3 events, Summit 11, 12 (30. 01.18) and 13 (May, 2017)

11th Swiss CISO Summit, 18 October, 2018 for CHF 450.– (single event)

First name

Last name


Organisation

Street / No.


ZIP / City

Phone

Email



Join this peer-to-peer summit for sharing strategies to mitigate latest information security threats.



FACT SHEET I

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 do we maintain confidentiality?

The Swiss CISO Summit is provided as a closed-door event. This exclusive CISO Executive three ticket 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.


Why 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. The summits are held strictly under the Chatham House Rules, which is the ruleset to treat the shared information with full discretion.


- 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 the current strategies on managing security threats today and to prepare for the future
- Make new connections and equip yourself with insider 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.



Walk away with the knowledge
and insights to make informed decisions
on today's CISO challenges!



FACT SHEET II

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 where 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 has been adopted in Norway where it ran under the name Sikkerhetstoppmøte. All this experience gained by Prof. Dr. Hämmerli is put into the today's Swiss CISO Summit.

Who prepares and facilitates it?




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 experience in information security in governments, industry and academia. He is also leading the Cyber Security activities of the Swiss Academy of Engineering Sciences SATW. 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. Additionally, he is also teaching at the Norwegian University of Science and Technology 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
- 13.15 Welcome and introduction
- 13.30 Keynote from experts or members
- 14.20 Round-table session I
- 15.20 Exchange between the groups and wrap-up of round-table I
- 15.40 Break
- 16.00 Round-table session II
- 16.50 Exchange between the groups and wrap-up of the round-table II
- 17.10 Summary note
- 17.30 Cocktail and aperitif

The meeting is held three times per year.



Active participation guaranteed!
«Enjoy dedicated networking with
like-minded senior peers»



SWISS CISO SUMMIT SPONSORS

PLATINUM SPONSOR

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



At PwC, our purpose is to build trust in society and solve important problems. PwC looks at cybersecurity as one of the biggest challenges to solve in today's times and provides a full stack of cybersecurity consulting services. PwC's Cybersecurity 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. We're a network of firms in 157 countries with more than 208,000 people who are committed to delivering quality in assurance, advisory and tax services. Within PwC Switzerland around 2,800 employees and partners in 14 locations in Switzerland and one in the Principality of Liechtenstein help to create the value organisations and individuals are looking for.