Personal Invitation to 21th

swisscisosummit

Traditional and New Forms of System Security Testing and Verification:

Available Options and Success Cases

26th January Part I, and 9th February 2021 Part II, online

DETECON CONSULTING

pwc

SWITCH

SWISS POST

Sponsorships:

Platinum

Gold

Silver

Detecon (Schweiz) AG
Löwenstrasse 1
8001 Zürich
Schweiz
www.detecon.ch

Contents

Introduction

Dear CISO,

You are kindly invited to the 21th 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

Traditional and New Forms of System Security Testing and Verification: Available Options and Success Cases

Part I	**Security Testing Methods, Evaluation & Diversity: In which situation to apply which method** Bernhard Tellenbach ZHAW Professor & Valentin Zahnd Partner Scanmeter
Date	**26th January 2021**
Time	**Summit starts 13:15 and ends 15:30** (virtual room opens at 13:00)
Format	**Webex online**
Part II	**Participative Security: How to co-operate with hackers successfully?** Marcel Zumbühl, CISO Swiss Post
Date	**9th February 2021**
Time	**Summit starts 13:15 and ends 15:30** (virtual room opens at 13:00)
Format	**Webex online**
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

Security testing has traditionally multiple methods: Software module, system and integration test may be considered a technique. However, recently, only very few software had proper security specifications, and therefore those tests were more of operational nature. Code walkthrough is also a traditional test, but with today‘s complexity and numbers of code lines, this is only with excellent tools feasible. Another test form is to check systematic security (conformance to standards as e.g. ISO 27000 series, NIST, BSI baseline protection profiles). In specific situations, testing might be raised to certification. General penetration testing (corporate crew and external crew) also has a long tradition. As the severity and the amount of attack increased, the new testing forms came up.

The degree of automation in testing has relevantly increased. Vulnerability scanning, attack simulation, automatic penetration suites are just a few examples of automated testing. The strategic goals of the Europe Research Funding Agency are to develop software suites that test up to certification level software and systems. With the keynote of Bernhard Tellenbach and Valentin Zahnd, we get insights into the state-of-the-art of automated testing.

Penetration testing has a long history but is seen today as „conditio sine qua non“ to be performed in addition to systematic information security. Depending on the company‘s size and sensitivity of the application and data, companies make bi-annually, annually, semi-annually, quarterly, monthly, or even bi-weekly penetration tests. Newer forms include

- **Bug Bounty programs.** Crowed sourced cybersecurity testing approach based donating award money for reported weaknesses, a test from which allows continuous testing.

- **Red teaming.** A full-scope, multi-layered attack simulation designed to measure how well a company‘s people and networks, applications and physical security controls can withstand an attack from a real-life adversary.

- **Purple Teaming.** Security methodology whereby red and blue teams work closely together to maximize cyber capabilities through continuous feedback and knowledge transfer.

- **Ethical Hacking.** Performed by black, grey and white hackers.

The keynote of Marcel Zumbühl gives insights and practical hints.

With this summit, we want to strengthen the participant‘s knowledge of security testing. On 26th January (Part I) and 9th February (Part II) each part features a keynote and is followed by an one-hour roundtable discussion.

Alike corona is security: good security means also testing, testing, testing …

Part I 26th January, online

Keynote

Security Testing Methods, Evaluation & Diversity: In which situation to apply which method?

In the past, testing your systems and infrastructure thoroughly and regularly for weaknesses was considered exotic. Fortunately, by today, companies recognized that IT plays a central role in business performance and must be robust. Besides, growing political and regulatory pressure from Europe resulted e.g. in the Regulation (EU) 2019/881 (Cybersecurity Act) and discussions on a Common Criteria based European Cybersecurity Certification Scheme (EUCC). Against this background, security testing and verification approaches such as Bug Bounty programs, Ethical Hacking, Penetration Testing, Red Teaming, Purple Teaming, Automated Security Testing, and Breach & Attack Simulation Solutions will be presented and debated in respect to advantages and disadvantages. Furthermore, we take a closer look at the approach, a top priority on the EU‘s research agenda - automated security testing and certification. Using the example of ‚scanmeter‘, we will touch on several use cases for security improvement programs and show that use cases rely on technical aspects and integration into existing process landscapes.

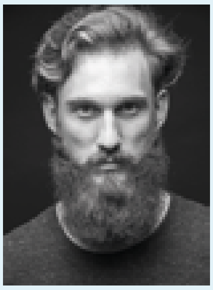
Roundtable Session

Economical and effective security testing: How to reach best fit for a specific case?

The options for security testing are very broad and comprises manual and automatic testing methods. Automation in security testing advances in recent times with numerous new tools. Methods like spear-phishing the workforce, red & purple teaming, ethical hacking, penetration testing and table-top exercises usually are manual methods. In contrast, vulnerability analysis, automated penetration test, automated web-application testing, attack simulation are often automated.

The debate will position a large number of services. Success stories, as well as failures, will be shared. The evaluation, in which case, which method might be best, will bring up economical, efficiency, and practical aspects. As a result, the participants have an in-depth understanding of security testing and can position the applicability of the available service options.

Bernhard Tellenbach (PhD from ETH Zurich) is Professor and head of the information security research group at the Zurich University of Applied Sciences (ZHAW). Before he worked as security researcher at ETH Zurich, lecturer at HSR, and senior security consultant at Consecom AG. He is an active member of the security community in Switzerland and Europe. He leads the Swiss Cyber Storm association, represents Switzerland in the steering committee of the European Cybersecurity Challenge coordinated by ENISA, heads the Cyber Security thematic platform of the Swiss Academy of Engineering Sciences (SATW), and is a member of the Cyber Security Advisory Board of SATW.



Valentin Zahnd worked in security research and as a security consultant for several years and is now a partner at scanmeter, which focuses on next-generation cybersecurity assessments and all its surrounding integration and managed security services. In addition, Valentin is a member of the board of Swiss Cyber Storm and coaches the Swiss National Hacking Team for the European Cyber Security Challenge.

Part II 9th February, online

Keynote

Participative Security – How to co-operate with hackers successfully?

As one of the first Swiss companies, Swiss Post Group has launched a Bug Bounty Program. Ethical hackers are invited to probe the security of selected online services. Bugs found are evaluated and bounties paid subsequentially. In this session, Swiss Post Group will share their experience with the program, both from a legal, security and operational/development perspective. The program is part of Swiss Post's information security strategy to establish participative security and focus on building trust for digital services.

Roundtable Session

Bug Bounty: How to professionally set up a program and taking advantage?

In general, the corporate co-operation with hackers for the benefit of cybersecurity is this session's focus. How to deal with hints on vulnerabilities coming from hacker communities? When is a contract an option? How to test hackers on their honesty towards their own company? How to deal with the risks when co-operating with hackers? Which measure should be taken when the belly feelings are indicating red? What is the difference in outcome between a penetration test and bug bounty?

The roundtable's final target is to exchange on new models and clarify engagement rules, risks, and precautions.

Marcel Zumbühl works for Swiss Post as Chief Information Security Officer (CISO) and member of the IT Board since August 2018 and is responsible for the information security in the Group. The 50-year-old holds a master's degree in computer science with a minor in business administration. After studying at the University of Berne, he worked both in Switzerland and abroad for various companies such as Accenture, Swisscom and Credit Suisse. Since 2009, Marcel has also been a guest lecturer for risk management and risk communication at ETH Zurich, and since summer 2020 is Co-President of the Information Security Society Switzerland (ISSS).

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

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 Sponsorships

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

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 21th 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 events, Summit 21 (26.01. & 09.02.2021), Summit 22 (01.06.2021) and Summit 23 (12.10.2021)

□ **21th Swiss CISO Summit, 26.01. & 09.02.2021 online for CHF 400.-**
(single event part I & II, corona discount, no single part booking foreseen)

First Name ____________________ **Surname** ____________________

Organisation ____

Street / No. ____________________ **ZIP / City** ____________________

Phone ____________________ **Email** ____________________

Signature ____________________ *Date* ____________________ swisscisosummit

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

DETECON CONSULTING

pwc

SWITCH

SWISS POST

Sponsorships:

Platinum

Gold

Silver