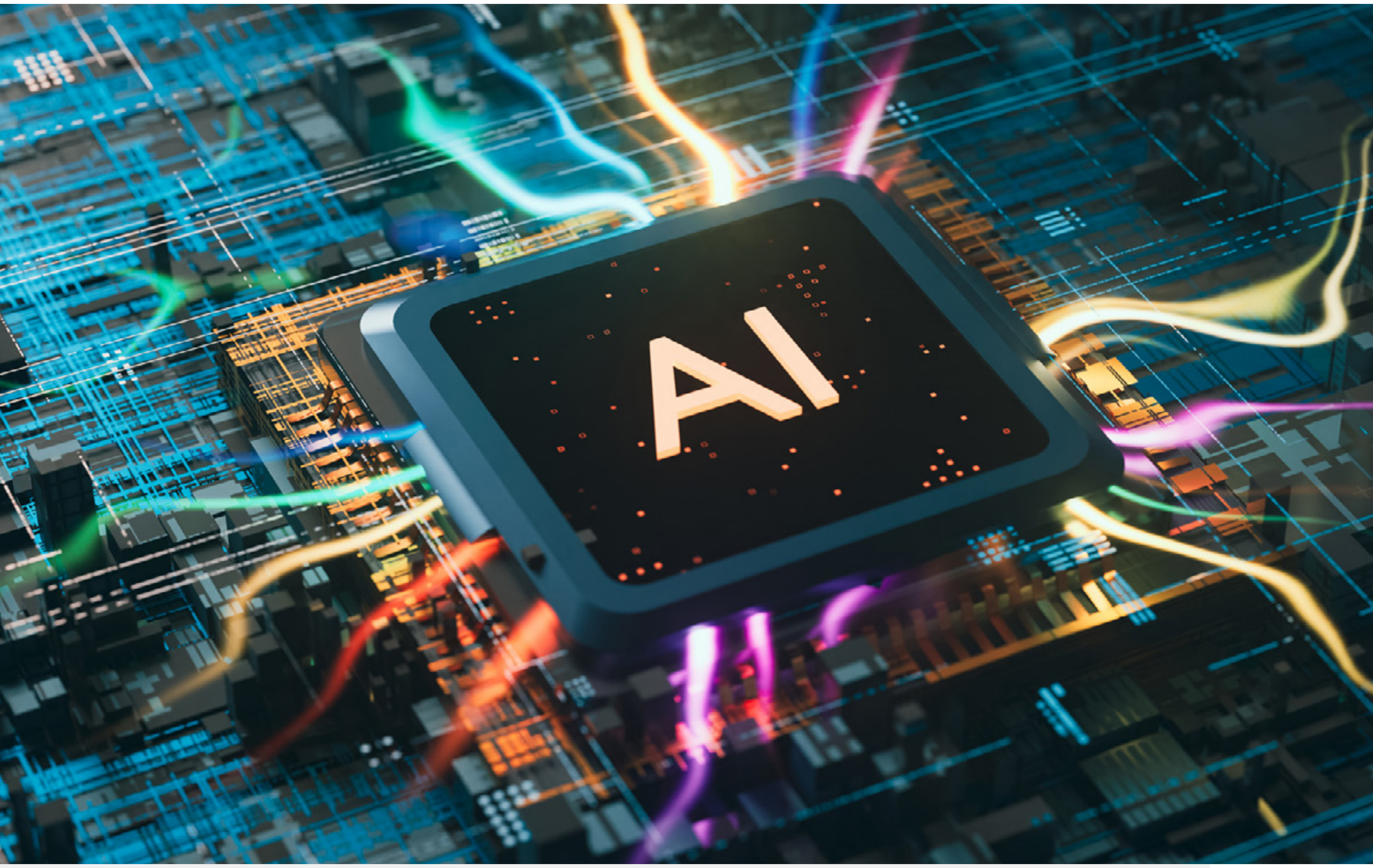
PERSONAL INVITATION to 32nd

swisscisosummit



AI causes a radical change for security and attackers: who profits more?

22nd October 2024, Kursaal Bern, Bern
(upon requests, virtual participation will be organized)

Sponsorships:

DETECON

Platinum

pwc

Gold

Lucerne University of Applied Sciences and Arts HOCHSCHULE LUZERN

SWITCH

paloalto NETWORKS

SWISS POST

Silver

Partner:

satw it's all about technology

Contents

1 Introduction

Dear CISO,

You are kindly invited to the 32nd 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

AI causes a radical change for security and attackers: who profits more?

Date	22nd October 2024, co-located with Swiss Cyberstorm
Time	9-19h with Cyberstorm visit, CISO Summit only: 12:15 to 19:00h
Location	Kursaal Bern, Room Panorama

Keynote 1 **The reality behind Large Language Models (LLMs) hype in cybersecurity: What is the short-term technological forecast for offensive and defensive use?**
Andrei Kucharavy, Ass. Professor at HES-SO Valais-Wallis, and Co-director of the Generative Learning Center at HES-SOLearning Center at HES-SO

Keynote 2 **AI in Cybersecurity: How does the Double-Edged Sword for Attackers and Defenders work?**
Mark Barwinski, global cybersecurity executive

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

AI causes a radical change for security and attackers: who profits more?

In cyber security, AI and LLM are applied to log data to detect indicators of compromise (IoC) and reduce IoC by prioritization to a digestible number: this saves a lot of work in the security operation centers. The detection includes relevant improvement in detecting zero-day exploits.

For cyber attackers, AI offers unprecedented opportunities to enhance their malicious activities. AI-driven tools can automate the discovery of vulnerabilities, craft sophisticated phishing attacks, and even evade traditional security measures by learning and adapting to defensive strategies. Processing vast amounts of data quickly allows attackers to identify and exploit weaknesses with greater precision and speed. This technological edge can make cyber-attacks more efficient, scalable, and more difficult to detect because of the enormous number of variations of attacks.

The first discussion round on **"AI and Large Language Models: How to position the technologies and their use in cyber defense and offense?"** will provide a deeper understanding of the topic and the associated technologies.

The second discussion round on **"AI-based products with real-time threat detection, predictive analytics, and automated response mechanisms: Why to install it, and which attacks can and cannot be defended?"** will explore how AI technology can be used for the future of cyber-security. Will AI tip the balance in favor of attackers, making cyber threats more pervasive and harder to combat? Or will defenders harness AI's potential to create impenetrable defenses and outsmart their adversaries? This session aims to spark a lively discussion on the transformative impact of AI in cybersecurity, inviting you to share your perspectives and experiences as we collectively navigate this complex and evolving landscape.

With Andrei Kucharavy and Mark Barwinski, we have two excellent speakers who will guide us through the AI / LLM world, preparing us for a vivid discussion.

Finally, we are embedded into Swiss Cyber Storm, which is also dedicated to AI in cyber. Take advantage of the free entrance and inform yourself more broadly.

Artificial intelligence (AI), in its broadest sense, is intelligence exhibited by machines, particularly computer systems. It is a research-filed that develops and studies methods and software that enable machines to perceive their environment and use learning and intelligence to take actions that maximize their chances of achieving defined goals. High-profile AI applications are e. g. advanced web search engines; YouTube recommendation system, self-driving, ChatGTP and Amazon.

A **large language model (LLM)** is a computational model capable of language generation or other natural language processing tasks. As language models, LLMs acquire these abilities by learning statistical relationships from vast amounts of text during a self-supervised and/or semi-supervised training process. The largest LLM is by today artificial neural networks built with a decoder-only transformer-based architecture, which enables efficient processing.

3 KEYNOTE I AND ROUNDTABLE I

Keynote I:
The reality behind Large Language Models (LLMs) hype in cybersecurity: What is the short-term technological forecast for offensive and defensive use?

The recent jump in capabilities and accessibility of LLMs led to an expectation of technological disruption across industries – including cyber-security. However, almost two years after the original release of ChatGPT and grandiose speculations of LLM applications in cyber, their real-world usage remains scant and mostly experimental. This keynote provides the attendees clues as to why and what disruption applications LLMs might or might not have in cyber, offensively or defensively.

Andrei Kucharavy is an Assistant Professor at HES-SO Valais-Wallis, Co-director of the Generative Learning Center at HES-SO, and an ex-distinguished Cyber-Defence Campus Fellow. Since 2020, his research has focused on the offensive use of Generative AI in cyber operations and ways to counter it.

Combining his technical expertise with a more holistic approach to technological monitoring and forecasting, over the last two years, he led the redaction of the "Fundamentals of Generative Large Language Models and Perspectives in Cyber-Defense" public report for armasuisse S+T the "LLMs in Cybersecurity: Risks, Exposure, Mitigations" Springer reference handbook.

Roundtable I:
AI and Large Language Models: How to position the technologies and their use in cyber defense and offense?

KEYNOTE II AND ROUNDTABLE II

3

AI in Cybersecurity: How does the Double-Edged Sword for Attackers and Defenders work?

Artificial intelligence (AI) has emerged as a powerful tool that cyber attackers and defenders can use. As organizations increasingly rely on digital infrastructure, the stakes in the cybersecurity battle have never been higher. AI's ability to process vast amounts of data, identify patterns, and make autonomous decisions presents opportunities and challenges.

From the perspective of a cyber attacker, AI offers unprecedented opportunities to enhance their malicious activities. AI-driven tools can automate the discovery of vulnerabilities. Processing vast amounts of data quickly allows attackers to identify and exploit weaknesses with greater precision and speed. This technological edge makes cyber-attacks more efficient, scalable, and difficult to detect.

From the Chief Information Security Officers' (CISO) perspective, AI can be leveraged to bolster their defenses against these increasingly sophisticated threats. AI enhances the capabilities of cyber defenders by providing real-time threat detection, predictive analytics, and automated response mechanisms. Products like Darktrace, CrowdStrike, IBM's QRadar, and Microsoft's Defender are revolutionizing security teams' operations. These tools reduce the window of opportunity for attackers. Additionally, AI supports managing the overwhelming volume of security alerts, allowing analysts to focus on the most critical incidents. By integrating AI, organizations can stay one step ahead of adversaries.

Will AI tip the balance in favor of attackers, making cyber threats more pervasive and harder to combat? Or will defenders harness AI's potential to create impenetrable defenses and outsmart their adversaries?

Mark Barwinski is a global cybersecurity executive with over 21 years of experience leading large-scale initiatives across the financial, professional services, manufacturing, governmental, and private sectors. As the former Global Head of Cyber Operations at UBS, Mark defined and executed global strategies and operated the Security Operations Center (SOC), incorporating standards and machine learning to enhance detection and operational efficiency.

Mark began his career at the National Security Agency (NSA), where he played a key role in offensive and defensive cyber operations. His work included advising military officers, securing high-risk operations, and leading advanced bi-lateral cybersecurity programs, leading to several mil-awards.

Roundtable II:
AI based products with real-time threat detection, predictive analytics, and automated response mechanisms: Why to install it, and which attacks can and cannot be defended?

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, 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 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 32 (22.10.2024), 33 (28.01.2025), 34 (14.05.2025)

□ **32nd Swiss CISO Summit**
22.10.2025: CHF 450.– for all forms of participation

First Name ____________ Surname ____________

Organisation ____________

Street / No. ____________ ZIP / City ____________

Phone ____________ Email ____________

Signature ____________ *Date* ____________

7 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 **SWITCHFOUNDATION**

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 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

7

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**
paloalto® NETWORKS	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.
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.

swissciso summit

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

Sponsorships:

DETECON

Platinum

pwc

Gold

HOCHSCHULE LUZERN

SWITCH

paloalto NETWORKS

SWISS POST

Silver

Partner:

satw it's all about technology