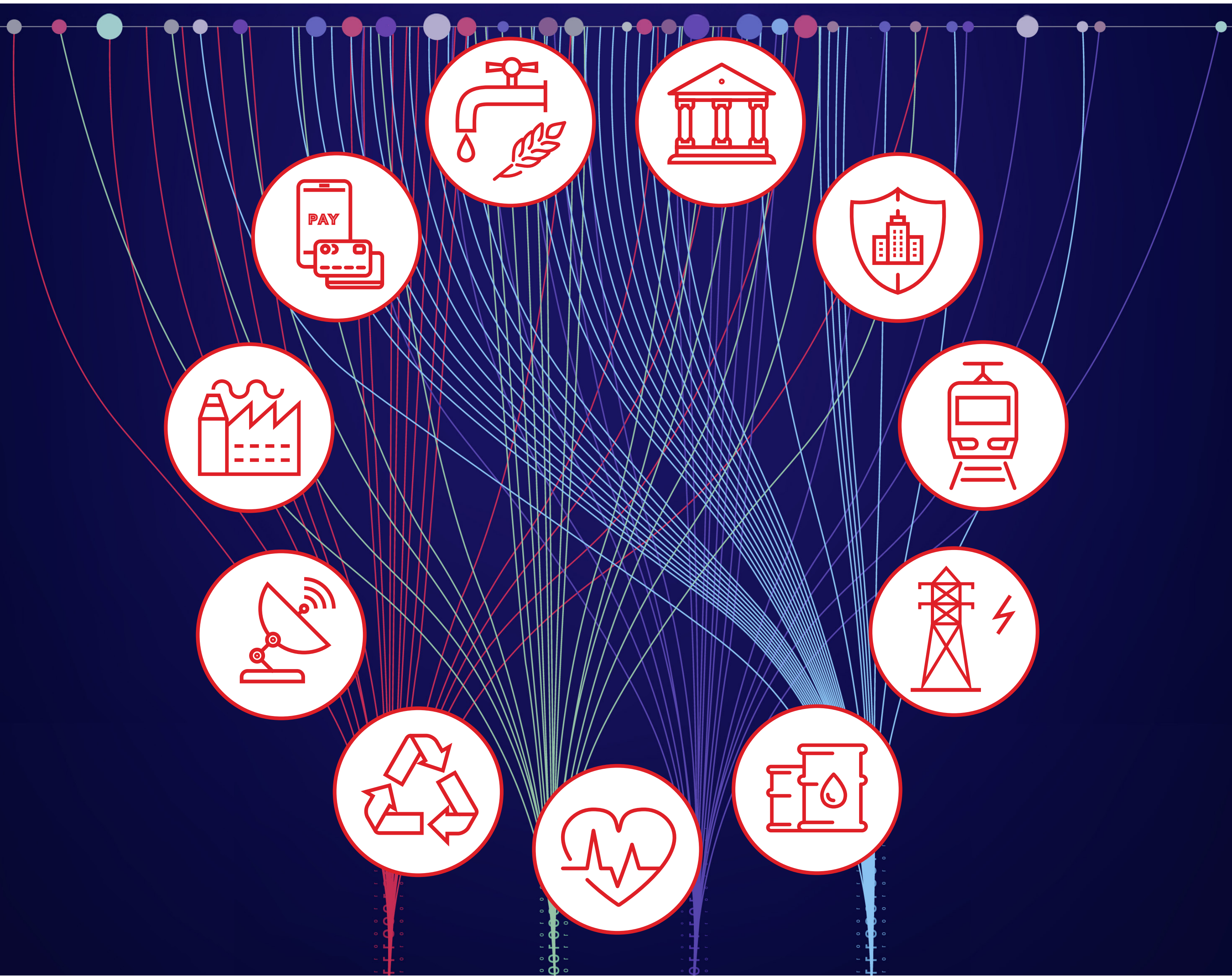
SWISS **OT-IT**
CYBER SECURITY
FORUM



Detailed Asset Management for Software and Hardware: **how do SBOM and HBOM impact security?**

SBOMs and hardware asset management are prerequisites for fast incident response. Knowing what we have and where enables rapid mitigation—hence why NIS2 and NIST emphasize SBOMs.

17th Forum, March 5, 2026, 12:00-20:30 h

Vetropack, Schützenmattstrasse 48, 8180 Bülach (parking available)

SWISS **OT-IT**
CYBER SECURITY
FORUM

Mission

Why should you attend?

The Swiss OT-IT Cyber Security Forum Series is a sequence of events which takes place three times per year, with the strategic goal to unify OT and IT decision makers. The main objective is achieving significant advances in security.

Background:

Historically, the two communitities had completely different set-ups:

- IT used to follow the speed of technology evolvement, with product cycles of about three years and extremely fast fixing of faults and errors: short reaction time of less than one hour is common practice by today.
- OT used to create solutions in the mechanical space with life cycles reaching from 25 to 70 years, with little maintenance on average every 3-5 years.
  In the past few years the use of IT in OT installation has been increasing dramatically and OT is now fully integrated in cyberspace. Therefore, the need to connect the two communitities is now more important than ever before in order to address the mutually dependent topics including security issues.

Design of the forum:

- 3 meetings per year
- 2-3 talks from industry leaders delivered in English
- Several roundtables lasting 1 hour in D and E at every meeting

Participation fee:

- CHF 360 per event, alternatively CHF 960 for three events (one year)
- Participation by invitation only. Proposal for inviting additional key persons mail to: bmhaemmerli@OT-IT-CyberSecurityForum.ch

Content:

The content will be coordinated by Prof. Dr. Bernhard M. Haemmerli, Hochschule Luzern, and will be created by the organizing committee.

Organizing Committee:

Drives the process for the meetings with delegates, sponsors and selected partners.

MAIN SPONSOR

KUDELSKI SECURITY

LOCATION SPONSOR

vetropack

SPONSORS

ALSEC protect critical infrastructure

HSLU Hochschule Luzern

CKW.

PARTNER

satw it's all about technology

Detailed Asset Management for Software and Hardware: **how do SBOM and HBOM impact security?**

Asset Management is the first prerequisite to understand the organization's real risk exposure. But a simple inventory of devices and software packages is often not enough. To respond quickly to vulnerabilities and incidents, you need to know the components inside your hardware and software – this is where SBOMs and component-level visibility matter.
SSL-related incidents showed how a single vulnerable component can make a difference, particularly when this single component is implemented in 100 different applications. If you already have a component-based asset management in place, you can rapidly identify where a component is used, prioritize the most exposed systems, and drive remediation (patching, upgrades, compensating controls) with much less downtime. If you first must build the inventory during a crisis, the time you remain vulnerable – and the operational impact – becomes significantly longer.

The Broader Landscape: SBOMs, Supply Chain Security and NIS2 in Context

NIS2 is one step in a broader regulatory reform that helps making supply chain security a high priority area in cybersecurity compliance:

- EU Cybersecurity Act (2019): Established ENISA (the EU cybersecurity agency) as a permanent agency and created a voluntary cybersecurity certification framework for Information and Communication Technology (ICT) products. SBOMs were not required, but third-party supplier component management was specified as best practice.
- ETSI Standards (2020): ETSI (European Telecommunications Standards Institute) first published standards for consumer IoT security in June 2020. These recommended maintaining a list of third-party software and managing known vulnerabilities, which aligns with SBOM principles, even though "SBOM" does not explicitly appear in the standards.
- NIS2 Directive: Proposed in December 2020 and adopted as law January 2023, emphasizes supply chain security and third-party supplier component management.
- TR-03183 Part 2: SBOMs become mandatory (October 2024) for third-party supplier component management.

- EU Cyber Resilience Act (CRA): Adopts the mandatory SBOM requirement from TR-03183 Part 2 when it is adopted as law in November 2024, though not fully enforced until December 2027.
- Digital Operational Resilience Act (DORA): Couldn't wait for EU CRA enforcement and requires SBOMs now. Proposed January 2023 and enforced as of January 2025 for financial services including traditional banking, fintech, and crypto services.
- US Executive Order 14028, established in May 2021, aims to enhance the country's cybersecurity by mandating that software vendors supplying the federal government submit a software bill of materials (SBOM) for each product. This order necessitates the automatic generation of software inventories in a machine-readable format, rendering SBOMs that don't support automation non-compliant.

We typically face two linked challenges: (1) building and maintaining asset management and SBOM capability, and (2) preparing for online / real-time KPI and compliance monitoring. The key is to phase this journey – starting with what you need for faster vulnerability response and incident handling, and then expanding to broader compliance and continuous assurance.

Detailed Asset Management for Software and Hardware: **how do SBOM and HBOM impact security?**

These speeches prepare the two discussion rounds:

1. SBOM and requirements today and in future: What is it, why we do it and how to manage stakeholder expectancy?

Daniel Heppner, Head of Intelligence & Defence, Roche Diagnostics

2. Implementation and Experience: How to identify KPI, organize data gathering, and sharing dos and don’ts?

Chris Ditze-Stephan, HSLU lecturer and OT Expert @ zentric

Discussion Round 1:

SBOM definitions and goals: By when and how to successfully initiatea project?

Discussion Round 2:

The journey of SBOM implementation: What are the critical factors for sustainable success?

We are looking forward to your participation, so that we can develop forward- thinking approaches and gain clarity and knowledge on AI in OT and IT security.

Bernhard Hämmerli on behalf of the organizing committee

Date:	**March 5, 2026**
Time:	**12:00-20:30 h**
Location:	**Vetropack, Schützenmattstrasse 48, 8180 Bülach (parking available)**

SWISS **OT-IT CYBER SECURITY** FORUM

17th Swiss OT-IT Cyber Security Forum
March 5, 2026, 12.00 – 17:30 h
Social activity and dinner end at 20:30 h

Agenda

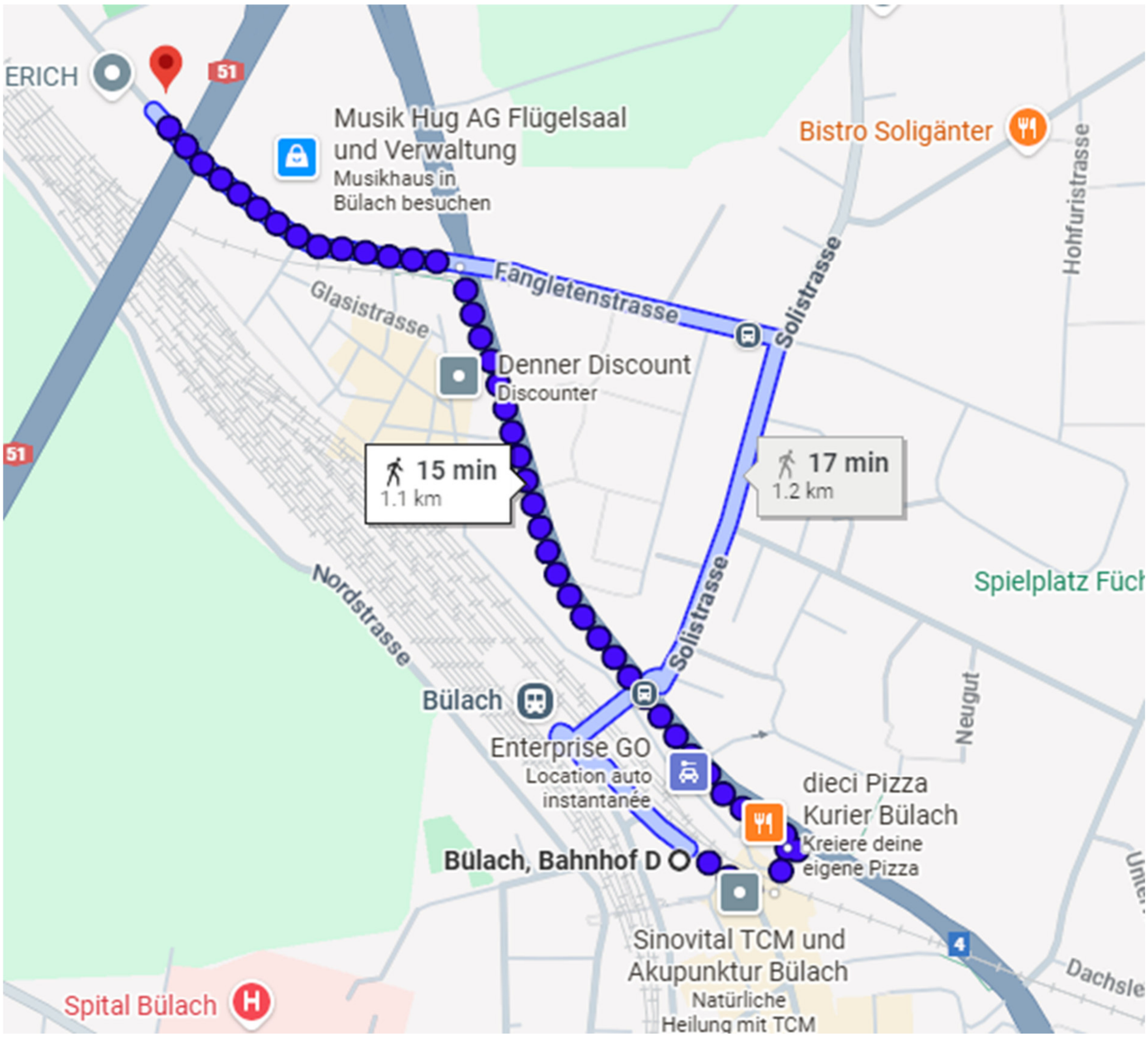
In-Person Meeting: Vetropack, Schützenmattstrasse 48, 8180 Bülach

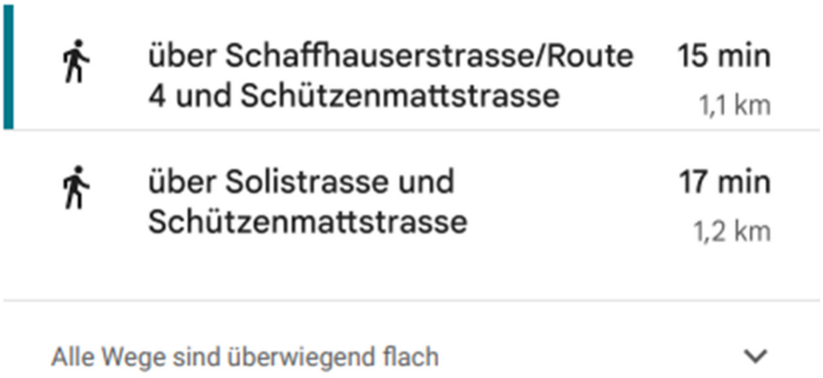
An online roundtable will be offered with online streaming of presentations (high quality video and audio)

12:00	Lunch at Vetropack
12:45	Networking among participants
13:10	Welcome note by Markus Mueller-Fehrenbach, Vetropack Security and Prof. Bernhard Hämmerli
13:30	**SBOM and requirements today and in future: What is it, why we do it and how to manage stakeholder expectancy?** Daniel Heppner, Head of Intelligence & Defence, Roche Diagnostics
14:10	Roundtable 1: **SBOM definitions and goals: When and how to successfully initiate a project?**
15:00	Exchange between groups
15:15	Break
15:45	**Implementation and Experience: How to identify KPIs, organize data gathering, and sharing dos and don’ts?** Chris Ditze-Stephan, HSLU lecturer and OT Expert @ zentric
16:25	Roundtable 2: **The journey of SBOM implementation: What are the critical factors for sustainable success?**
17:05	Exchange between groups
17:20	Wrap-up and information on next meeting
17:30	Social activity at Vetropack: Vetropack Insights: What people normally do not know about, and are surprised to learn…
18:45	Invited Dinner **Restaurant zum goldigen Winkel**, Obergasse 13, 8180 Bülach, parking available, 4 min by car, and 13 min walking to Bülach SBB
20:30	End of the forum

Bülach, Bahnhof D, 8180 Bülach nach Vetropack AG, Schweiz, Schützenmattstrasse 48, 8180 Bülach

Zu Fuß 1,1 km, 15 min





über Schaffhauserstrasse/Route 4 und Schützenmattstrasse — 15 min, 1,1 km

über Solistrasse und Schützenmattstrasse — 17 min, 1,2 km

Alle Wege sind überwiegend flach

Outlook on Forum 18 and 19

Swiss OT-IT Cyber Security Forum 18

Auditing OT systems: What are the audit options, processes, and reporting approaches to enable the best response? (reconfirmation by votes)

Audit and security testing offer many different options – but which option is best for a specific situation? It is therefore important to gain an overview of the spectrum, from bug bounty, red teaming, and penetration testing to more compliance-oriented framework audits. In addition, legal frameworks (e.g., NIS2) demand real-time / online compliance reporting. The results must be communicated – but how? Is classic reporting the best option, or is risk communication more effective? We expect a vivid discussion and an exchange of experience on these topics.

Date:	Tentative: Thursday, June 11, 2026, 12:00-20:30 h
Place:	Zurich Area
Speakers:	TBD
Roundtable 1:	Understanding security testing and audits: What are the options, and what criteria should be used to select the right approach?
Roundtable 2:	Reporting, risk communication, and other ways to influence decision-makers: What are the best options to drive the desired actions?

Swiss OT-IT Cyber Security Forum 19

Topic not defined yet

One option is workforce development: How can the knowledge and expertise be secured in future? How can employees be brought up to speed with AI innovations? And how will job profiles change because of AI?

Date:	Tentative: Thursday, September 10, 2026, 12:00-20:30 h
Place:	Emmi, Milchstrasse 9, 3072 Ostermundigen (Bern)
Speakers:	TBD
Roundtable 1:	TBD
Roundtable 2:	TBD

SWISS **OT-IT CYBER SECURITY** FORUM

Registration

Please register by replying to the invitation email providing all your details – or by filling or by filling out this form, scanning it in or taking a picture, and sending the completed form to: info@OT-IT-CyberSecurityForum.ch

□ Three consecutive forums for CHF 960.–
Forum 17 (05.03.2026), Forum 18 (11. 06, 2026) and Forum 19 (10.09.2026)

□ 17th OT-IT Cyber Security Forum, March 5 11, 2025 only, at the price of CHF 360.– .

□ Please register for social activity 17:30-18:45

□ Please register for the sponsored Dinner 19:00-20:30 at
Restaurant XXXXX,

□ Online attendance: I will participate online via WebEx (see link iin the calendar entry)

First Name .... Last Name ....

Organisation ....

Job Title ....

Street / No. .... ZIP / City ....

Phone .... Cellphone ....

Email ....

Please add instructions for invoice, needing an offer etc.:

....

....

....

SWISS **OT-IT**
CYBER SECURITY
FORUM

Mission

The Swiss OT-IT Cyber Security Forum Series is a sequence of events which takes place three times per year, with the strategic goal to unify OT and IT decision makers and bring culture, language and security priorities on level of mutual understanding.

The main objective is achieving significant overall advances in security (OT & IT).

MAIN SPONSOR

KUDELSKI SECURITY

LOCATION SPONSOR

vetropack

SPONSORS

ALSEC protect critical infrastructure

HSLU Hochschule Luzern

CKW.

PARTNER

satw it's all about technology