SWISS **OT-IT**
CYBER SECURITY
FORUM

During Incident:
Stabilize or Isolate infected systems?

How to determine strategy and which actions lead to success? Debate on real-world response options for OT and IoT incidents, focusing on how to choose a course of action when safety, continuity, and national security must be equally considered, and all stay in the balance

15th Forum, June 12, 2025 12:00-20:30 h
Aula von Swissgrid, Bleichemattstrasse 31, 5001 Aarau

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 cyber-space. 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, F 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.

During Incident: **Stabilize or Isolate infected systems:**

How to determine Strategy and which actions lead to success? Debate on real-world response options for OT and IoT incidents, focusing on how to choose a course of action when safety, continuity, and national security must be equally considered, and all stay in the balance.

When something breaches your OT environment, the pressure is immediate. Do you monitor the attacker to gather intel, try to quietly contain the threat, or shut it all down—and risk disrupting critical operations and burning Swiss francs in the process?

Mark Barwinski will walk through real-world response options for OT and IoT incidents, fo-cusing on how to choose a course of action when safety, continuity, and national security are all in the balance.

In addition, he explains lessons from the Colonial Pipeline ransomware attack, explores today's geopolitical backdrop—where reports of pre-positioned malware in U.S. infrastructure point to longterm OT targeting—and consider how defenders can prepare. Drawing on early-career work in SCADA protocol research and time spent at Sandia and Pacific Northwest National Labs, Mark will share what still holds true about visibility gaps, decision-making under pressure, and what you can—and can't—turn off in a crisis. He presents, how digital twins are being used to safely simulate real environments, helping teams rehearse the unthinkable and refine their incident playbooks before the stakes are real.

The next speaker refines the processes between SOC and SOC client. Depending on specific use cases, the business stakeholders will be selected, which will be included in the decision-making process of the case. Furthermore, plenty of agreements must be made before, that experts know, where (Soc or SOC user) will be performed which activity.

Finally, Frank Papae will present innovative concepts and solution, how through reduction of controllability, the hackers could be icked out of critical systems. What do the attendees think of this compromise and what is the practical value?

These speeches prepare the two discussion rounds:

1. Refining OT-IT and IoT Detection and Response:
What are the options, who needs to decide, and what is the impact?

2. OT SOC processes: Learning from real cases and Experience sharing:
Which strategies lead to success, and what should be avoided?

We are looking forward to your participation, that we can elaborate forward think approaches, and innovative structuring of SOC decision making processes.

Bernhard Hämmerli on behalf of the organizing committee.

15th Swiss OT-IT Cyber Security Forum

During Incident:
Stabilize or Isolate infected systems:

Keynotes:

Watch, Wait, or Shut It Down? Tough Calls in OT/IoT Incident Response
Mark Barwinski, Global Security Executive

SOC – SOC User: Who are the persons to be included, and how does the decision process work?
Martin Scheu, OT Security Engineer, Switch

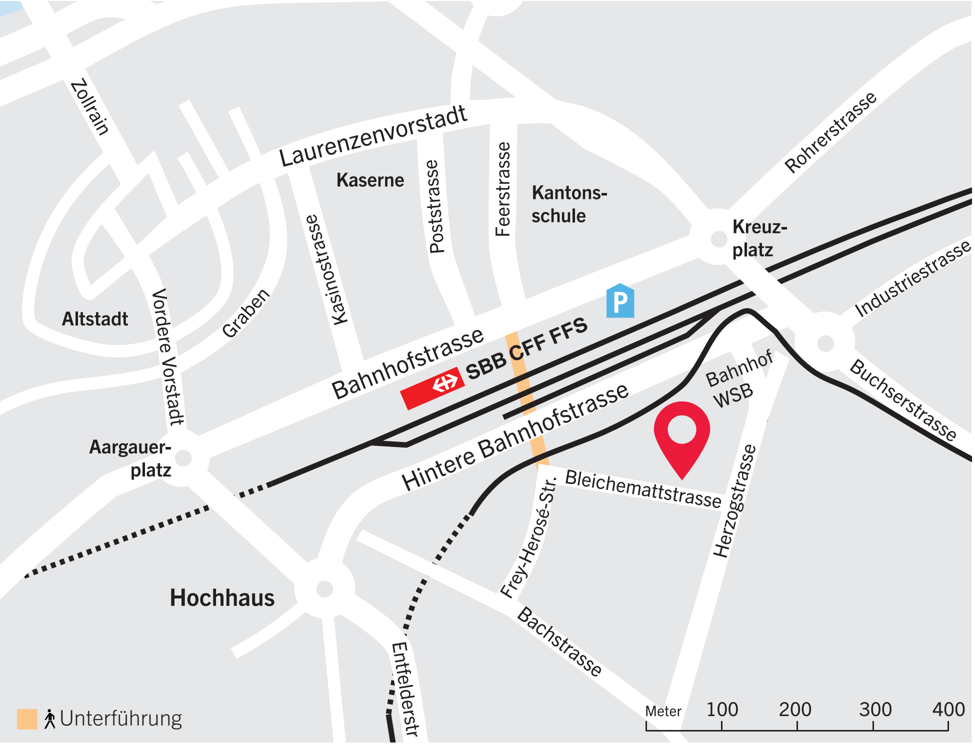
How to isolate hackers
Frank Pape, Axpo

Roundtables:

Roundtable 1:
Refining OT-IT and IoT Detection and Response: What are the options, who needs to decide, and what is the impact?

Roundtable 2:
OT SOC processes: Learning from real cases and Experience sharing: Which strategies lead to success, and what should be avoided?

Date:	**June 12, 2025**
Time:	**12:00-20:30 h**
Location:	**Bleichemattstrasse 31, 5001 Aarau**
Parking:	**Please use SBB Parking, handicaped: ask Bernhard for onsite parking**
ID:	**To be admitted to Swissgrid secure zone, you need an ID**



SWISS **OT-IT**
CYBER SECURITY
FORUM

15th Swiss OT-IT Cyber Security Forum
June 12, 2025 12:00-17:30 h
Social activity and dinner end at 20:30h

Agenda

In-Person Meeting: Swisgrid, Bleichemattstrasse 31, 5001 Aarau

Online Table will be offered, and online streaming of presentations (good online quality)

12:00	Lunch at Roche Diagnostics international
12:45	Networking among participants
13:10	Welcome note by Michael Knuchel, Swissgrid and Prof. Bernhard Hämmerli
13:30	**Watch, Wait, or Shut It Down? Tough Calls in OT/IoT Incident Response** Mark Barwinski, Global Security Executive
14:10	Roundtable 1: **Refining OT-IT and IoT Detection and Response: What are the options, who needs to decide, and what is the impact?**
15:00	Exchange between groups
15:15	Break
15:45	**Prepare to react. How to evaluate options and identify stakeholders with a framework?** Samuel Jassim, Security Operations Specialist, TEMET AG **No access – no damage: How air-gapped Security Zones create ineffectiveness of Hacker's effort.** Frank Pape, Senior Asset Manager, Axpo Grid AG
16:25	Roundtable 2: **OT SOC processes: Learning from real cases and experience sharing: Which strategies lead to success, and what should be avoided?**
17:10	Exchange between groups
17:25	Wrap-up and information on next meeting
17:30	Social Activity at Swissgrid: Swissgrid Insights: Organisation and Operation, Net 2040 Strategy, visit SGC (Swiss Grid Control).
18:45	Invited Dinner **Restaurant Mürset**, Schachen, 18, 5000 Aarau (13 min walking to train station Aarau).
20:30	End of the meeting

Swiss OT-IT Cyber Security Forum 16

Tentative – to be verified by votes: Auditing OT-systems: Which are the options for audit and its processes, and how to report for creating the best response?

Audit and security testing offers many different options: but which option is the best for a specific situation? Therefore, it is important to get an overview from bug bounty, red teaming, penetration test to more compliance-oriented framework audits. The result must be communicated, but how? Is reporting the best option, or is risk communication better? We expect a vivid discussion and experience exchange on these issues.

Date:	Thursday, tentative September 11, 2025, 12:00-20:30h
Place:	Bern Area
Speakers:	TBD
Roundtable 1:	Understanding security testing and audit: What are the options, and what are the criteria to select a specific approach?
Roundtable 2:	Reporting, risk communication and other influence on decision makers: What are the best options to invoke the desired actions?

Swiss OT-IT Cyber Security Forum 17

Detailed Asset Management for Software and Hardware (SOBM): What is its security impact?

Asset Management is the very first step one must do, to experience its own risk profile. But is general asset management of devices and software packages sufficient: No: it needs more. We must know the components in hardware and software. The SSL attack demonstrated that just one component can be wrong. But this component might be implemented in 100 different applications. If a component-based asset management is done, we can easily replace in the known software the packages. If we have first to make asset management – the down time or theme being vulnerable is much longer.

Date:	Tentative: Thursday, March 5, 2026, 12:00-20:30h
Place:	Zurich Area
Speakers:	TBD
Roundtable 1:	Understanding asset management and the variety of approaches which exists today.
Roundtable 2:	Strategy, tools, methodology: Choice we have, and must finetuned and adopt to specific use cases in the corporation.

SWISS **OT-IT**
CYBER SECURITY
FORUM

Registration

Register by replying to the invitation email with all your details – or by filling out this form, scanning it in or taking a smartphone picture.
Send the completed form to: info@OT-IT-CyberSecurityForum.ch

□ Three consecutive forums for CHF 960.–
Forum 15 (12. 06, 2025), and Forum 16 (tentative 11.09.2025), Forum 17 (05.03.2026)

□ 15th OT-IT Cyber Security Forum, June 12, 2025 only, at the price of CHF 360.– .

□ Register for social activity 17:30-18:45

□ Register for the sponsored Dinner 19:00-20:30 at **Restaurant Mürset**, Schachen 18, 5000 Aarau (13 min walking to train station Aarau)

□ Online Attendance: I will attend online in Teams (the link will be sent to you on request)

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

Organisation ....

Job Title ....

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

Phone .... Cellphone ....

Email ....

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

....

....

....