SWISS **OT-IT CYBER SECURITY** FORUM


# Outsourcing detection and response: **Identifying key issues for constructing successful partnerships**

**6th Forum, June 21, 2022, 12:00-20:00**
**In-Person, Kernkraftwerk Leibstadt**

SWISS OT-IT CYBER SECURITY FORUM

# Mission

## Why should you attend?

The Swiss OT-IT Cyber Security Forum is a series 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 German, French, and English 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

SPONSORS

ALSEC protect critical infrastructure

KPMG

HSLU Hochschule Luzern

axians

Monti Stampa Furrer

PARTNER

satw it's all about technology

SWISS OT-IT CYBER SECURITY FORUM

# Outsourcing detection and response: **Identifying key issues for constructing successful partnerships**

Cybersecurity itself is already quite challenging, but when it comes to detection and response, the complexity is increasing by far: Plenty of very special knowledge must be available for different tiers in analysis (detection) and response (the coordinated reaction between external provider and internal operations and management). The services an enterprise needs for the detect and response functions as well as the processes between external partner and the company play a crucial role on effectiveness and performance.

In this context, we will discuss key issues and share experiences of outsourcing detection and response with the goal to have a clear view on people, process, and technology. The following questions are relevant:

- Which part of detection and response will always stay with your company?
- By when to approach an outsourcing partner, and how to select specific services needed?
- Which changes do you need in organization, technology, processes?

Keynotes:

**SOC partnership from a client view: Opportunities, pitfalls, and recommendation for success**
Daniel Schirato, IT/OT Security Officer, Axpo

**The diversity of outsourcing detection and response services: How to identify quality, right settings, and expectations?** Olivier Spielmann, Vice President, Global Managed Detection and Response, Kudelski Security

Roundtables:

Roundtable 1
**Identify services, processes, and exercises to prepare a perfect integration into incident and crises management setup?**

Roundtable 2
**How to assess (potential) partners, and identify essential criteria for success?**

**Date: June 21, 2022**
**Time: 12:00 h - 20:00 h Place:**
**Kernkraftwerk Leibstadt (KKL),**
**directions will be communicated to registered participants.**

SWISS **OT-IT CYBER SECURITY** FORUM

**6th Swiss OT-IT Cyber Security Forum**

**June 21, 12.00 – 17:30**
**respective with visiting tour and dinner 20:00h**

# Agenda

**In-Person Meeting Kernkraftwerk Leibstadt**
on participants special request, online attendance may be made possible

| | |
|---|---|
| 12:00 | Lunch |
| 12:45: | Networking amongst participants |
| 13:15 | Welcome note by Kudelski Security and Prof. Bernhard Hämmerli |
| 13:30 | **SOC partnership from a client view: Opportunities, pitfalls, and recommendation for success**<br>Daniel Schirato, IT/OT Security Officer, Axpo |
| 14:00 | Roundtable 1:<br>**Identify services, processes, and exercises to prepare a perfect integration into incident and crises management. How to successfully set them up?** |
| 14:55 | Exchange between groups |
| 15:10 | Break |
| 15:40 | **The diversity of outsourcing detection and response services: How to identify quality, right settings, and expectations?**<br>Olivier Spielmann, Vice President, Global Managed Detection and Response, Kudelski Security |
| 16:10 | RoundTable 2:<br>**How to assess (potential) partners, and identify essential criteria for success?** |
| 17:05 | Exchange between groups |
| 17:20 | Warp up and information on next meeting |
| 17:30 | Visiting Tour Nuclear Power Station Leibstadt |
| 19:00 | Apéro riche |
| 20:00 | End of Meeting |

SWISS OT-IT CYBER SECURITY FORUM

# Swiss OT-IT Cyber Security Forum 7

Securing networks with old and non-patchable devices or other insecure black boxes: Strategies, concepts, and implementation in context of critical infrastructure like e. g. hospitals and energy providers.

Core topic: Insecure devices need micro segmentation as narrow as the functionality allows. In addition, the analysis and monitoring of networks streams should be another line of defense: automated search for unusual behavior and anomalies with advanced machine learning and artificial intelligence method may disclose otherwise hidden activities.

| | |
|---|---|
| Date: | Tuesday, September 13, 2022, 12:00-20:00h |
| Place: | Die Mobiliar, Bundesgasse 35, 3001 Berne |
| Speakers: | TBA |
| Roundtable 1: | Challenges with legacy devices: Discussing the scenarios and sharing experience |
| Roundtable 2: | Discussing latest and future solutions: What must happen, that the security can be fostered, which technologies help, and what corporate and community activities must be started(?)/induced? |

# Swiss OT-IT Cyber Security Forum 8

Improving OT security: Architecture, zoning, secure identity (IAM), privileged access (PAM), secured remote access (RAS), and other measures.

OT security personnel is challenged by rapidly increasing internet connections of OT installations. Core topic: Which measures are quick wins, and/or easy to install? Which measures are to most effective ones? And in this debate, we will focus on all options, including personnel and organizational issues. As the takeaway we want to elaborate a large variety of options, with examples of proven approaches.

| | |
|---|---|
| Date: | Thursday, March 02, 2023, 12:00-20:30h |
| Place: | Hitachi Energy Baden |
| Speakers: | TBA |
| Roundtable 1: | Organizational measures: How technology is enabled to its full security power? |
| Roundtable 2: | Technology for better security: A debate on options and performance of measures? |

SWISS **OT-IT CYBER SECURITY** FORUM

# Registration

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

Online participation will be available on your special request to the organizer.

☐ Three consecutive forums for CHF 960.–
Forum 6 (16.06.2022), Forum 7 (13.09.2022), and Forum 8 (02.03.2022)

☐ 6th OT-IT Cyber Security Forum, June 21, 2022 for CHF 360.– (single event)

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

Organisation .....

Job Title .....

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

Phone ..... Cellphone .....

Email .....

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

.....

.....

.....