



# United Crisis Management OT-IT:

How to benefit from better  
and well-tuned collaboration?

# 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 communities had completely different set-ups:

- IT used to follow the speed of technology evolution, 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 communities 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](mailto: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



## SPONSORS



# United Crisis Management OT-IT

## How to benefit from better and well-tuned collaboration?

Traditionally, IT has its way how to deal with crises, and OT has also its own way to deal with crises. In earlier times there has been very little interaction between those two incident handling entities. With the rapid growth of the internet, the integration of business processes and control systems, and the connection of many OT devices, potential incidents may concern both organizations, and the collaboration between them makes the big difference for success when facing such crises. This event will give examples, debate the topic, and provide insights on:

- How the interaction between OT and IT crises management can be improved.
- How the crises collaboration of OT and IT can be assessed and tested with exercises.
- What are typical learnings to be drawn from such exercises?

---

Keynotes:

**Domestic Robotik (Domotik): what it means to bring the OT and IT network on a single protocol together**

Roland Ebnöther and Mark Vadalà, Domotik in Swiss Defense Department

**Tabletop exercise on united OT-IT cyber crises management: what is the setup, how to bring the two communities together, and which findings will result.**

Nicolas Tinguely KPMG and Ivo Maritz MSFPartners

**Third party risks: Mitigations, Detections, and Investigations**

David Cowen, Managing Director KPMG US, SANS trainer, and Blackhat & RSA speaker

In two discussion rounds the topics are controversially reflected and options will be discussed:

Roundtable 1:

**United Crises Management OT-IT: What are advantages and draw backs of joint incident response training/exercises, and how to close the OT-IT gap?**

Roundtable 2:

**Third party risks: How to detect, mitigate and improve the general situation?**

---

**Date:** September 23, 2021

**Time:** 12:00 h - 20:30 h

**Place:** ABB Baden, Information will follow, depending on Covid situation

**Online:** Online option for those who can not attend in person

# Agenda

- 12:00 Offered Lunch, if Corona allows for: in person meeting.
- 
- 12:45 Opening of Webex for testing of online participants.
- 
- 13:00 Onboarding participants.
- 
- 13:15 Welcome notes, by Kudelski Security and Prof. Hämmerli
- 
- 13:30 **Domestic Robotik (Domotik): what it means to bring the OT and IT network on a single protocol together**  
Roland Ebnöther and Mark Vadalà, Domotik in Swiss Defense Department
- 
- 14:00 **Tabletop exercise on united OT-IT cyber crises management: what is the setup, how to bring the two communities together, and which findings will result.**  
Nicolas Tinguely KPMG and Ivo Maritz MSFPartners
- 
- 14:20 Roundtable 1:  
**United Crises Management OT-IT: What are advantages and draw backs of joint incident response training/exercises, and how to close the OT-IT gap?**
- 
- 15:10 Sharing results
- 
- 15:25 Break
- 
- 15:50 **Third party risks: Mitigations, Detections, and Investigations**  
David Cowen, Managing Director KPMG US, SANS trainer and Blackhat & RSA speaker
- 
- 16:20 Roundtable 2:  
**Third party risks: How to detect, mitigate and improve the general situation?**
- 
- 17:00 Sharing results
- 
- 17:15 Wrap up
- 
- 17:30 Apéro, social activity in Baden and offered dinner, if online: End of Forum 2
- 
- 20:00 End of meeting.
-

# Swiss OT-IT Cyber Security Forum 5

Next generation OT-IT architecture: Impact of IPv6, 5G and LPWAN on industrial applications.

Core topic: Cyber space is continuously developing, and we face three protocols: LPWAN (Low-Power Wide-Area Network) such as LoRa (Long Range Wide-Area Protocol, for low data rates in widely distributed environments), 5G (next generation cell phone protocol, which is much faster, can handle nearly unlimited numbers of nodes and has extremely low delays) and IPv6 the new internet protocol. What do we need to prepare, to ensure companies get best value and usage of these technologies while keeping security at a high level?

Date: March 03, 2022, 12:00-20:30h

Place: Axpo Kernkraftwerk Leibstadt, request pending

Speakers: TBA

Roundtable 1: What are the new OT business cases, how to take advantage of, and how to prepare strategically for security?

---

# Swiss OT-IT Cyber Security Forum 6

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

Core topic: For most enterprises the necessary knowledge for detection and response is far beyond of the own capacity as well as 24h by 7day service beyond any economic reality. Therefore, it is about to find the right partner, and to tune the organization to each other for best benefit. In addition, the options to identify and improve difficulties in the relationship with your outsourcing partner will be discussed.

Date: June 16, 2022, 12:00-20:30h

Place: TBA

Speakers: TBA

Roundtable 1: Outsourcing detection and response: What must be done in preparation and evaluation phase, and how to reach the critical maturity for well-functioning?

Roundtable 2: Finetuning operation: What are key issues, and how to continuously assess common operation?

# Registration

Register by replying to the invitation email with all your details – or by filling out this form and sending through a scan or alternatively through a smartphone picture. Send this completed form to: [info@OT-IT-CyberSecurityForum.ch](mailto:info@OT-IT-CyberSecurityForum.ch)

.....

Three consecutive forums for CHF 960.–  
3 Forums: Forum 4 (23.09.2021), Forum 5 (03.03.2022), and Forum 6 (16.06.2022)

4<sup>th</sup> OT-IT Cyber Security Forum, September 23, 2021 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.:

.....

.....

.....