

31.01.2018 - ISH Research & Strategy



08:00 Registration/Light breakfast

10:00 Official opening by representatives of the management of Flughafen München GmbH as well as representatives of politics and business

10:40 Break

11:00 Cyber Security Range Live Demonstration

The speaker demonstrates live on the systems of the CSR how a training within the CSR feels like and which skills get imparted to the prospective analyst. Typical threats against the infrastructure will be triggered, detected and processed by security analysts within their SOC tasks and transferred into the Incident Process.

iT-CUBE Systems AG

11:30 Representatives of European and international institutions

12:30 Lunch

13:30 Five Defensive Measures to Improve the Cyber Security of European Air Traffic Management

There is a growing realisation that state-sponsored agencies around the globe are developing offensive cyber security (OC) techniques – this is justified as a deterrent given that well-known vulnerabilities affect most, if not all, national critical infrastructures. In this talk we will consider the implications of the new arms race for defensive cyber security (DC). In particular, we will describe the Dubai Paradox that arises when the technical capability of offensive cyber security outstrips the development of appropriate policy on how to deploy these weapons, while in defensive cyber security there is a mass of policy and guidance but huge gaps in the detailed technical capability that would, for example, be needed to protect Europe's airport infrastructure.

Prof. Chris Johnson, Glasgow University

14:30 OT&IT Roadmap: Joint approach for Information Security

New communication technologies enable networks of complex, distributed systems (IoT). However, these technologies not only affect "classic" IT components but also increasingly include sensors of machines and building control systems (Industry 4.0).

This results not only in a large number of opportunities but also in new risks, e.g. for safety issues, especially for critical infrastructures (CRITIS) such as airports.

Munich Airport manages to combine the two areas of IT and OT in a particularly outstanding way, thus ensuring an optimal balance between new business areas and maintenance models as well as an efficient and robust security architecture via a common IT platform (Airport 4.0)

Michael Zaddach, CIO Münchener Flughafen GmbH/ Elke Eckstein, Münchener Flughafen GmbH

15:00 Break

15:30 Fit for Cyber Security- Sustainable Security Awareness

In this talk we will cover the psychological aspect of security awareness: changing behavior.

Topics to be covered are the fundamental pillars of successful behavior change such as the top down approach, central knowledge pool, creating a community, and Best Practices.

Frank von Stetten, HvS-Consulting

16:30 Potential Open Talk slot or additional Cyber Security Range Live Demonstration

17:30 Closing Procedure

17:45 "Aviation After Hours"



01.02.2018 - ISH Tech Track



08:00 Registration/Light breakfast

09:00 Second Day Keynote- Enno Rey

10:00 Break

11:00 CRITIS and IoT Environments - Challenges in the requirements, SDLC and PLC on long term live products

CRITIS and IoT Environments are rapidly changing our way of life - and the way our development processes are implemented. We have to deal with new and old systems in the same environment, how to handle the Secure Development Life Cycle (SDLC) and also the Product Life Cycle (PLC) for long term live products and systems. Such products are designed for a long life period (physically) but often not meet any IT Security requirements needed in KRITIS environments - e.g. like vulnerability and patch management - for system live times up to 20 years and even much more.

Currently a lot of Industrial Control Systems (ICS) and IoT devices are low hanging fruits for many attacks. The challenge will be to implement security and even safety into the SDLC and PLC for CRITIS and also ICS systems and applications. IT Security and Information Security Management is a mandatory part for CRITIS systems and applications.

This talk indicates problems we need to address in development of applications and systems for CRITIS environments to make them secure against common hacking attacks - and full fill law regulations and long life time. It is necessary to evaluate the applicability of the SDLC and PDL for rapid prototyping and long term life time and the disposal or reuse of such systems. This talk will introduce potential methodologies and tools to achieve this.

Christopher Scheuring, ERNW GmbH

11:30 Cyber Security Range Live Demonstration

12:00 Lunch



01.02.2018 - ISH Tech Track



13:00 Cyber Simulation Training – Technology & Background

The referent explains the technological base of the Cyber Simulation Range and gives a first insight into the upcoming analyst trainings.

Andreas Günther, iT-CUBE SYSTEMS AG

13:30 ISMS in critical infrastructure organizations

In this talk attendees will understand the challenges of an information security management system based on ISO 270xx and EN 16495 / TC377.

Topics to be covered are core elements like scoping, Organization of information security, Leadership and management commitment, Information security risk management and Information security policies and processes.

Attendees will also learn Best Practices for implementation of an ISMS for aviation organizations.

Michael Hochenrieder, HvS-Consulting

14:30 Break

15:00 Opportunities and Challenges of setting up a SOC

You will get to know about opportunities and challenges of setting up a Security Operation Center. Plus you will get an insight into current Best Practices, which you should regard while launching and establishing a SOC. After this lecture you know everything about implementing this complex endeavor.

Andreas Mertz, Founder & CEO of iT-CUBE SYSTEMS AG

16:00 Potential Open slot or early closing

17:00 Closing Procedure

