FUTURE FORCES FORUM
International Platform for Trends & Technologies in Defence & Security
www.future-forces-forum.org

International Security Conference

SCADA SECURITY

Organized as a part of FUTURE FORCES FORUM

12 – 13 October 2017

Hotel DAP, Prague, Czech Republic

FUTURE FORCES FORUM

General R&D Partner of Future Forces Forum

CZECH TECHNICAL UNIVERSITY IN PRAGUE

General Partner of Future Forces Forum

LOM PRAHA

Partner of Future Forces Forum

VOP CZ

Conference General Partner

FORTINET

Conference Main Partner

CYBERGYM® EUROPE

Conference Partners

KASPERSKY lab · ABB · Flowmon · GREYCORTEX · VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ · TREND MICRO · paloalto · Bohemia Market cz

TableTop Conference Partners

era bhc · CORPUS SOLUTIONS · VUMS DataCom

Executive programme guarantor

European Cyber Security Excellence Center

Conference topic guarantors

CZECH TECHNICAL UNIVERSITY IN PRAGUE · AFCEA · ČIMIB · ZEPSR · ictunie

Vážení účastníci konference SCADA Security,

s potěšením a úctou mohu poděkovat všem partnerům, především společnostem Fortinet a CyberGym Europe, členům přípravného výboru a odborným garantům, že se podařilo zorganizovat další atraktivní konferenci v rámci mezinárodního projektu Future Forces Forum také pro oblast bezpečnosti průmyslových řídicích systémů.

Projekt FFF je souborem komplementárních aktivit, které mají za cíl podpořit konkurenceschopnost a obchodní potenciál českého průmyslu a výsledků vědy a výzkumu na domácím i zahraničním trhu. Tyto aktivity probíhají kontinuálně a vrcholí vždy ve dvouletém cyklu sérií samostatných odborných akcí (B2B, B2G, G2G) s různou tématikou spolu se statickými a dynamickými ukázkami na jednom místě, tradičně již na PVA EXPO PRAHA.

V portfoliu akcí FFF má konference SCADA dlouhodobé ambice řešit aktuální i budoucí hrozby, postihovat trendy a určovat správný směr vývoje ve své oblasti.
V době tzv. hybridních válek se právě úspěšná kybernetická obrana stává významným prvkem celkové bezpečnosti nejen průmyslu.

Věřím, že dvoudenní říjnová konference a setkání vás - odborníků v hotelu DAP v Praze přinese všem jeho účastníkům mnoho nových poznatků a cenných kontaktů, obchodních příležitostí i celkového profesního obohacení v příjemné pracovní atmosféře.

Za tým SCADA Security konference a celého projektu FFF

Daniel Kočí
generální ředitel

Dear participants of the SCADA Security Conference,

I am very pleased and honored, that I can say thank you to all partners, especially to the companies Fortinet and CyberGym Europe, members of the program committee and professional guarantors, that we managed to organize another attractive conference in the framework of the international project Future Forces Forum, also for the safety industrial control systems.

Project FFF is a set of complementary activities that aim to support the competitiveness and business potential of the Czech industry and the results of science and research on the domestic and also foreign market. These activities takes a place continuously and culminates always in the two-year cycle of a series of separated professional expert events (B2B, B2G, G2G), with different topics, along with static and dynamic demonstrations in one place, traditionally at the PVA EXPO PRAHA.

In the portfolio of FFF events, SCADA conference has long-term ambitions to solve current and future threats, affect trends and determine the correct direction of development in the area.
At the time of so-called hybrid wars, a successful cyber defence is becoming an important element of the overall security, not just for the industry.

I believe, that two-day October conference and meeting of you - the experts in the hotel DAP in Prague, will bring a lot of new insights, valuable contacts, business opportunities and overall professional enrichment to all participants in an enjoyable work atmosphere.

On behalf of SCADA Security team and the whole project FFF

Daniel Kočí
Managing Director

CYBERGYM® EUROPE

SCADA ENABLED!

KYBERNETICKÝ SVĚT SE STAL NOVODOBÝM BOJIŠTĚM

JEDINEČNÝ PŘÍSTUP CYBERGYM EUROPE

UCELENÝ TRÉNINKOVÝ PROGRAM KYBERNETICKÉ OBRANY A OCHRANY

TÝMOVÉ VÝCVIKY POSTAVENÉ NA MÍRU V TRÉNINKOVÉ ARÉNĚ

V jedinečné tréninkové aréně poskytujeme výcvik v kybernetické obraně a ochraně – postavený na vzájemné interakci týmů s důrazem na lidský faktor a týmový výkon. Ucelený vzdělávací program následně promítáme do konzultační práce s klienty pro efektivní využívání bezpečnostních technologií a procesů v praxi. Jsme držitelem bezpečnostní prověrky NBÚ a postupujeme podle ISO standardů.

THE CYBER-WORLD HAS BECOME TODAY'S BATTLEFIELD

UNIQUE APPROACH BY CYBERGYM EUROPE

COMPREHENSIVE CYBER DEFENSE AND SECURITY TRAINING PROGRAM

TAILOR-MADE TEAM TRAINING IN OUR TRAINING ARENA

Unique training arena providing skills in cyber defense and security - based on team interaction with emphasis on human factor. The comprehensive training program is followed by engaging clients in efficient usage of security technologies and processes. Holder of security clearance and follower of ISO standards.

www.cybergymeurope.com

Vážení,

je mojí milou povinností uvést první ročník mezinárodní SCADA Security konference, který se koná v Praze ve dnech 12. a 13. října 2017 v hotelu DAP. Dovolte mi, abych úvodem poděkoval všem organizátorům a partnerům akce za vzornou odbornou přípravu a propagaci této konference. Zejména díky jejich úsilí se podařilo získat zajímavé řečníky, kteří jsou vynikajícími mezinárodními odborníky ve svém oboru a mohou se tak podělit s auditoriem o své bohaté zkušenosti.

Zvláště bych chtěl na tomto místě poděkovat zahraničním návštěvníkům této konference, kteří váží cestu, aby se stali součástí této akce. Je to pro nás důkazem, že bezpečnost SCADA systémů je opravdu vážným problémem.

Jak již z názvu konference vyplývá, nosným tématem celé konference je kybernetická bezpečnost průmyslových řídicích systémů. Bohužel, tato oblast se stala v poslední době zájmem útočníků. Jejich motivace jsou spojeny v tom lepším případě s cílem získat citlivé informace o výrobních postupech či patentech. Horším případem je jiná forma konkurenčního boje, kde je veden kybernetický útok přímo na prostředí průmyslových řídicích systémů. Dopady těchto útoků jsou viditelné na výrobních systémech. Jsou spojené se změnou výrobních receptur a tím i s porušením kvality výrobků, případně poškozením nebo úplným odstavením výrobní kapacity. Nejhorší je však situace u těch průmyslových podniků, kde případné dopady kybernetických útoků na výrobní systémy znamenají následné dopady na společnost – ekologickou katastrofu, ztráty na životech či celospolečenský chaos. Za útoky tohoto typu již mohou stát jiné státy, vlády a jejich armády. Tato forma napadení je typickým příkladem zneužití kybernetického prostoru jako bojového nástroje.

Lze očekávat, že množství útoků spojených s konkurenčním soubojem a se zneužitím kybernetického prostoru jako bojového nástroje se bude v nejbližší budoucnosti dramaticky zvyšovat. Dnešní relativně malé zastoupení těchto útoků je dáno faktem, že svět průmyslových systémů byl donedávna velmi uzavřený a pro hackerskou komunitu poměrně nedostupný. To se však mění tím, jak se kybernetičtí útočníci profesionalizují. Zároveň se zranitelnosti těchto systémů dostávají do obecného povědomí a objevuje se stále více relativně snadno dostupných útočných scénářů na průmyslová zařízení. Toto povede v nejbližší době ke zvyšování počtu útoků s razantními dopady na potencionální oběti.

Všechny tyto skutečnosti nás přiměly k tomu, že jsme se rozhodli uspořádat tuto výjimečnou mezinárodní konferenci. Našim cílem je demonstrovat rizika těchto systémů a současně ukázat auditoriu cestu k jejich řešení. V rámci konference proto zazní nejnovější trendy a poznatky v této rychle se rozvíjející oblasti, pozornost bude věnována i lidskému faktoru, který vždy byl a stále zůstává největší slabinou u mnoha společností.

Závěrem mi dovolte vyjádřit přesvědčení, že díky atraktivitě tématu a velmi dynamickému vývoji trhu v této oblasti, nezůstane pouze u tohoto prvního ročníku konference. Přeji proto všem, kteří stáli u zrodu této akce, účastníkům, řečníkům a partnerům, aby se tento ročník maximálně vydařil a abychom se již nyní všichni mohli těšit na druhý ročník, který se bude konat v příštím roce.

S přáním příjemně stráveného času v průběhu konference

Tomáš Přibyl
předseda sdružení EuCybSec

Dear ladies and gentlemen,

It is my pleasant duty to introduce the first year of the international SCADA Security conference which takes place in Prague in hotel DAP on 12th and 13th October. At first let me thank to all organizers and partners of the event for exemplary preparation and propagation of this conference. Especially thanks to their endeavor we managed to get interesting speakers who are excellent international experts in their field and they can share their experience with the audience.

On this place I would like to thank to the foreign visitors of this conference who traveled here to be a part of this event. It is a proof for us that the security of SCADA systems is a serious problem.

How the name of the conference suggests, the key topic of the whole conference is cyber security of the industrial controlling systems. Unfortunately, this area became a target of attackers. Their motives are connected, in a better scenario, with the goal to obtain sensitive information about production processes or the patents. In the worse scenario it is a different form of a competitive fight where the cyber attack is led precisely on the environment of the industrial controlling systems. The impacts of these attacks are visible on the production. They are connected with the change of the production procedures and by that with the violation of the quality of the products or damaging or completely stopping of the production capacity. The worst is the situation in those industrial businesses where the potential impacts of the cyber attacks on the production systems cause impacts on the society – ecological disaster, casualties on life or chaos through the whole society.

It can be expected that the number of the attacks connected with the competitive fight and with the misuse of the cyber space as a tool for fighting will rise drastically in the near future. Contemporary relatively small number of these attacks is given by a fact that the world of industrial systems was mostly closed until recently and for the hacker community was relatively unavailable. However, this changes by how the cyber attackers professionalize. At the same time the vulnerability of these systems get into the general awareness and more relatively easily available attack scenarios on the industrial facilities appear. This will lead towards the increase of the number of the attacks with the strong impacts on the potential victims in the near future.

All these facts forced us that we decided to organize this exceptional international conference. Our goal is to demonstrate risks of these systems and at the same time to show to the audience the way to the solution. The newest trends and knowledge in this fast developing field will be heard throughout the conference. The attention will be focused on the human factor which has always been and still remains the biggest weakness in many companies.

In the conclusion let me express the believe that thanks to the attractive topic and very dynamic development of the market in this field, we will not stay only with the first year of the conference. Because of this I wish to all who stood at the beginning of this event, participants, speakers, and partners that this year will be maximally successful and we could look forward to the second year which will take place next year.

With the wish of pleasant time during the conference,

Tomáš Přibyl
chairman of the association EuCybSec

Kaspersky Industrial Cybersecurity

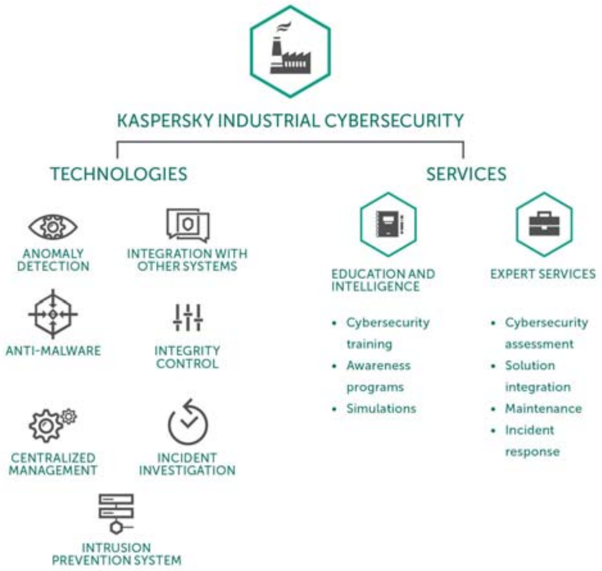
Specialized protection for industrial control systems

Although air gaps between industrial floors and the outside world used to be sufficient to offer a good level of protection, that's no longer the case. Recent research has found that cyber-attacks cause 35% of industrial network malfunction incidents.

Malicious attacks on industrial environments have increased significantly in recent years. Risk to supply chains and interruptions to business operations have ranked as the number one business risk concern globally for the past three years; cyber-incident risk is the number one emerging concern. For businesses operating industrial or critical infrastructure systems, the risks have never been greater.

Industrial security has consequences that reach far beyond business and reputational protection. In many instances, there are significant ecological, social and macro-economic considerations when it comes to protecting industrial systems from cyber threats. Every critical infrastructure needs the highest possible levels of protection against a growing range of threats.

At the same time, industrial environments need an integrated solution that maintains the availability of technological processes by detecting and preventing actions (intentional or accidental) that could disrupt or halt vital services.



The solution: Kaspersky Industrial Cybersecurity

Kaspersky Industrial Cybersecurity is a portfolio of technologies and services designed to secure every industrial layer, including SCADA servers, HMI panels, engineering workstations, PLCs, network connections and people – without impacting on operational continuity and the consistency of the technological process. Flexible, versatile settings mean the solution can be configured to meet the unique needs and requirements of individual industrial facilities.

The solution has been developed to protect critical infrastructures, built on a number of different industrial control systems. The flexibility and scope of Kaspersky Industrial Cybersecurity allow organizations to configure their solution in strict accordance with the requirements of their specific ICS environment. The optimal configuration of security technologies and services is established through a full infrastructure audit carried out by Kaspersky Lab experts.

Kaspersky Lab's approach to protecting industrial systems is based on more than a decade's expertise in discovering and analyzing some of the world's most sophisticated industrial threats. Our deep knowledge and understanding of the nature of system vulnerabilities, coupled with our close collaboration with the world's leading law enforcement, government and industrial agencies, including Interpol, Industrial Internet Consortium, various ICS vendors and regulators has enabled us to take a leadership role in addressing the unique requirements of industrial cybersecurity.

Conference Programme

12 OCTOBER 2017 Prague, Hotel DAP

Welcome Session – Recent & Future Cyber Threats

Moderator: **Mr. Petr JIRASEK**, Chairman Czech Cyber Security Working Group & Chairperson SCADA Security Working Group, Czech Republic

9:30 - 11:15

09:35 **Actual State of Cyber Security in the Czech Republic**;
Mr. Dušan NAVRÁTIL, Director, National Cyber and Information Security Agency, Czech Republic

10:00 **SCADA Systems as Target of Cyber Attacks**;
Mr. Ondřej ŠŤÁHLAVSKÝ, Regional Director, CEE, Fortinet, Czech Republic

10:20 **Legal liability of the entrepreneur in case of cyber-attacks;**
Mr. Václav SCHOVÁNEK, AKS Legal, Czech Republic

10:45 **The Concept and benefits of the Incident Response Team training in arena**;
Mr. Martin UHER, Vice president, CyberGym Europe, Czech Republic

11:05 **Q & A**

11:15 - 11:50 Coffee break

New Technological Trends in ICS Security

Moderator: **Mr. Igor TOMEŠ**, Board Member, ČIMIB, Czech Republic

11:50 - 13:25

11:55 **Manage cyber security over the life time of the control system**;
Mr. Frank HOHLBAUM, Cyber Security Product Manager, Grid Automation, ABB, Switzerland

12:15 **Using Machine Learning for Next Generation ICS Security**;
Mr. Mateusz FLAK, Cyber Security Regional Manager CEE, Darktrace/Auris, Great Britain

12:35 **Development of application software for CII in power engineering**;
Mr. Lukáš OBOŘIL, Head of Department for ICS SW, I & C Energo, a. s., Czech Republic

12:55 **Network traffic monitoring & analysis in SCADA Networks**;
Mr. Pavel MINAŘÍK, Chief Technology Officer, Flowmon Networks, Czech Republic

13:15 **Q & A**

13:25 - 14:10 Lunch break

Industrial Scada Security & Connected Cars

Moderator: **Mr. Jaroslav BURČÍK, Ph.D.,** Director, ITU Center, Czech Technical University, Czech Republic

14:10 - 15:55

14:15 **Live hacking show – internet of things**;
Mr. Tobias SCHRÖDEL, IT-Security expert, Expert on TV and the world's first Comedyhacker®, Germany

14:45 **Security Threats of Internet of Thing**s;
Assoc. Prof. Zdeněk LOKAJ, Ph.D., Expert on transport telematics, cooperative systems in road transport and safety at the Faculty of Transport CTU, Czech Republic

15:05 **Next-generation Industrial environment protection**;
Mr. Jakub JIŘÍČEK, CISSP, CNSE I Systems Engineer - Eastern Europe, Palo Alto Networks, Czech Republic

15:25 **Platform for fully autonomous vehicles**;
Dr. Václav KOBERA, Director, Department of Intelligent Transport Systems, Space Activities and Research, Development and Innovations, Ministry of Transportation, Czech Republic

15:45 **Q & A**

15:55 - 16:25 Coffee break

IT vs. OT & Cyber security as an investment to protect own business

Moderator: **Mr. Joao Annes**, Cybersecurity Board Member, AFCEA Portugal, Portugal

16:25 - 18:00

16:30 **Operational Technology (OT) cyber security IS NOT SAME AS Information Technology (IT) cyber security**,
Mr. Petr ROUPEC, CEO, Bohemia Market CZ, Czech Republic

16:50 **Protect Your SCADA Systems from Modern Cyber Attacks**;
Mr. Ondřej ŠŤÁHLAVSKÝ, Regional Director, CEE, Fortinet, Czech Republic

GRID AUTOMATION SERVICE

Enabling smarter system protection.

Cyber Security Care

17:20 **Human Factor to create a digital trustworthy environment for CII**;
Mr. Paolo MONIZ, Cyber Security Expert, EDP, Portugal
17:40 **Q & A**
17.50 **Closing Remarks**;
Mr. Tomáš PŘIBYL, Board chairperson, European Cyber Security Excellence Center, Czech Republic
18:00 - 18:15 First day conference closing
18:30 **SCADA PARTY** (by invitation only)

13 OCTOBER 2017 Prague, Hotel DAP

Second Day Opening

Opening speech and Moderator: **Mr. Tomáš PŘIBYL**, Board chairperson, European Cyber Security Excellence Center, Czech Republic
9:00 - 10:25
09:05 **Security in industrial Automation - friend or foe?**;
Mr. Udo SCHNEIDER, Security Evangelist, Trend Micro, Germany
09:30 **SCADA Security Framework?**;
Mrs. Paola ROCCO, Senior Consultant NTT Data Italia, Member AFCEA Rome Chapter, Italy
09:50 **Finding SCADA devices and what next**;
Mr. Ragnar RATTAS, Senior Cyber Security Expert, BHC Laboratory, Estonia
10:15 **Q & A**
10:25 - 11:05 Coffee break

Industrial Cyber Security - Industry 4.0

Moderator: **Assoc. Prof. Zdeněk LOKAJ**, Ph.D., Expert on transport telematics, cooperative systems in road transport and safety at the Faculty of Transport CTU, Czech Republic
11:05 - 12:50
11:10 **Industry 4.0 Concept**; Dr. Radek ŠINDELÁŘ, Researcher, Vienna University of Technology, Institute of Software Technology and Interactive Systems, Czech Republic
11:40 **Kaspersky Industrial Cyber Security**; Mr. Petr KUBOŠ, Regional Sales Manager CEE & Mr. Michal LUKÁŠ, Presales Engineer & Certified Trainer, Eastern Europe, Kaspersky Lab, Czech Republic
12:00 **New approaches to detection - Malware Industroyer**;
Mr. Michal DROZD, Chief Security Analyst, GreyCortex, s. r. o. & Mr. Radek Fujdiak, PhD., Researcher, Brno University of Technology, Faculty of Electrical Engineering, Czech Republic
12:20 **Wireless communication and security**;
Mr. Vladimír ŠULC, Ph.D., CEO, IQRF Tech, s. r. o., Czech Republic
12:40 **Q & A**

12:50 - 13:40 Lunch break

Cyber Security & Human Factor

Moderator: **Mr. Martin UHER**, Board Member, European Cyber Security Excellence Center, Czech Republic
13:40 - 15:30
13:45 **Haven't you forgotten something (or somebody);**
Mr. Karel MACEK, Head of Department, ICT Security Department, Ministry of Labour and Social Affairs, Czech Republic
14:05 **Building up needed skills for an effective corporate cyber defence**;
Mr. Tomáš PŘIBYL, Board chairperson, European Cyber Security Excellence Center, Czech Republic
14:25 **Legal liability of the entrepreneur in case of cyber-attacks**;
Mr. Tomáš NIELSEN, Partner, NIELSEN MEINL, Czech Republic
14:50 **Case study**
Mr. Luděk NOVÁK, Ph.D., Member Czech Cyber Security Working Group, Czech Republic
15:10 **Q & A**
15:20 **Closing Remarks**
Mr. Petr JIRASEK, Chairman Czech Cyber Security Working Group & Chairperson SCADA Security Working Group, Czech Republic
15:30 - 15:45 Conference closing

Challenges and Solutions in Securing Industrial Control Systems

Exclusive interview with Nick Feifer Regional Channel Manager in Central and Eastern Europe at Fortinet, the global leader in high-performance cybersecurity solutions, about securing Industrial Control Systems.

istockphoto.com /PhotoBylove

In recent years, the Industrial Control Systems (ICS) upon which much of our critical infrastructure and manufacturing industry depends have come under increasingly frequent and sophisticated cyber-attacks.

In part, this is a consequence of the inevitable convergence of Operational Technology (OT) with Information Technology (IT). As in all spheres of computing, the advantages of increased network connectivity through open standards such as Ethernet and TCP/IP, as well as the cost savings derived from replacing dedicated proprietary equipment with off-the-shelf hardware and software, come at the cost of increased vulnerability.

Do you think SCADA environments are secure?

Designed for longevity and at a time when cybercrime specifically targeting the industrial sector was not widespread, SCADA systems have not been taken into account within the network security scheme. Because of the isolated nature of industrial systems and the non-existence of interconnection to an IP network, security was not initially considered to be necessary.

However, SCADA architectures have evolved and now robots, measurements systems, command and control tools and remote maintenance systems are all interconnected via a conventional IP network. The problem is not the use of IP itself but rather that they are administered by potentially vulnerable environments, such as the HMI interface platform, which is typically equipped with an unpatched Windows operating system. Considered highly sensitive, these environments generally do not have operating system patches or updates applied for fear of disrupting the industrial system. Often, this fear prevails over the fear of potential IT attacks.

Identified as critical, SCADA environments are thus paradoxically less secure and become a potential target for cybercriminals.

What are the consequences of SCADA attacks for industrial companies?

Once compromised, a hacker would then have full control over the system.

While the impact of a security breach on most IT systems is limited to financial loss, attacks on Industrial Control Systems (ICS) have the added potential to destroy critical equipment, threaten national security, and even endanger human life.

How industrial companies deploying SCADA can improve their security?

Today some industrial companies started to integrate security measures into their systems. However, much more is needed before SCADA systems can be considered secure. As a first step, companies deploying SCADA must consider them as a part of their overall IT infrastructure, apply the same security measures and techniques that they do for their internal IT infrastructure and get the support from their senior executives for the related additional IT budgets and resources.

As a leader in cybersecurity solutions, what are your advices for securing such environments?

There are important steps that should be taken to ensure the security of SCADA environment, considered as sensitive:

- **Regular updates**: Applying software patches on a regular basis to the SCADA operation system, applications and components is an essential step to avoid security breaches due to vulnerabilities already known by security vendors.

In addition, the implementation of a tool for detection and analysis of vulnerabilities that allows to intercept malicious Internet threats before they impact the network or the target server will enable proactive measures to prevent attacks, avoid service interruptions, and respond quickly and in real-time against emerging threats.

- **Partition and isolate the SCADA network**: It is essential to isolate the SCADA network from any other corporate network. Thus, the HMI network will be separated from robots and measuring devices, supervisory systems, remote control units and communications infrastructures, allowing each environment to be confined and protected from bouncing attacks.

In short, SCADA networks need to be secured in the same way as enterprise networks from malware and intrusion, using Intrusion Prevention Systems (IPS) and anti-malware solutions, which are not just SCADA specific.

- **Segregate administrators from users**: In addition to the segmentation of the network, it is crucial to segregate users from administrators and provide different access levels between the two groups. For example, an administrator could have full access, including configuration changes via the HMI, whereas the user may have read-only access.

- **Get an overall view of the network**: The need for a correlation and event management tool is essential. It is critical that the network administrator has the ability to fully understand the security state of the entire network and for instance know at the same time the robot state, the HMI patch level and its relation to a specific user or component of the architecture.

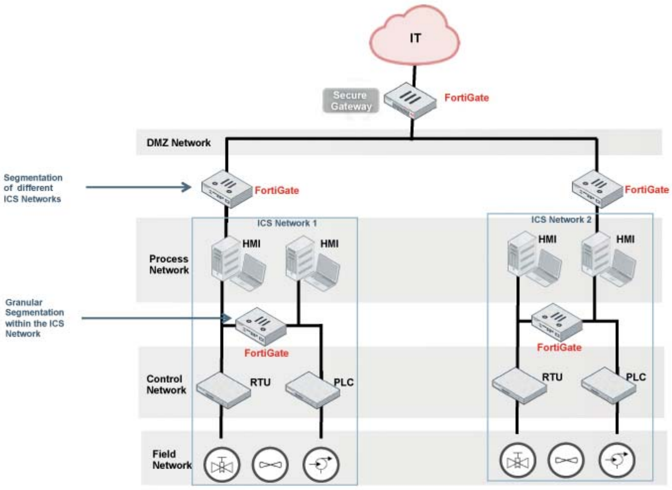
The generation of security alerts is equally important. By understanding what is happening in the network, the administrator gets the ability to correctly react to network events and take appropriate actions.

The implementation of these steps, although sometimes cumbersome, will ensure that there is a comprehensive security strategy throughout the network and provide an in-depth defense with a security layer at all levels, even at PLC units, for a precise control of exchanges and communications between the SCADA environment and the network infrastructure.

Does Fortinet offer such security?

Of course! Fortinet delivers an industry-specific, tightly integrated solution that combines the connectivity and security needed for distributed industrial control systems in form factors that are designed for the extreme environments in which they must be deployed.

The Fortinet Security Fabric provides an organization using ICS with an approach to address its unique security issues and requirements and implement consistent security anywhere in the network thus ensuring IT/OT convergence. How? First, by deploying a FortiGate in strategic locations in the network, each location and any Fortinet device attached to it, become secure. Expanding on this, because each FortiGate in these separate locations is running a common OS, FortiOS, the entire network environment (i.e. both the IT and OT network) behaves as a single entity from a policy and logging perspective reducing the risk from advanced threats for broad security coverage. Furthermore, as a powerful security platform, FortiGate can deliver comprehensive security while aligning to the bandwidth demands of the underlying network. In addition, with each FortiGate receiving security updates from our threat intelligence, FortiGuard, end-to-end, seamless security is maintained as elements can rapidly exchange threat intelligence and coordinate actions for an automated response to threats. Finally, when Fabric ready partners like Nozomi join the network, the Fortinet Security Fabric facilitates their integration making them part of the secure Eco System.



What are your key differentiators from the competition?

Since its creation, in 2000, Fortinet's technology has been developed fully in-house from Day 1 and the company has total control over the design of its products, making no compromises on quality, performance and reliability.

Technological innovation is at the heart of Fortinet to address the stringent security requirements of its customers. Our solutions are continuously enhanced with the latest technological innovations to remain at the forefront of the industry in terms of functionality and performance.

In addition, Fortinet is the only network security vendor, which has its own global threat research & response team continuously monitoring the threat landscape and providing customers with ongoing and real-time protection against the latest Internet threats. Our FortiGuards' expert team is composed of over 200 dedicated researchers analysts, engineers and forensic specialists located around the world to deliver security updates 24/7, with industry-leading response times to new and emerging threats targeting customers' networks, content and mobile devices.

■

TREND MICRO™

Trend Micro Midyear Report Highlights Need for Proactive Security

2017 Midyear Security review demonstrates importance of cybersecurity investments

Trend Micro, a global leader in cybersecurity solutions, today released its 2017 Midyear Security Roundup: The Cost of Compromise, detailing the threats from the first half of 2017, which continue to disrupt and challenge IT planning. Businesses are faced with increased ransomware, Business Email Compromise (BEC) scams and Internet of Things (IoT) attacks, and now also contend with the threat of cyberpropaganda.

Trend Micro detected more than 82 million ransomware threats in the first half of the year, along with more than 3,000 BEC attempts, reinforcing the need for security prioritization. Despite the rising percentage of security spending in IT budgets, a recent analyst report by Forrester[1] notes that funds are not properly being allocated to address the growing threats facing enterprises today.

"Enterprises need to prioritize funds for effective security upfront, as the cost of a breach is frequently more than a company's budget can sustain," said Max Cheng, chief information officer of Trend Micro. "Major cyberattacks against enterprises globally have continued to be a hot-button topic this year, and this trend is likely to continue through the remainder of 2017. It's integral to the continued success of organizations to stop thinking of digital security as merely protecting information, but instead as an investment in the company's future."

In April and June, the WannaCry and Petya ransomware attacks disrupted thousands of companies across multiple industries world-wide. The global losses from the attack, including the resultant reduction in productivity and cost of damage control, could amount to as much as US$4 billion. In addition, BEC scams raised the total of global losses to US$5.3 billion during the first half of 2017, according to the Federal Bureau of Investigation (FBI).

As predicted, January through June experienced a rise in IoT attacks, as well as the spread of cyberpropaganda. In collaboration with Politecnico di Milano (POLIMI), Trend Micro showed it is possible for industrial robots to be compromised, that could amount to massive financial damage and productivity loss, proving that smart factories can ill-afford to dismiss the importance of securing these connected devices. There was also an increased abuse of social media with the rise of cyberpropaganda.
Given the tools available in underground markets, the spread of Fake News, or bad publicity, will cause serious financial ramifications for businesses whose reputation and brand equity is damaged by cyberpropaganda.

Trend Micro XGen™ security provides proactive protection and guidance for companies facing these pressing and growing threats with a cross-generational approach to threat defense. The threats that have manifested throughout the beginning of 2017 are only a fraction of what is likely to come. Cybercriminals are getting smarter with their attacks every day and companies should be prepared by having the appropriate budgets and solutions in place.

[1] Jeff Pollard, Security Budgets 2017: Increases Help But Remain Reactionary, Benchmarks: The S&R Practice Playbook (Forrester, 2016).

Conference Programme Committee

Mr. **Petr JIRÁSEK**,
Member of International Cyber Committee, Czech Republic
Chairman

prof. **Boris ŠIMÁK**
Czech Technical University in Prague, Czech Republic
Honorary Chairman

Assoc. Prof. **Josef POŽÁR**
Vice dean for Study and development, Faculty of Security Management, Police Academy of the Czech Republic in Prague, Czech Republic
Honorary Chairman

Members

Mr. **J. Miguel ANNES**
Cybersecurity Board Member, AFCEA Portugal, Portugal

Col. (Ret.) **Miroslav BRVNIŠŤAN** (Ret.)
President,
AFCEA Slovak Chapter, Slovakia

Mr. **Jaroslav BURČÍK**
Czech Technical University in Prague, Czech Republic

Assoc. Prof. **Jaroslav DOČKAL**
Vice-rector for Science and creative activity,
Karel Englis College,
Czech Republic

Mr. **Tomáš HEJLÍK**
Member,
European Cyber Security Excellence Centre,
Czech Republic

Mr. **Andrej HRADŇANSKÝ**
Member,
European Cyber Security Excellence Centre,
Czech Republic

Mr. **Michal KOHÚT**
Member,
European Cyber Security Excellence Centre,
Czech Republic

Mr. **Zdeněk LOKAJ**
Member,
European Cyber Security Excellence Centre,
Czech Republic

Mr. **Peter LUKÁČ**
Specialist Counselor
Department of Security and Crisis Management, Czech Telecommunication Office, Czech Republic

Ing. Karel MACEK
Head, ICT Security Department,
Ministry of Labour and Social Affairs,
Czech Republic

Mr. **Tomáš MÜLLER**
President,
AFCEA Czech Chapter,
Czech Republic

Mr. **Vladimír ONDROVIČ**
President,
Slovak Association of Electrotechnical Industry,
Slovakia

Mr. **Radim OŠŤÁDAL**
Director of Government CERT,
National Cyber Security Center,
Czech Republic

Mr. **Josef PROKEŠ**
Director,
Administrative section,
The Office for Personal Data Protection, Czech Republic

Mr. **Tomáš PŘIBYL**
Chairperson
European Cyber Security Excellence Centre, Czech Republic

Mr. **Vladimír ROHEL**
National Agency for communication and information technology,
Czech Republic

MGen. (Ret.) **Erich STAUDACHER** GEAF,
General Manager,
AFCEA Europe, Germany

Mr. **Igor TOMEŠ**
Board Member, ČIMIB,
Czech Republic

CYBERGYM® EUROPE

HUMAN FACTOR

AN OVERLOOKED ASPECT IN CYBER SECURITY

The human factor plays a crucial role in defending against cyber-attacks: it can be the weakest or the strongest element of security. There is no product or product combination providing a security guarantee without a proper involvement of the human factor.

Cyber-defenders often rely too much on correct settings of security technologies and their ability to automatically detect a cyber-attack. If automated protection fails (practice show that it is failing quite often), untrained IT staff has a very limited ability to detect the attack and, as a consequence, no possibility to react. Moreover, the training of complex detection and reaction techniques is often impossible on production systems.

To ensure cyber security, it is not enough to rely solely on the implementation of security technologies, standards, regulations and similar compliance requirements – mainly due to the fact that they predominantly relate to known threats. Such standards do not recognize the cruciality of an alert, skilled and ready IT staff to detection an attack and react to it properly. Particularly, the human factor is extremely important when non-technical threats are involved, such as social engineering or physical security disruption.

It is necessary to realize that a modern cyber-attack comprises a whole chain of events, starting from gathering information about the victim, "groping" for security barriers, searching for vulnerabilities, up to a successful penetration. Still, the penetration is just a first step and, in most of cases, does not necessarily mean any impact on assets (such as destruction or deterioration), but rather a "foothold" for the attacker. Starting from the penetration point, he then tries to reach the asset. This nearly always means several further steps (such as lateral movement and escalation of privileges) before attacking the final target.

Already in the first phase (gathering information about the victim), detection is possible (for example, using honeypots), but most other phases the attacker's activity can be detected. Properly configured technology is a prerequisite, but the most crucial thing is the ability of humans to evaluate all the information that security technologies provide.

The next step is to use the capabilities of security staff to block the attacker's further movement. Without such human skills, detection capabilities are useless - merely allowing to trail the attacker's progress until the impact occurs. The key is the ability to conduct a dynamic defense.

The only way to prepare a security team is to let them experience such an attack in real time, to face it and to have the opportunity to test their reactions to it. This applies not only to the security team, but also to the entire decision-making hierarchy, including managers. Without having experienced such a situation, no one will ever be able to respond to it adequately.

Phishing or social engineering was the first and primary cause of approximately **30%** of successful cyber-attacks in 2016.

Uninformed, uninstructed and untrained employees and partners are involved in more than **50%** of security incidents.

Nearly **60%** of all targeted and sophisticated attacks involve a company insider.

The human factor affects **95%** of all cyber security incidents.

More than **90%** of targeted attacks rely on spear-phishing - a malware-based initiation vector distributed by email attachments.

More than **60%** of data leakage and theft incidents began with an attack on weak user passwords.

Conference Speakers

Mr. João Annes
Cybersecurity Board Member, AFCEA Portugal, Portugal
Moderator

IT vs. OT & Cyber security as an investment to protect own business

Mr. Jaroslav BURČÍK, Ph.D.
Director, ITU Center, Czech Technical University, Czech Republic
Moderator

Industrial Scada Security & Connected Cars

Jaroslav Burčík vystudoval mikroelektroniku na Fakultě elektrotechnické ČVUT v Praze (ČVUT). Později zde získal titul, Ph.D. v oboru telekomunikační technika. Od roku 2008 pracuje na různých vedoucích pozicích. Získal řadu zkušeností jako zakladatel a ředitel Centra pro spolupráci s průmyslem a následně Inovacentra - hlavním subjektem pro transfer technologií na ČVUT (2008 - 2015).

Má bohaté zkušenosti s mezinárodní spoluprací jak s podniky, tak i s neziskovými sektory. V současné době buduje na ČVUT centrum pro kybernetickou bezpečnost a motivuje studenty středních škol ke studiu inženýrských oborů.

Mr. Michal DROZD
Chief Security Analyst, GreyCortex, s. r. o.

New approaches to detection - Malware Industroyer

Michal Drozd is Chief Security Analyst at GREYCORTEX, the company behind the MENDEL network security solution. Michal, co-founder and co-owner of GREYCORTEX, currently oversees teams engaged in the analysis of advanced network security threats. Prior to his work with GREYCORTEX, he spent many years a university researcher and as an ethical hacker and security consultant at Czech company AEC, where he was able to repeatedly penetrate and improve the security of critical infrastructure and well-known financial institutions.

Mr. Mateusz FLAK
Cyber Security Regional Manager CEE, Darktrace/Auris, Great Britain

Using Machine Learning for Next Generation ICS Security

Sales manager with creative vision, business acumen and strong technical background. Experience in operations management, business process improvements and strategic IT projects implementation. Areas of strength include structured and strategic approach to Business and IT edge with proven records of costs optimisation, IT operations process improvements and building competitive advantage through IT technology. Responsible to establish business foundation for Darktrace in CEE region with building sales channel to contribute in revenue growth.

Mr. Radek Fujdiak, PhD.
Researcher, Brno University of Technology, Faculty of Electrical Engineering, Czech Republic

New approaches to detection - Malware Industroyer

Radek Fujdiak is a researcher at the Brno University of Technology (Czech Republic). He received his PhD degree in Communication Technologies at the Brno University of Technology in 2017. He is involved in the research group of prof. Jiri Misurec. His research activity is related to the cyber security, cryptography, in particular on low-power devices and Smart Technologies.

Mr. Frank HOHLBAUM
Cyber Security Product Manager, Grid Automation, ABB, Switzerland

Manage cyber security over the life time of the control system

Today I am a Product Manager for Cyber security within ABB Substation Automation, but I've spent 20 years at ABB working across R & D and Product Management within Substation Automation. I'm passionate about developing cyber security awareness and simple-to--understand processes and programs that ensure our customers have a smarter system protection.

ALL SYSTEMS GO

paloalto NETWORKS

Security for ICS and SCADA

> Ensure availability

> Safely enable applications and protocols

> Segment critical systems

> Protect unpatched systems

paloalto NETWORKS | TechData

ALL SYSTEMS GO

paloalto NETWORKS

What We Do

We deliver a complete security platform that addresses the ICS cybersecurity challenges to help keep uptime and safety high.

The core capabilities of our platform lending to this mission include:

> Unrivaled network traffic visibility via deep packet inspection of ICS protocols and applications as well as user and content threat info.

> Zero Trust network segmentation with role-based controls that support ICS-specific standards and regulations.

> Protection of vulnerable automation systems from known and zero-day threats via network AV/IPS, sandboxing and endpoint security.

paloalto NETWORKS | TechData

Mr. Petr JIRASEK

Chairman Czech Cyber Security Working Group & Chairperson SCADA Security Working Group, Czech Republic
Moderator

Welcome Session – Recent & Future Cyber Threats

Mr. Jakub JIŘÍČEK

CISSP, CNSE | Systems Engineer - Eastern Europe, Palo Alto Networks, Czech Republic

Next-generation Industrial environment protection

Již během studií na ČVUT FEL, obor Elektronické počítače, pracoval Jakub Jiříček v oboru informačních technologií. Zkušenosti nasbíral mj. ve společnostech Digital Equipment, Symantec a také při vlastním podnikání. Od roku 2002 se specializuje na oblast počítačové bezpečnosti. Ve společnosti Palo Alto Networks má na starosti technické pre-sales aktivity ve východní Evropě.

Dr. Václav KOBERA

Director, Department of Intelligent Transport Systems, Space Activities and Research, Development and Innovations, Ministry of Transportation, Czech Republic

Platform for fully autonomous vehicles

Mr. Petr KUBOŠ

Regional Sales Manager CEE

Kaspersky Industrial Cyber Security

Petr Kuboš má více než 15 let zkušeností na různých obchodních pozicích, zejména v oboru Telekomunikací a IT. V Kaspersky Lab má Petr na pozici Regionálního Sales Managera pro region CEE na starosti rozvoj obchodních aktivit týkajících se komplexních bezpečnostních řešení pro segment Enterprise, B2B zákazníci, a xSP poskytovatelům služeb.

Assoc. Prof. Zdeněk LOKAJ, Ph.D.

Expert on transport telematics, cooperative systems in road transport and safety at the Faculty of Transport CTU, Czech Republic

Security Threats of Internet of Things

doc. Ing. Zdeněk Lokaj, Ph.D. je expertem na dopravní telematiku, kooperativní systémy v silniční dopravě a bezpečnost na Fakultě dopravní ČVUT v Praze, kde pravidelně přednáší a vede výzkumné projekty. Kariéru začínal ve společnosti Accenture, kde se zaměřoval na informační systémy pro oblast dopravy (elektronické mýtné, elektronické jízdné apod.). Následně pracoval pro společnost Microsoft, kde měl na starosti dodávku služeb zákazníkům v oblasti výroby a energetiky. V roce 2009 se vrátil do akademické sféry a vede výzkumné a vývojové projekty v oboru dopravní telematiky, elektronické identifikace a dopravních systémů v silniční dopravě, zejména kooperativních systémů a bezpečnosti. Je soudním znalcem a od roku 2012 spolupracuje s Fakultou elektrotechnickou ČVUT v Praze v oblasti výzkumu identifikačních systémů.

Mr. Michal LUKÁŠ

Presales Engineer & Certified Trainer, Eastern Europe, Kaspersky Lab, Czech Republic

Kaspersky Industrial Cyber Security

Michal Lukáš má více jak patnáct let zkušeností v oboru IT a bezpečnostních technologií a také byznysu společnosti Kaspersky Lab. Již čtvrtým rokem zastupuje Kaspersky Lab ve východní Evropě na pozici Presales Engineer.

Mr. Karel MACEK

Head of Department, ICT Security Department, Ministry of Labour and Social Affairs, Czech Republic

Haven't you forgotten something (or somebody)…

Ing. Karel Macek - v oblasti informačních technologií se pohybuje celý svůj profesní život. Informační bezpečnosti se intenzivně věnuje od roku 2004 nejdříve v prostředí samosprávy, následně v komerčním sektoru a od roku 2015 ve státní správě, kde se na pozici manažera kybernetické bezpečnosti věnuje komplexnímu řízení systému bezpečnosti informací a kybernetické bezpečnosti v subjektu veřejné správy s celostátní působností, jímž je resort Ministerstva práce a sociálních věcí včetně všech svých přímo řízených organizací, kterými jsou především Úřad práce ČR, Česká správa sociálního zabezpečení, Státní úřad inspekce práce a Úřad pro mezinárodněprávní ochranu dětí.

Mr. Pavel MINAŘÍK

Chief Technology Officer, Flowmon Networks, Czech Republic

Network traffic monitoring & analysis in SCADA Networks

Pavel Minařík se zabývá oblastí kybernetické bezpečnosti od roku 2006. Účastnil se řady výzkumných projektů v oblasti analýzy provozu datových sítí a detekci pokročilých hrozeb jako výzkumný pracovník Ústavu výpočetní techniky Masarykovy univerzity. Během posledních čtyř let se účastnil několika desítek projektů nasazení řešení pro monitorování provozu a detekci pokročilých hrozeb. V současné době pracuje jako technologický ředitel ve společnosti Flowmon Networks, zodpovědný za návrh a vývoj produktů společnosti pro Flow Monitoring a Network Behavior Analysis.

Pavel Minarik has worked in the area of cyber security since 2006. During this time period he has participated in several research projects as a senior researcher of Institute of Computer Science of Masaryk University. Minarik is the author of more than ten publications in the domain of behavior analysis and numerous algorithms for traffic processing and anomaly detection, all summarized in PhD thesis: "Building a System for Network Security Monitoring". As Chief Technology Officer at Flowmon Networks, Pavel is responsible for technology roadmap, product design and development as well as technical support and customer projects worldwide.

Mr. Paolo MONIZ

Cyber Security Expert, EDP, Portugal

Human Factor to create a digital trustworthy environment for CII

With 20 years of experience in the world of information technology, began his career as a systems administrator at EDP Distribution and subsequently moved to EDINFOR where he participated in several international projects for the development of IT solutions as an analyst, programmer and also as a trainer. Latter devoted himself to project management and has embraced the Security area in 2008, when he assumed the leadership of the Security Practice at Logica Iberia. Currently is in charge of Information Security and IT Risk department at EDP and is also a board member for the CyberSecurity committee at AFCEA in Portugal.

He has a degree in Electrical and Computer Engineering from Instituto Superior Técnico and has completed successfully a post-degree in Information Systems (POSI) in the same institution. He also has an, Msc. in Information Security from Carnegie Mellon University and an, Msc. in Information Security from the Faculty of Science, University of Lisbon.

Mr. Dušan NAVRÁTIL

Director, National Cyber and Information Security Agency, Czech Republic

Actual State of Cyber Security in the Czech Republic

Mr. Tomáš NIELSEN

Partner, NIELSEN MEINL, Czech Republic

Legal liability of the entrepreneur in case of cyber-attacks

Tomáš Nielsen absolvoval Právnickou fakultu Univerzity Karlovy v Praze.
V minulosti působil jako šéfredaktor odborného časopisu Technologies & Prosperity, ředitel rozvoje podnikatelské sítě IT podnikatelů TUESDAY Business Network (dříve First Tuesday), následně též jako právník a partner mezinárodní advokátní kanceláře Rowan Legal.
V roce 2011 založil advokátní kancelář existující pod názvem NIELSEN MEINL.
Tomáš Nielsen se dlouhodobě věnuje právu telekomunikací a médií, finančnímu právu a mezinárodním investičním projektům.
Přednáší telekomunikační právo na Právnické fakultě Univerzity Karlovy a právo ICT na Fakultě dopravní ČVUT. Je rovněž rozhodcem Mezinárodního rozhodčího soudu v Rize. Tomáš Nielsen je autorem či spoluautorem řady odborných článků a publikací, například komentáře k zákonu o elektronických komunikacích (Linde, 2014), Základy softwarového práva (Wolters Kluwer, 2011), apod.

Mr. Luděk NOVÁK, Ph.D.

Member Czech Cyber Security Working Group, Czech Republic

Case study

Luděk Novák vystudoval v roce 1991 Vojenskou akademii v Brně, kde působil do roku 1994 jako odborný asistent se zaměřením na počítačovou bezpečnost. Do poloviny roku 1999 pracoval jako odborník na bezpečnost informací v různých pozicích na Generálním štábu Armády České republiky. Od léta 1999 uplatňuje zkušenosti s řízením informatiky v komerčním sektoru. V současnosti je samostatným konzultantem a auditorem se zaměřením na řízení informačních rizik, řízení bezpečnosti informací a řízení procesů ICT. Luděk Novák je držitelem certifikátů CISA (Certified Information Systems Auditor), CISSP (Certified Information Systems Security Professional), CGEIT (Certified in the Governance of Enterprise IT), CRISC (Certificate in Risk and Information Systems Control) a má kvalifikaci vedoucího auditora pro ohodnocení souladu podle norem ISO/IEC 27001 (systémy řízení bezpečnosti informací), ISO/IEC 20000 (systémy řízení služeb IT) a ISO 22301 (systém řízení kontinuity činností organizace). Luděk je též členem pracovní skupiny AFCEA – Kybernetická bezpečnost.

era bhc
Working with us to make your
Cyberspace safe

Luděk Novák graduated in 1991 at the Military academy in Brno, where he worked till 1994 year as a lecturer with focused to computer security. To second half of 1999 he worked as information security expert in different positions on the General Staff of the Army of the Czech Republic. Since the summer of 1999, applied experience in managing of information technology in the commercial sector. At present time he working as an independent consultant and auditor with a focus on information risk management, information security management and ICT management processes. Luděk Novák is CISA (Certified Information Systems Auditor), CISSP (Certified Information Systems Security Professional), CGEIT (Certified in the Governance of Enterprise IT), CRISC (Certificate in Risk and Information Systems Control) and is qualified lead auditor for ISO/IEC 27001 (information security management system), ISO/IEC 20000 (IT service management) a ISO 22301 (business continuity management system). Ludek is also a member of the AFCEA Cyber Security working group.

Mr. Lukáš OBOŘIL
Head of Department for ICS SW, I & C Energo, a. s., Czech Republic

Development of application software for CII in power engineering

Mr. Tomáš PŘIBYL
Board chairperson, European Cyber Security Excellence Center, Czech Republic

Closing Remarks

Ing. Tomáš Přibyl graduated from Cybernetics from Faculty of Electrical Engineering in ČVUT. He does in Cyber Security field since 1996. He is the founder, co-owner and Chairman of the Board in Corpus Solutions Inc., which is profiled as a consulting technology company that helps clients effectively to fight with the risks in cyberspace. Tomáš Přibyl actively promotes a consults with clients the need of changes in their approach to solving cyber risks. Together with the clients looking for a solution to integrate the cyber security into their corporate culture. He places the emphasis on education and practical training associated with the detection and the managing cyber incidents. He found the inspiration in Israel and he tries to transmit to clients this know-how. He is also Chairman of the Board in EuCybSec, which is a professional platform for sharing the latest knowledge in the field of cybersecurity.

Mrs. Paola ROCCO
Senior Consultant NTT Data Italia, Member AFCEA Rome Chapter, Italy

SCADA Security Framework?

Paola has been working for more than 13 years on Cybersecurity. Paola is a Senior Consultant in NTT Data Italia SPA, in the Business Security Service Line. He holds a bachelor's degree in computer Engineering from the „Federico II" University, Lead Auditor ISO/IEC 27001:2013 and ISO 22301:2012. He has worked in many industries to provide IT and network solutions, security assessment and policy compliance.

Member of the Scientific Committee of the University Master in „Data Protection Officer and Privacy Expert" with the patronage of the Italian Data protection Authority. Since 2014,she is chairman of the Commission „Information Security" at the Order of Engineers in Rome. She is involved in organizing and training a large number of cybersecurity conferences, seminars and courses in Rome. In November 2017 she will participate in the Word Engineer Forum with an abstract and a speech about Information Security for humankid's heritage. Paola is also a member of the AFCEA Rome chapter.

Mr. Petr ROUPEC
CEO, Bohemia Market CZ, Czech Republic

Operational Technology (OT) cyber security IS NOT SAME AS Information Technology (IT) cyber security

Cyber Security for Operations Technology Systems
Since graduation from the Technical University at Brno, Petr worked at various roles in automation business. The assignments ranged from small machinery automation up to designing and commissioning control systems for refineries and power stations.
These decades of hands-on experience empowered and enabled him to lead an international team designing nuclear power station control and electrical systems from 2009 – 2015.
Petr is very experienced with Distributed Control Systems and related underlying technologies, such as networking.
Ultimately, Petr applied his skills and experience in engineering management and running an industrial service organization to build his own company, Bohemia Market. Its purpose is to provide state of the art support to existing industrial facilities, which suffer from poor OEM support and the high costs that come with fast electronic products obsolescence.
This problematic obsolescence of high value operational control systems, which is directly on collision course with the current cyber security threads, led to the design of our cyber security hand book for industrial facilities.

Mr. Udo SCHNEIDER
Security Evangelist, Trend Micro, Germany

Security in industrial Automation – friend or foe?

Udo Schneider knows not only the dangers lurking in the Internet but also how to protect oneself from them. In his current position as Security Evangelist he focuses primarily on Industrial Automation and IoT Security. Before he started his current position he concentrated on topics like cloud-computing, virtualisation encryption as well as network security as a Solution Architect for several years. Before that, he also served as Product Marketing Manager and as Channel Development Manager at Trend Micro.
Udo looks back on many years of experience he has gained at leading vendors within the IT security market: Amongst others, in his five years' stay at Check Point Technologies he worked as Systems Engineer, as Senior Consultant, as Security Analyst, and as trainer. At Perimetrix Systems, he was Technical Director.

Mr. Václav SCHOVÁNEK
AKS Legal, Czech Republic

Legal liability of the entrepreneur in case of cyber-attacks

5 let pracoval v přední české reklamní agentuře MARK/BBDO
Vystudoval Právnickou fakultu Univerzity Karlovy v Praze
Od roku 2005 se zabývá právem ICT, reklamy, autorským právem a ochranou osobních údajů
Od roku 2008 vede vlastní advokátní kancelář pod značkou // AKS LEGAL
Člen České advokátní komory a PRIVACY EUROPE NETWORK
Lektor Google Academy v roce 2015 a 2016
Pravidelně přednáší na téma právní problematiky v oblasti IT

Mr. Tobias SCHRÖDEL
IT-Security expert, Expert on TV and the world's first Comedyhacker®, Germany

Live hacking show – internet of things

For almost 14 years, Tobias Schrödel has worked for TSystems International as a consultant for IT-security. Before that, he had been responsible for the development of logistic solutions in the Enterprise Business Segment of United Parcel Service Europe. He is a certified instructor for IT-specialists und is working for the German Chamber of Commerce as an auditor of soon to be IT-specialists for over a decade.

Mr. Ragnar RATTAS
Senior Cyber Security Expert, BHC Laboratory, Estonia

Finding SCADA devices and what next

Dr. Radek ŠINDELÁŘ
Researcher, Vienna University of Technology, Institute of Software Technology and Interactive Systems, Czech Republic

Industry 4.0 Concept

Mr. Ondřej ŠŤÁHLAVSKÝ
Regional Director, CEE, Fortinet, Czech Republic

SCADA Systems as Target of Cyber Attacks

Ondřej Šťáhlavský is respected expert within IT Security field almost 15 years. He has joined Fortinet 9 years ago as the first Territory Manager for the CEE region. Within those years Ondřej served in multiple roles, one of them was EMEA Technical Support Director where he built the new Technical Assistance Center supporting the EMEA region from Prague (Czech Republic). Once this mission has been finished Ondřej came back to CEE salesforce in the role of Regional Director.

Mr. Vladimír ŠULC, Ph.D.
CEO, IQRF Tech, s. r. o., Czech Republic

Wireless communication and security

Ing. Vladimír Šulc, Ph.D. - Autor bezdrátové technologie IQRF, jejíž vývoj započal v roce 2004. Absolvent FEL ČVUT, zakladatel a jednatel firmy MICRORISC, s. r. o. V roce 2014 technologie IQRF oceněna Českou hlavou, dnes je rozšířena ve stovkách tisíc zařízeních po celém světě.

Mr. Igor TOMEŠ
Board Member, ČIMIB, Czech Republic
Moderator

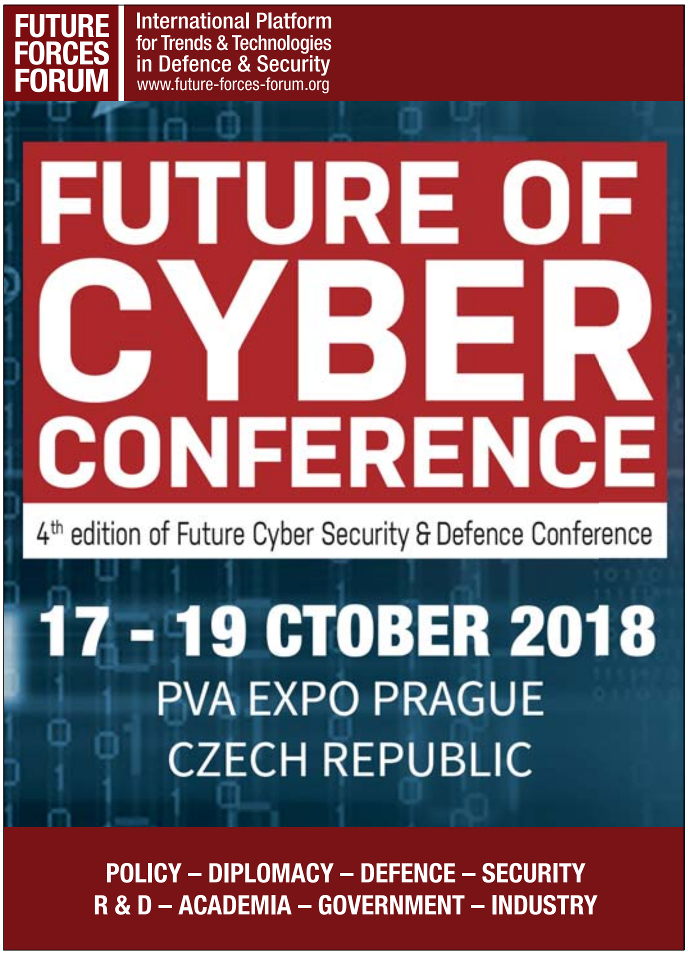
New Technological Trends in ICS Security

Ing. Igor Tomeš, CSc, vystudoval ČVUT obor sdělovací technika. Po studiích se věnoval vědecké práci na ČVUT FEL a ve výzkumném ústavu TESLA VUST, kde se zabýval optickými lokálními sítěmi. Po roce 1990 začal podnikat. Po 13 letech přešel do korporátní sféry a věnuje se kybernetické bezpečnosti. V současné době pracuje ve společnosti DataSpring.

Mr. Martin UHER
Board Member, European Cyber Security Excellence Center, Czech Republic
Moderator

Cyber Security & Human Factor

Geo:
Geoconnexion International Magazine
SPOT THE DETAIL
PLÉIADES 50 CM IMAGERY CAPTURES IT ALL



FUTURE FORCES FORUM
International Platform
for Trends & Technologies
in Defence & Security
www.future-forces-forum.org

FUTURE OF CYBER CONFERENCE

4th edition of Future Cyber Security & Defence Conference

17 - 19 CTOBER 2018
PVA EXPO PRAGUE
CZECH REPUBLIC

POLICY – DIPLOMACY – DEFENCE – SECURITY
R & D – ACADEMIA – GOVERNMENT – INDUSTRY

Future of Cyber Conference 2018 PARTNERSHIP Conditions

General Partner 10 000 €

Partner 6 000 €

Cyber Pavilion Sponsor 4 000 €

Topic Sponsor 3 000 €

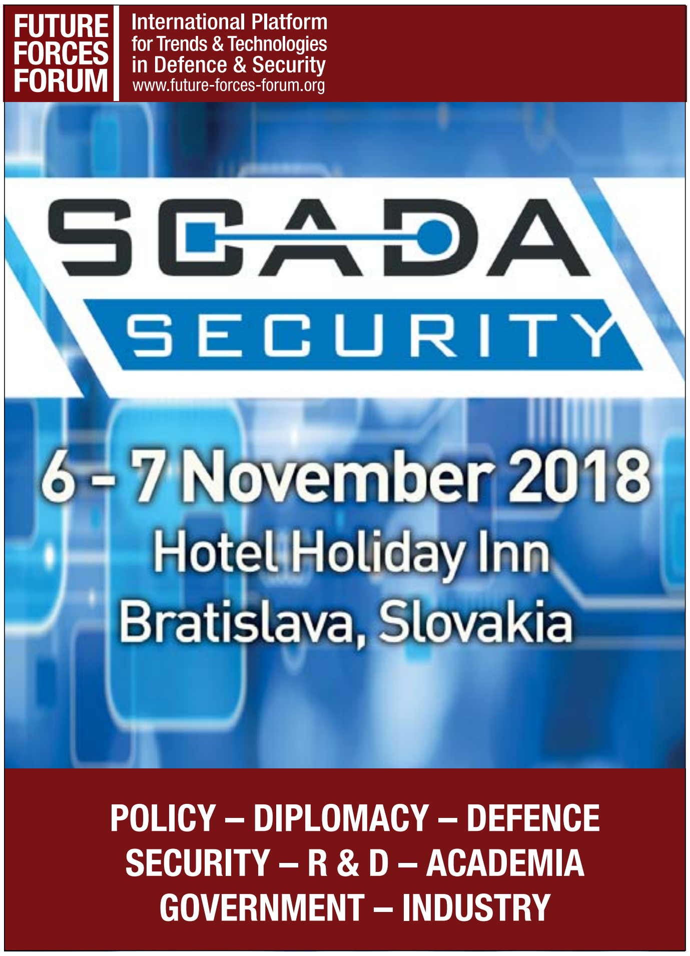
Table Top + Partner Slot 2 600 €

Cyber Workshop Partner 1 900 €

Service Partner 1 800 €

Partner Slot 1 600 €

Table Top Presentation 1 200 €



FUTURE FORCES FORUM
International Platform
for Trends & Technologies
in Defence & Security
www.future-forces-forum.org

SCADA SECURITY

6 - 7 November 2018
Hotel Holiday Inn
Bratislava, Slovakia

POLICY – DIPLOMACY – DEFENCE
SECURITY – R & D – ACADEMIA
GOVERNMENT – INDUSTRY

SCADA Security Conference 2018 PARTNERSHIP Conditions

General Partner 10 000 €

Main Partner 5 600 €

Partner with Speaker Slot and Table Top 3 200 €

Partner with Speaker Slot 2 400 €

Partner with the Table Top 1 000 €

For more information, please, contact:
BG (Ret.) **Jaroslav DIENSTBIER**
E-mail: dienstbier@future-forces-forum.org
Tel.: +420 601 335 470
www.future-forces-forum.org

FUTURE FORCES FORUM

International Platform for Trends & Technologies in Defence & Security

www.future-forces-forum.org

SAVE THE DATE OF THE NEXT GLOBAL FORUM

17-19 October 2018

PRAGUE, Czech Republic

FFF 2016 at a glance:

7,652 Participants from over **59** countries

1,200+ Official delegates and VIP guests representing armed, security, and emergency domain (**5** Ministers of Defence, **3** CHODs, **6** Air Force Commanders, **13** Ambassadors, **20+** Defence/Military/Air Attachés)

Official delegates from **59** countries, **35+** international organisations, and **24** universities

40+ Generals representing **22** countries and international organisations

15 NATO working groups and expert teams, **300+** members

240+ Speakers from **24** countries, **11** international organizations, and **21** universities

20 Specialized events at one place (exhibition, congress, **3** conferences, **13** workshops, **2** round tables)

169 Exhibitors from **25** countries

210+ Represented companies and brands

15 National Expositions/International Organisation Expositions

57 Accredited journalists

65 Official Media Partners

8M+ Hits of worldwide media campaign

POLICY - DIPLOMACY - DEFENCE - SECURITY - R&D - ACADEMIA - GOVERNMENT - INDUSTRY

BAXI GROUP
METRO
HORADO

GREYCORTEX

All-Seeing Network Security

GREYCORTEX MENDEL helps organizations protect their futures by detecting cyber threats others miss.

Powerful Detection

- Most advanced behavioral detection

- Unique detection algorithms

- Powerful signature-based detection with DPI

Unique Visualization

- Enriched network flows

- Filter individual subnets, hosts, devices, and applications on the network

- Monitor IoT and SCADA devices

What’s hiding in your network?

www.greycortex.com

FUTURE FORCES FORUM

POLICY

DIPLOMACY

DEFENCE

SECURITY

R & D

ACADEMIA

INDUSTRY

www.future-forces-forum.org