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

4 – 5 November 2019

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

CORPUS SOLUTIONS
CYBERSECURITY EXPERTS

Check Point®
SOFTWARE TECHNOLOGIES LTD

Conference Main Partners

FORTINET®

SAMSUNG

Conference Partners

Bohemia Market.cz
COLSYS AUTOMATIK
Flowmon
GREYCORTEX
veracomp
Service & Support

Partners with Speaker Slot

ALEFNULA
CYBERG

Patronage and Programme Guarantors

European Cyber Security Excellence Center
NÚKIB
ČIMIB
ictunie

FUTURE FORCES FORUM

International Platform for Trends & Technologies in Defence & Security

www.future-forces-forum.org

SAVE THE DATE OF THE NEXT GLOBAL FORUM

21-23 October 2020

PRAGUE, Czech Republic

FFF 2018 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

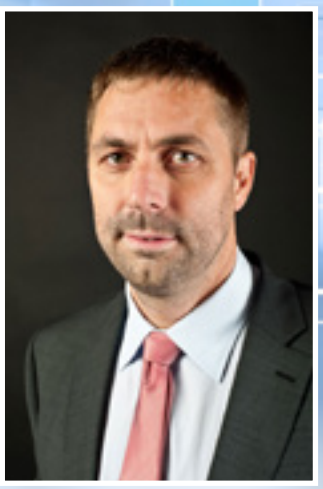
15 National Expositions/International Organisation Expositions

57 Accredited journalists

65 Official Media Partners

8M+ Hits of worldwide media campaign

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



Vážení účastníci konference SCADA Security,

s potěšením jsme pro Vás připravili pokračování bezpečnostní konference pro oblast průmyslových řídicích systémů. Bezpečnost ICS, které jsou často důležitou součástí kritické infrastruktury, spolu s rychlým rozvojem Internetu věcí a navazujícími oblastmi je stále důležitějším kritériem zvláště v době, kdy se blíží nasazení a rozvoj komunikačních sítí páté generace. Potenciál těchto mocných technologií přinese nutně také nový pohled na bezpečnost systémů na nich provozovaných.

Věříme, že kombinace již probíhajících 5G workshopů s konferencí SCADA Security 2019 splní Vaše očekávání od takto koncipovaných akcí, jejichž záměrem je přinášet ucelené informace o trendech v této oblasti, pomáhat správné orientaci v problematice, propojovat odborníky, mapovat moderní řešení a přístupy, či objevovat nové obchodní příležitosti.

V rámci jednotlivých odborných akcí platformy FUTURE FORCES FORUM (FFF) je naším cílem rozvíjet aktuální témata v oblasti obrany a bezpečnosti tak, aby se každé dva roky v říjnu na PVA Expo Praha prezentovaly závěry z celého období a zhodnotily výsledky plnění cílů.

Rád bych poděkoval všem podporovatelům FFF a aktuálně zejména těm, kteří podpořili konferenci SCADA 2019, především společnostem Corpus Solutions a Check Point jako generálnímu partnerovi a hlavním partnerům Fortinet a Samsung. Bez jejich laskavé podpory bychom nedokázali akci připravit na úrovni, na kterou jste zvyklí, a kterou očekáváte.

Věřím, že si užijete dva přínosné konferenční dny v příjemné atmosféře a že si odnesete řadu nových poznatků a kontaktů. Za celý přípravný výbor konference a realizační tým FFF Vám přeji mnoho úspěchů ve Vaší náročné práci.

Za tým SCADA Security konference a celého projektu FFF

Daniel Kočí
generální ředitel

Dear SCADA Security Conference participants,

It is with pleasure that we have prepared for you the continuation of the security conference for industrial control systems. The security of ICS, which is often an important part of critical infrastructure, along with the rapid development of the Internet of Things and related areas, is an increasingly important criterion, especially at a time when the next, fifth generation communication networks are approaching and developing. The potential of these powerful technologies will also necessarily bring a new perspective on the security of the systems running on them.

In combination with the already running 5G workshops we believe that our conferences will meet your expectations of such conceived events, bring comprehensive information and trends in this field, help you to orientate in the field, meet the necessary experts, map modern solutions and approaches, and discover new business opportunities.

In the framework of selected events of the Future Forces Forum, our goal is to develop current defence and security topics so that it culminates every two years in October at the PVA Expo Prague, where conclusions from the entire period will be presented and results achieved.

I would like to thank all FFF supporters and, in particular, those who have supported the SCADA conference, especially Corpus Solutions and Check Point as the general partner and main partners of Fortinet and Samsung. Without their kind support and the support of all of you, we would not have been able to prepare the event at the level you are used to and expect.

I believe that you will enjoy two beneficial conference days in a pleasant atmosphere and that you will take with you a lot of new knowledge and contacts.

On behalf of SCADA Security team and the whole project FFF

Daniel Kočí
Managing Director

GREYCORTEX

Bring IT Security and SCADA Engineers Together

GREYCORTEX offers an advanced Network Traffic Analysis solution for IT and OT networks by using traditional detection techniques as well as advanced artificial intelligence and machine learning.

Protect your network from known threats

See all connected devices

Passive solution

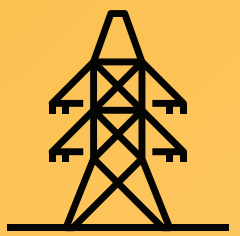
Identify anomalous behaviors and misconfigurations

Monitor multiple locations from one central point

Stable IT and OT networks

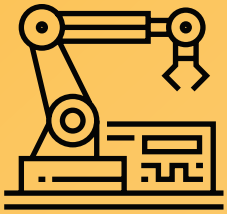
GREYCORTEX focuses on the following industries:

Transmission Grids



Energy Distribution

Public Utilities



Industry 4.0

Česká pobočka AFCEA se svými pracovními skupinami pracovala společně s hlavním organizátorem na přípravě SCADA Security konference nepřetržitě téměř rok. Dovoluji si to uvést především jako důkaz toho, že pokládáme problematiku non-IT resp. IOT bezpečnosti za kriticky důležitou pro bezpečnost nejen průmyslových podniků či jiných institucí, firem či samotných osob, které dané technologie používají, ale i pro bezpečnost České republiky jako celku. Na bezpečném chodu technologií jsme v současné době životně závislí všichni a nebude tomu jinak ani v budoucnu.

Dle mého názoru je důležité se na různých fórech a konferencí setkávat, diskutovat současné a předvídat budoucí hrozby a s nimi související trendy v oblasti bezpečnosti, ale pokládám za neméně důležité výsledky této diskuze aplikovat do reality. Domnívám se, že v obraně a bezpečnosti kybernetického prostoru máme značné rezervy. Není na místě ale kritizovat současný stav, ale dělat vše pro to, aby byla v co nejbližší budoucnosti situace jiná - lepší. K tomu je třeba učinit řadu nezbytných legislativních kroků, kroků v oblasti vzdělávání i vzájemné spolupráce odborné veřejnosti, akademické sféry, státního sektoru i samotných průmyslových společností. Česká pobočka AFCEA je připravena být nadále aktivní v této oblasti i v oblastech dalších ICT & bezpečnostních témat.

Přeji SCADA Security konferenci hodně zdaru při projednávání důležitých témat v oblasti SCADA, přeji České republice a nám všem, aby výsledky a závěry tohoto setkání byly co nejdříve aplikovány a realizovány ve prospěch obrany a bezpečnosti našeho společného kybernetického prostoru.

Ing.Tomáš Müller
Prezident, Česká pobočka AFCEA

The AFCEA Czech Chapter and its working groups worked together with the main organizer on the preparation of the SCADA Security conference for almost a year. I would like to mention this primarily as proof that we consider the issue of non-IT, respectively IOT security as critically important for the security not only of industrial enterprises or other institutions, companies or persons using the technology, but also for the security of the Czech Republic as a whole. Today, we are all dependent on the safe operation of technology, and it will not be otherwise in the future.

In my opinion, it is important to meet at various forums and conferences to discuss current and anticipate future threats and related security trends, but I consider it equally important to apply the results of this discussion to reality. I believe that we have considerable reserves in the defence and security of cyberspace. But it is not appropriate to criticize the current situation, but to do everything possible to make the situation different - better. To do this, a number of necessary legislative steps, steps in the field of education and mutual cooperation of the professional public, academia, the state sector and industrial companies themselves must be taken. The AFCEA Czech Chapter is ready to remain active in this area as well as in other ICT & security topics.

I wish the SCADA Security conference good luck in discussing important SCADA topics, I wish the Czech Republic and all of us that the results and conclusions of this meeting are applied and implemented as soon as possible in favour of the defense and security of our common cyberspace.

Tomáš Müller
President, AFCEA Czech Chapter


CYBER DEFENSE
MEDIA GROUP
WHERE INFOSEC KNOWLEDGE IS POWER
To The Moon and Back!
Only with Cyber Defense Media Group
www.cyberdefensetv.com
www.cyberdefenseradio.com
www.cyberdefenseawards.com
www.cyberdefensemagazine.com

Úvodem bych rád poděkoval organizátorům konference, kteří mi opakovaně vyjádřili důvěru a svěřili mi napsání úvodního slova ke SCADA konferenci. Přiznám se, že když jsem přemýšlel, jak bych co možná nejlépe namotivoval Vás, potencionální zájemce o tuto konferenci, přinesl mi kolega zajímavý dopis z konce října tohoto roku. V rámci tohoto dopisu se ředitel české pobočky nejmenované významné nadnárodní společnosti vyrábějící automatizační prvky omlouval svým zákazníkům, že jeho systémy byly pod úspěšným kybernetickým útokem, který firmu totálně paralyzoval. Co mě však obzvláště zaujalo, bylo následující prohlášení rozeslané všem odběratelům této společnosti, cituji: … „naše společnost vynakládá nemalé částky na kybernetickou bezpečnost, pravidelně aktualizuje své systémy, zálohuje data, používá firewally, antivirové programy, přístupová hesla apod., přesto jsme nedokázali zabránit škodám, které útok přinesl. Nejsme si tak vědomi jakéhokoliv pochybení v této oblasti a jsme přesvědčeni, že uvedenému útoku jsme nemohli předejít a považujeme jej za překážku mající charakter vyšší moci.“ Asi nikdo z nás by se nechtěl vžít do role majitele této společnosti, který na základě této události není schopen plnit své smluvní závazky vůči třetím stranám a bojuje o reputaci své společnosti.

Toto však nebyla jediná nepříjemná zpráva, kterou jsem od posledního ročníku SCADA konference zaregistroval. Koncem roku 2017 se objevil nový malware Triton. Triton je první malware platforma, která postihuje systémy funkční bezpečnosti SIS (Safety Instrumented Systems) značky Triconex od společnosti Schneider Electric. Tyto systémy se používají na zajištění bezpečnosti obzvláště rizikových procesů s trojitou redundancí. Útočníkovi se podařilo získat vzdálený přístup na inženýrskou pracovní stanici, kde malware Triton nainstaloval a byl schopný přeprogramovat bezpečnostní programovatelné automaty SIS. Bohužel důkaz toho, že ve SCADA světě se v případě kybernetických útoků nebavíme pouze o poškození businessu, ale také o možném ohrožení lidských životů.

Bezesporu všechny tyto příklady, související legislativní rámec spolu společně s aktivitami regulátora NUKIB mají za následek celkovou změnu přístupu společností k řešení témat kybernetické bezpečnosti ve SCADA prostředí. Vnímám, že zatímco minulému ročníku vládla hlavně osvěta, dnes jsou to již konkrétní způsoby řešení bezpečnosti a nové rozvojové oblasti (Chytrá města, 5G sítě, Industry 4.0, IoT), které mají konkrétní business přínosy a kde kybernetická bezpečnost musí být nedílnou součástí architektonického návrhu každého projektu, který se o tyto trendy opírá.

Přijměte proto mé pozvání a přijďte se v rámci probíhající konference setkat s předními odborníky v této oblasti, kteří Vám pomohou s řešením aktuálních problémů a ukáží Vám nové technologické oblasti, které mohou ovlivnit Vaši budoucnost. Přeju Vám, abyste nikdy nemuseli řešit žádnou událost mající charakter „vyšší moci“, kde by v pozadí figurovalo kybernetické napadení a pevně věřím, že návštěva této konference je dobrou k tomu dobro prevencí.

Těším se na Vaši návštěvu.

Tomáš Přibyl
CEO, Corpus Solutions, a.s.

CORPUS SOLUTIONS
CYBERSECURITY EXPERTS

SCADA/OT SECURITY

Pomůžeme vám s řešením kybernetické bezpečnosti vašich průmyslových řídících systémů.

www.corpus.cz

Conference Programme

4 NOVEMBER 2019 — Prague, Hotel DAP

Opening Session

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

9:00 - 10:15

Welcome Speech
Tomáš MÜLLER, President, AFCEA Czech Chapter, Czech Republic

09:05 **Opening Speech – Industry 4.0 – Artificial Intelligence – 5G Strategy**
Mr. Karel HAVLÍČEK, Minister, Ministry of Industry & Trade, Czech Republic

09:20 **Czech Digital Agenda**
Mr. Vladimír DZURILLA, Prime Minister Advisor, Chief Digitial Officer, Government of the Czech Republic, Czech Republic

09:35 **Opening Speech**
Mr. Dušan NAVRÁTIL, Director, National Cyber and Information Security Agency, Czech Republic

09:50 **Involve IOT technologies into Civil Protection Services**
Col. Daniel MIKLÓS, Fire Rescue Service of the Czech Republic, Czech Republic

10:05 **General Partner Speech**
Mr. Tomáš PŘIBYL, CEO, Corpus Solutions, a.s., Czech Republic

10:15 - 10:50 Coffee break

Current and Future Cyber Threats – protect your SCADA systems

Moderator: **Mr. Aleš ŠPIDLA**, President, ČIMIB, Czech Republic

10:50 - 12:40

10:50 **What will be the critical infrastructure of tomorrow?**
Mr. Vladimír ROHEL, Security Director, National Agency for Communication and Information Technology, Czech Republic

11:10 **ICS accessible from the Internet = bad (and very common) practice**
Mr. Jan KOPŘIVA, Coordinator – Computer Security Incident Response Team (CSIRT), ALEF NULA, Czech Republic

11:30 **SCADA Systems as Target of Cyber Attacks**
Mr. Jan VÁCLAVÍK, Systems Engineer, Fortinet, Czech Republic

11:50 **New approaches to detection of SCADA threats**
Mr. Vladimír SEDLÁČEK, Technical Director, GREYCORTEX, Experienced Developer, Analyst, Certified Ethical Hacker, Certified Livewire Investigator, Czech Republic

12:10 **Heartbeat to hell**
Mr. Tobias SCHROEDEL, Cyber Expert, Germany

12:40 - 13:30 Lunch break

Current and Future Cyber Threats – protect your SCADA system

Moderator: **Mr. Aleš ŠPIDLA**, President, ČIMIB, Czech Republic

13:30 - 14:30 PANEL DISCUSSION

Panelists:

Mr. Tomáš PŘIBYL, CEO, Corpus Solutions, a.s., Czech Republic
Mr. Martin FABRY, Owner & Cybersecurity Consultant, Accura s.r.o., Czech Republic
Mr. Jan VÁCLAVÍK, Systems Engineer, Fortinet, Czech Republic
Mr. Dettmer HENDRIK, Head of IoT Security Lab, TÜV TRUST IT GmbH, Austria
Mr. Kamil TICHÝ, Ministry of Defence of the Czech Republic, Czech Republic

14:30 - 15:00 Coffee break

Check Point
SOFTWARE TECHNOLOGIES LTD

KEEP **CRITICAL INFRASTRUCTURE** UP AND RUNNING

Check Point Industrial Control Protection
A Single Architecture for:

- Perimeter Protection and Network Segmentation
- Secure Remote Access
- Granular SCADA traffic Control and Logging
- Intrusion Detection & Prevention
- Industrial Grade Security Gateways for Control Rooms, Production Floors and Field deployments
- Central Management and Compliance Tracking

checkpoint.com

Conference Programme

New Technological Trends in ICS Security

Moderator: **COL (RET.) Martin UHER**, Vice President, EUCYBSEC, Czech Republic

15:00 - 17:40

15:00 **Expert Session Opening**
Mr. Lukáš OBOŘIL, Head of Control Systems Department – Software, IC Energo, a.s., Czech Republic

15:25 **Network monitoring and anomaly detection in ICS/SCADA**
Mr. Pavel MINAŘÍK, Chief Technology Officer, Flowmon Networks, Czech Republic

15:45 **1 + 1 = 3 : Joining forces for greater security of the inseparable worlds of IT and SCADA / ICS and IoT**
Mr. Tomáš BÁRTA, Channel Sales Executive, VERACOMP, Czech Republic

16:05 **Threat Monitoring in SCADA ICS**
Mr. Martin FABRY, Owner & Cybersecurity Consultant, Accura s.r.o., Czech Republic

16.30 **UKENERGO experience in counteracting cyber-security strikes**
Mr. Serhii HALAHAN, Chief Information Officer, NPC UKENERGO, Ukraine

17.00 **Research on vulnerabilities of remotely controlled industrial equipment**
Mr. Jiří GOGELA, Member, Czech Cyber Security Working Group, Cyber Expert, Trend Micro, Czech Republic

17.20 **Q & A**

17.40 **1st Day Cloasing Remarks**
Mr. Petr JIRÁSEK, Chairman, Czech Cyber Security Working Group, AFCEA, Czech Republic

18:00 -> **SCADA PARTY** (by invitation only)

Parallel Workshops

ICS (SCADA) Security for C-Level

Moderator: **Mr. Jan DIENSTBIER**, Vice President, ČIMIB, Czech Republic

10:45 - 12:30

Presenters:
M**r. Tomáš PŘIBYL**, CEO, Corpus Solutions, a.s., Czech Republic
M**r. Tobias SCHROEDEL**, Cyber Expert, Germany

Programme:

10:45 **Workshop opening**
10:50 **How to protect your business**
11:10 **How to build Cyber Security in industrial environment**
11:40 **Cyber Show**
12:15 **Discussion**
12:30 **Closing Remarks**

ICS (SCADA) Security for MILINT

Moderator: **Mr. Petr JIRÁSEK**, Chairman, Czech Cyber Security Working Group, AFCEA, Czech Republic

14:45 - 16:15

Presenters:
M**r. Tomáš MÜLLER**, President, AFCEA Czech Chapter, Czech Republic

Programme:

14:45 **Workshop opening**
15:15 **Discussion**
16:15 **Closing Remarks**


Be sure to realize everything DX has to offer for OT
The benefits of Digital Transformation are as equally applicable to OT as they are to IT. But only if Security is an integral part of the transformation.
Fortinet's security solutions, delivered through the Fortinet Security Fabric architecture, ensures that any organization's DX plans are securely achieved for both IT or OT environments.
FORTINET
www.fortinet.com
Copyright © 2019 Fortinet, Inc. All rights reserved.

5 NOVEMBER 2019 — Prague, Hotel DAP

Second Conference Day Opening

9:00 **2nd Conference Day Opening – SCADA Security as a part of security organization**
Mr. Miroslav BRVNIŠŤAN, President, Slovak AFCEA or AFCEA EUROPE, Slovakia

Modern Communication Systems, Future Networks – 5G, Cyber Security and SCADA/ICS

Moderator: **Mr. Petr JIRÁSEK**, Chairman, Czech Cyber Security Working Group, AFCEA, Czech Republic

09:10 - 10:55

09:10 **Opening Speech**
Mr. Petr OČKO, Deputy Minister, Ministry of Industry & Trade, Czech Republic

09:25 **Expert Opening Speech**
Mr. Terry HALVORSEN, Executive Vice President, Samsung Global 5G, USA

09:50 **How to make 5G trustworthy technology**
Mr. Tomáš PLUHAŘÍK, Czech Republic

10:10 **5G Technology**
Mr. Jan BENEŠ, Safetron, Czech Republic

10:30 **Standardization and procedures in design of critical communication infrastructure**
Mr. Jiří KASNER, Chairman of the Board, COLSYS – AUTOMATIK, a.s., Czech Republic

10:50 **Q & A**

10:55 - 11:30 Coffee break

Connected World – technical, business and legislative aspects

Moderator: **Assoc. Prof. Zdeněk LOKAJ**, Academic Expert, Czech Technical University in Prague, Czech Republic

11:30 - 12:30 **PANEL DISCUSSION**

11:30 **Opening Speech – New addictions as a source of new threats**
COL (RET.) Martin UHER, CEO, CyberG Europe a.s., Czech Republic

Panelists:
Dr. Josef PROKEŠ, Vice Chairman, Data Protection Office of the Czech Republic (invited), Czech Republic
Mr. Jan DIENSTBIER, Vice-President, ČIMIB, Czech Republic
Dr. Eva FIALOVÁ, LLM., Ph.D., Institute of State and Law of the Academy of Sciences, Czech Republic
COL (RET.) Martin UHER, CEO, CyberG Europe a.s., Czech Republic

12:30 - 13:15 Lunch break

SAMSUNG

Samsung Global Government Solutions

Imagine what we can achieve together.

For more information, please contact: GLBLGOVinfo@samsung.com

Industry 4.0 – Connected World, Mobility and IoT

Moderator: **Assoc. Prof. Zdeněk LOKAJ**, Academic Expert, Czech Technical University in Prague, Czech Republic

13:15 - 15:30

13:15 **Cyberattack in Industry 4.0 and its defence**
Mr. Rostislav DOUBEK, Offensive Security Team Member, Corpus Solutions, a.s., Czech Republic
Mr. Pavel KLIMEŠ, Director, Security Products Development, Corpus Solutions, a.s., Czech Republic
Mr. Robert KOMINKA, ICS Security Expert, Corpus Solutions, a.s., Czech Republic

13:40 **Weekend Warrior: Attacking the Future SCADA Now**
Dr. Bernhards BLUMBERGS, CERT.LV, Lead Cybersecurity Expert, Advisor to BHC Laboratory, Latvia

14:00 **One way data transfer. Entirely secure. Unlimited Tags.**
Mr. Petr ROUPEC, Chief Executive Officer & President, Bohemia Market, Czech Republic

14:20 **Big Data in ICS**
Mr. Ladislav STRAKA, Managing Consultant at Service & Support, Czech Republic

14:40 **Mr. Jozef ŠEREG**, The Prague Public Transit Co. Inc., Czech Republic

15:00 **C-ITS security solution in C-ROADS Czech Republic project**
Mr. Miloslav PAVELKA, O2 Czech Republic / TeskaLabs, Czech Republic

15:20 **Q & A**

15:30 **Conference Closing Remarks**
Mr. Tomáš MÜLLER, President, AFCEA Czech Chapter, Czech Republic

Parallel Workshop

Protect our business against SCADA attacks

Moderator: **Mr. Jaroslav PEJČOCH**, Vice Chairman, Czech Cyber Security Working Group, Czech Republic

11:00 - 12:45

Presenters:
Mr. Tomáš MÜLLER, President, AFCEA Czech Chapter, Czech Republic
Mr. Jan VYKOUKAL, Head of Department, Ministry of Interior, Czech Republic
Mrs. Barbora PÁLKOVÁ, CNP & Strategy Dept., Fire Rescue Service of the Czech Republic, Czech Republic
Assoc. Prof. Radomír ŠČUREK, Deputy Head, Department of Security Services, Faculty of Safety Engineering, Technical University of Ostrava, Czech Republic

Programme:

11:00 **Workshop opening**

11:05 **Security research in the Czech Republic – planned activities**

11:20 **Population protection concept**

11:35 **Cyber security in the Czech Republic in relation to the concept of population protection**

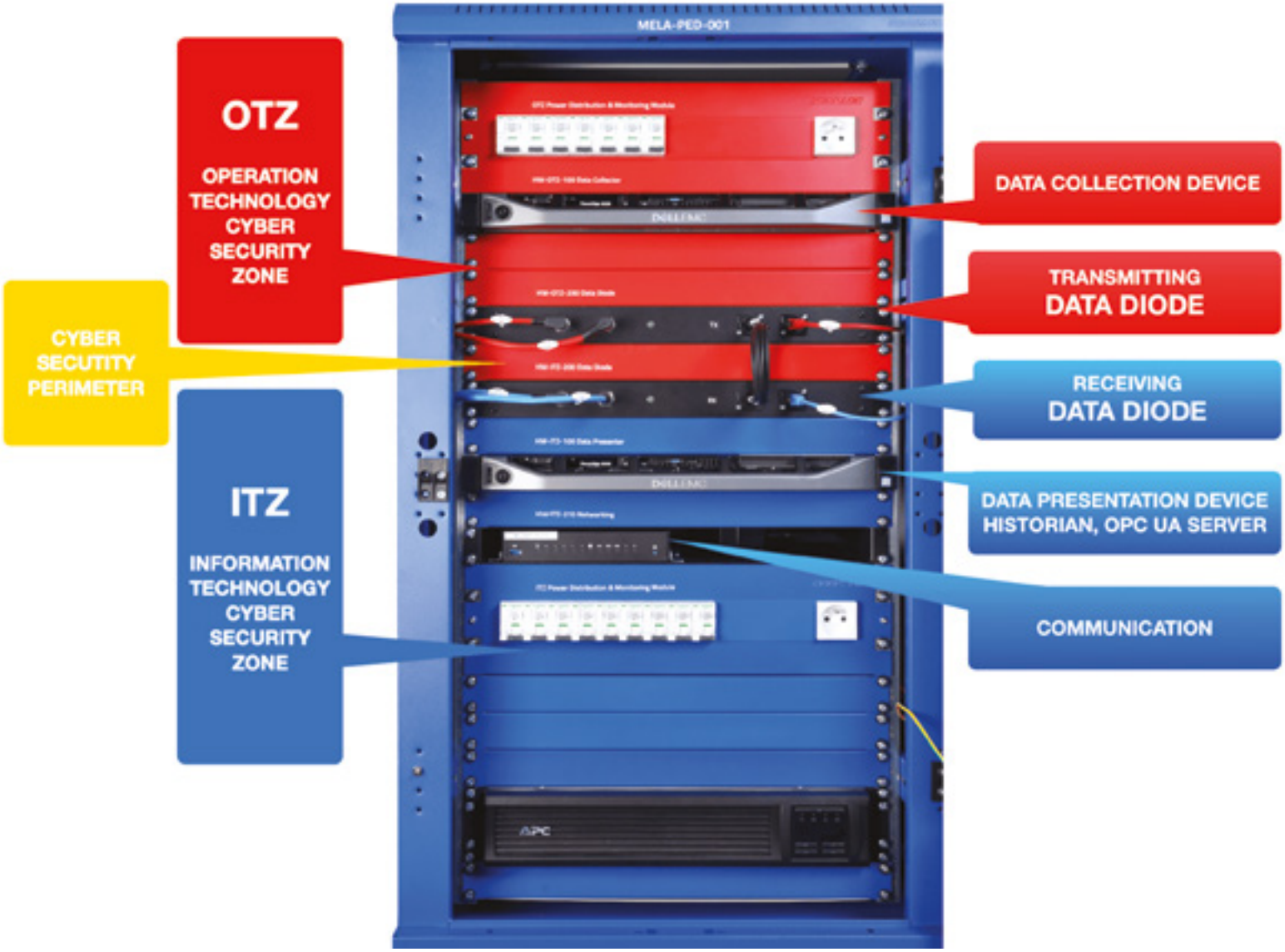
11:55 **Opportunities in the field of security research in relation to the concept of population protection and cyber security**

12:05 **Discussion**

12:40 **Closing Remarks**

PEDRONEL ONE

One Way Data Transfer.
Entirely Secure. Unlimited Tags.



Unbeatable One-Time Fee
to Keep You Competitive on the Grid

Learn more at **bm.company**

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 Chairmen

Assoc. Prof. **Josef POŽÁR**
Vice-Rector for Strategy and Development, Police Academy of the Czech Republic in Prague, Czech Republic
Honorary Chairmen

Members

Mr. **João Miguel ÃNNES**
Cybersecurity Board Member, AFCEA
Portugal

Mr. **Jaroslav BURČÍK**
Director ITU Cyber Security Center of Excellence, Czech Republic

Mr. **Jan DIENSTBIER**
Vice-president, ČIMIB
Czech Republic

LtCol. **Petr HRŮZA**
Member, Czech Cyber Security Working Group AFCEA, Univerzity of Defence, Czech Republic

Col. (Ret.) **Ladislav KOLLÁRIK**
Vice-president,
AFCEA Slovak chapter, Slovakia

Mr. **Zdeněk LOKAJ**
Faculty of Transport, Czech Technical University in Prague, Czech Republic

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

Mrs. **Barbora NEKOLOVÁ**
Representative, ČIMIB, Czech Republic

Dr. **Josef PROKEŠ**
Vice Chairman, Data Protection Office of the Czech Republic
Czech Republic

Mr. **Tomáš PŘIBYL**
Member, AFCEA, Czech Republic

Mr. **Vladimír ROHEL**
National Cyber and Information Security Agency, Czech Republic

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

Mr. **Jaroslav ŠMÍD**
Deputy Director, National Cyber and Information Security Agency, Czech Republic

COL (RET.) **Martin UHER**
Board Member, EUCYBSEC, Czech Republic

COLSYS AUTOMATIK

Společnost COLSYS – AUTOMATIK, a.s., se ve svém portfoliu věnuje již více než 20 let návrhu, projektování, nasazení, dodávkám a servisu průmyslových komunikačních sítí. V drtivém procentu se jedná o kritickou komunikační síťovou infrastrukturu v průmyslovém prostředí

Výrobci průmyslových řídících systémů a koncových komunikačních prvků kladou při vývoji nových zařízení stále silnější důraz na zajištění kybernetické bezpečnosti. Provádí důkladné penetrační testy komunikačních rozhraní svých výrobků, neboť si již zákazníci plně uvědomují možnosti zneužití výhod kybernetického světa komunikací a poptávají tudíž důvěryhodná a bezpečná zařízení. Související zákon o kybernetické bezpečnosti pak jen zdůrazňuje potřebu zohlednění průmyslových standardů kybernetické bezpečnosti i z pohledu infrastruktury státu.

Řídící systémy a další koncové komunikační prvky, jako jsou například frekvenční měniče motorů, vstupně-výstupní decentralizované periferie, senzory, jsou součástí komunikační síťové infrastruktury. Tato infrastruktura je zároveň tvořena i aktivními síťovými prvky, které informace distribuují mezi komunikačními partnery. V současné době je již zcela běžným standardem pro kritickou komunikační síťovou infrastrukturu využití plně manažovatelných síťových prvků, které umožňují ovlivnit šíření a směrování toků informací v síti. Právě obecná možnost ovlivňování toků informací je vlastnost, která je využívána pro zajištění vyšší bezpečnosti komunikačního řešení. Řádné projekční navržení fyzické a logické komunikační síťové topologie s následným nastavení komunikačních a bezpečnostních pravidel výrazně ovlivňuje odolnost proti kybernetickým hrozbám dané komunikační infrastruktury jako celku.

Společnost COLSYS – AUTOMATIK, a.s., využívá svých letitých zkušeností a pomáhá zákazníkům s projekčním návrhem a realizací nejen bezpečnostních funkcí síťové infrastruktury. Při volbě aktivních síťových prvků využívá produktů německé společnosti HIRSCHMANN, které je COLSYS – AUTOMATIK, a.s., zároveň i technickým partnerem v regionu střední Evropy. Síťové prvky HIRSCHMANN jsou známé zejména svojí spolehlivostí, která výrazně přispívá k provozní stabilitě celé infrastruktury. V nabídce jsou typické síťové prvky, jakými jsou L2/L3 switche, firewaly a routery v průmyslovém provedení, ale i zařízení pro průmyslovou bezdrátovou komunikaci a zařízení pro komunikaci přes veřejné sítě mobilních operátorů. Velmi důležitou částí návrhu a celého řešení jsou i monitorovací nástroje, které pomáhají identifikovat nestandardní chování komunikační infrastruktury a zajišťují dohled nad řádnou funkcí redundantních vlastností infrastruktury.

Každý zákazník přináší jinou bezpečnostní výzvu, kterou je nutné se zabývat individuálně. Jelikož neexistuje univerzální řešení, přichází na řadu zkušenost, která pomáhá vytipovávat kritické body a nasadit odpovídající technické řešení. Například se výrazně odlišují principy řešení pro jednotlivé typy zákazníků v odlišných segmentech průmyslu. Často řešeným tématem je zabezpečení existujících systémů proti kybernetickým hrozbám, u kterých již mnohdy nemusí být úplně snadné povýšit jejich vlastní zabezpečení.

Neustálý vývoj systémů řízení technologických procesů, integrace myšlenek Industry 4.0 a rozvoj Smart zařízení, dělá z průmyslové kybernetické bezpečnosti cyklický proces, který přináší nová témata a vyzývá ke kreativnímu přemýšlení.

HIRSCHMANN
A BELDEN BRAND

COLSYS-AUTOMATIK, a.s.
Huťská 1294, 272 01 Kladno
Tel.: +420 312 285 312
E-mail: info@colaut.cz

www.colaut.cz

Conference Speakers

Mr. Tomáš BÁRTA
Channel Sales Executive, VERACOMP, Czech Republic

For the past 15 years Tomas has been working in the field of information technology and information security especially as a consultant and sales manager in the field of security solutions at various levels. He has gained experience with solutions and security products on the side of the customer, at the system integrator, value add distributor in the field of security technologies and on the side of the solution manufacturer against cyber threats. While working as a business manager and consultant for security solutions and preparing these solutions together with security and technology experts, he also concentrated on the "reverse" part of the solution, which is training and education of users at various levels, including expert training for security technology administrators education, awareness and safety awareness of the users themselves.

1 + 1 = 3 : Joining forces for greater security of the inseparable worlds of IT and SCADA / ICS and IoT
Current technological trends are more and more connecting the previously ostensibly incompatible worlds of IT, OT, IoT and SCADA, and with respect to increasing risks and increasing numbers of cyber threats in all these areas, it is no longer enough to have an universal magic box or isolate the environment. It is necessary to have complete and complex knowledge and control and proactively protect each and individual potentially vulnerable asset of the connected world, taking into account the specifics of each area. As an independent distributor with a team of experts, we seek and provide the most appropriate solutions to protect all connected assets, an control of these assets, including visibility of the environment from the world's leading cyber security vendors with respect to minimizing connected world risks including necessity of education of users.

Mr. Jan BENEŠ
Safetron, Czech Republic

5G Technology

Dr. Bernhards BLUMBERGS
CERT.LV, Lead Cybersecurity Expert, Advisor to BHC Laboratory, Latvia

Weekend Warrior: Attacking the Future SCADA Now

Mr. Miroslav BRVNIŠŤAN
President, Slovak AFCEA or AFCEA EUROPE, Slovakia

2nd Conference Day Opening – SCADA Security as a part of security organization

Mr. Jan DIENSTBIER
Vice President, ČIMIB, Czech Republic
Moderator: ICS (SCADA) Security for C-Level

Connected World – technical, business and legislative aspects - PANEL DISCUSSION

Ing. Rostislav DOUBEK
Offensive Security Team Member, Corpus Solutions, a.s., Czech Republic

- Offensive security team member at Corpus Solutions a.s.
- Over 15 years of cyber security experience
- Practical experience in implementing technology application delivery
- Practical experience in implementing technology WAF
- Practical experience in implementing security technologies for IT and OT
- Practical experience in implementing, detecting and managing cyber attacks
- LAB co-author for training concept, implementation of SCADA elements
- Cyber Defense Academy training concept lecturer
- Cyber Security Instructor for IT and OT staff
- Working for major clients in the Czech Republic (ČSOB, KB, CNB, ŠKODA AUTO…)
- Work for important clients from abroad (training, presales, LABs for demonstration of cyber attacks and security technologies)
- CEH certificate holder, pentester
- Has received training at CyberGym Israel
- Participant in conferences and offline CTF events (Krakow, Prague, Hanoi, Tel Aviv)

Cyberattack in Industry 4.0 and its defence
Presentation of the typical SCADA / ICS infrastructure with all typical features of such customer environments. Possible pitfalls and possibilities of exploiting weaknesses to control the system will be pointed out. Subsequently, we will present modern approaches to defense.

Nový přístup k zabezpečení SCADA sítí

Již dávno totiž neplatí, že bezpečnost průmyslových sítí a systémů zaručuje jejich izolace od vnějšího světa v rámci tzv. ostrovních instalací. SCADA systémy jsou dnes i dvacet let staré, z mnoha důvodů neaktualizované a tedy nezabezpečené. Přechod na tradiční síťovou komunikaci a propojování v minulosti striktně oddělených systémů s komerčním IT, vystavuje prostředí SCADA velkému bezpečnostnímu riziku a otevírá nové příležitosti pro útočníky. Detekce nežádoucího chování v síti je nutným a univerzálním způsobem, jak posílit zabezpečení SCADA systémů a s nimi souvisejícího IoT.

Síť představuje společného jmenovatele v jinak heterogenním prostředí systémů SCADA, které se liší nejen napříč obory, ale dokonce i mezi jednotlivými podniky. K podchycení nových bezpečnostních rizik je proto vhodné zavést další vrstvu kontroly na úrovni sítě. Vycházíme přitom z předpokladu, že pokud dokážeme porozumět běžnému chování v síti, budeme zároveň umět odhalit nežádoucí chování, probíhající útok nebo jiné anomálie, které se od běžného provozu odlišují. Dobrým příkladem je škodlivý kód Black Energy, který stál v roce 2015 za napadením ukrajinské rozvodné sítě. Existují však i běžnější kybernetické hrozby cílené na organizační síťovou infrastrukturu, jako jsou například botnety (infekce botem). Bez vhodné monitorovací technologie jsou podobné hrozby pro administrátory v podstatě neviditelné.

Absence šifrované komunikace, chabý autentifikační mechanismus a nejasný perimetr daný podstatou IoT činí prostředí SCADA / ICS značně zranitelné vůči současným kybernetickým hrozbám. Přechod na komunikaci založenou na protokolu IP znatelně ztížil ochranu sítě a vytvořil z ní novou výzvu pro všechny bezpečnostní odborníky. Na druhou stranu nabízí tato situace důležitý zdroj informací pro toho, kdo je dokáže číst. Implementace vhodné monitorovací technologie jako je FLOWMON na bázi datových toků do bezpečnostního rámce umožňuje odhalit a reagovat na události ihned po jejich vzniku.

Tradiční monitoring zastoupený protokolem SNMP (Simple Network Management Protocol) poskytující přehled o IT infrastruktuře, považuje spousta síťových administrátorů za nezbytný. Sám o sobě však nedokáže nahlédnout do datového provozu, nemá informace o jeho struktuře a tím pádem je pro bezpečnostní monitoring nepoužitelný.

Omezení protokolu SNMP překonává až tzv. monitorování datových toků. Tato technologie pro moderní monitoring síťového provozu poskytuje detailní statistiku o síťové komunikaci ve formě IP toků (NetFlow v5/v9, IPFIX). Z analýzy síťové komunikace totiž získáme kompletně jiný pohled na monitorovanou IT infrastrukturu, takže dokážeme automaticky identifikovat infikované stanice, nežádoucí síťový provoz nebo aktivity uživatelů, útoky a obecně anomálie provozu datové sítě. Tzv. behaviorální analýza sítě (Network Behavior Analysis) je schopna, na rozdíl od systémů založených na signaturách, jako jsou antivirové programy, odhalit i nové nebo dosud neznámé hrozby a útoky.

Mr. Vladimír DZURILLA
Prime Minister Advisor, Chief Digitial Officer, Government of the Czech Republic, Czech Republic

Czech Digital Agenda

Mr. Martin FABRY
Owner & Cybersecurity Consultant, Accura s.r.o.

Current and Future Cyber Threats – protect your SCADA system - PANEL DISCUSSION

Threat Monitoring in SCADA ICS

What is important to monitor in SCADA ICS? Why passive monitoring is important and what are the criteria for choosing the right continuous threat detection tool, a description of the different network environments and ICS and DCS architectures, and the latest trends in SCADA ICS monitoring.

Dr. Eva FIALOVÁ, LLM., Ph.D.
Institute of State and Law of the Academy of Sciences, Czech Republic

Connected World – technical, business and legislative aspects - PANEL DISCUSSION

Mr. Jiří GOGELA
Member, Czech Cyber Security Working Group, Cyber Expert, Trend Micro, Czech Republic

Research on vulnerabilities of remotely controlled industrial equipment

---

Mr. Serhii HALAHAN
Chief Information Officer, NPC UKENERGO

UKENERGO experience in counteracting cyber-security strikes

SCADA as an element of IT environment for the transmission system operator, ways to ensure effective communication with transmission networks; Operational day-to-day functionality, maintenance and; development of business processes automatization by means of SCADA; Modern risks, challenges and threats of SCADA application; UKENERGO experience in counteracting cyber-security strikes

---

Mr. Terry HALVORSEN
Executive Vice President, Samsung Global 5G, USA

Expert Opening Speech

Mr. Karel HAVLÍČEK
Minister, Ministry of Industry & Trade, Czech Republic

Opening Speech – Industry 4.0 – Artificial Intelligence – 5G Strategy

---

Mr. Dettmer HENDRIK
Head of IoT Security Lab, TÜV TRUST IT GmbH, Austria

Current and Future Cyber Threats – protect your SCADA system - PANEL DISCUSSION

Mr. Petr JIRÁSEK
Chairman, Czech Cyber Security Working Group, AFCEA, Czech Republic
Moderator: ICS (SCADA) Security for MILINT; Modern Communication Systems, Future Networks – 5G, Cyber Security and SCADA/ICS

Closing Remarks

#ICTBLOG

SVĚT TECHNOLOGIÍ V SOUVISLOSTECH

PŘÍPADOVÉ STUDIE
INFRASTRUKTURA
BEZPEČNOST
TRENDY

WWW.ICTBLOG.CZ

Mr. Jiří KASNER

Chairman of the Board, COLSYS – AUTOMATIK, a.s., Czech Republic

Certificates

- UCLES FCE A (2004) – CEFR C1,
- CZ Civil aviation authority – state authorized professional inspector (2009 – 2015),
- chartered engineer (Czech chamber of chartered engineers) – (since 2009),
- HIRSCHMANN certified network professional.

Standardization and procedures in design of critical communication infrastructure

COLSYS – AUTOMATIK, a.s., provides critical communication infrastructure (CCI) design and complete solution delivery for more than 20 years. Major projects are based on hard industry applications.

We focus on redundant systems with maximum reliability, providing secure and safe solutions, but still being most transparent for all CCI communication participants. Correctly, well designed and implemented CCI brings also a security enhancement for all communication layer – this means PLC level (control level), decentral I/Os, actuators, SCADA layer and, at the end, HMI related controls.

Having well designed, well configured and well implemented CCI with appropriate components is the basic for having CCI for any mission critical application.

Our presentation will try to show you, how to proceed, how to solve basic problems – to get reliable CCI at the end.

Mr. Pavel KLIMEŠ

Director, Security Products Development, Corpus Solutions, a.s., Czech Republic

- Security Product Development Director at Corpus Solutions a.s.
- Head of the Offensive Security team at Corpus Solutions a.s.
- Defines effective cyber defense strategies for customers
- Practical experience in the implementation, detection and management of cyber attacks
- Author of the Cyber Defense Academy training concept
- Cyber security lecturer for IT and OT staff
- 21 years of experience in cyber security
- Works for major clients in the Czech Republic (ČSOB, KB, CNB, ŠKODA AUTO…)

Cyberattack in Industry 4.0 and its defence

Presentation of the typical SCADA / ICS infrastructure with all typical features of such customer environments. Possible pitfalls and possibilities of exploiting weaknesses to control the system will be pointed out. Subsequently, we will present modern approaches to defense.

Mr. Robert KOMINKA

ICS Security Expert, Corpus Solutions, a.s., Czech Republic

- 9 years of experience in industrial automation (PLC, SCADA, MES) on international projects (heavy industry, transportation, mining, manufacturing, automotive)
- ICS Security Specialist at Corpus Solutions a.s.
- Experience in defining technology roadmaps and security analysis for critical infrastructure, ICS penetration tests, Embedded devices
- Creator of SCADA Labs, Malicious Toys, Scripts and Industry Tools 4.0
- Practical experience with tools for the detection of operational / security incidents in ICS using elements of AI
- Cyber Security Instructor for IT and OT staff
- Working for major clients in the Czech Republic (ČEZ, PP, MERO, ŠKODA AUTO…)
- Work for important clients from abroad (training, presales, LABs for demonstration of cyber attacks and security technologies)

Cyberattack in Industry 4.0 and its defence

Presentation of the typical SCADA / ICS infrastructure with all typical features of such customer environments. Possible pitfalls and possibilities of exploiting weaknesses to control the system will be pointed out. Subsequently, we will present modern approaches to defense.

Jak vypadá informační bezpečnost v České republice?

Níže uvedené grafy a texty shrnují vybrané výsledky průzkumů a analýz provedených bezpečnostními specialisty ALEF v rámci přípravy zprávy ALEF Security Report 2019. Plné znění této zprávy, shrnující vývoj ve vybraných oblastech informační bezpečnosti v České republice v posledním roce, můžete nalézt na webových stránkách společnosti ALEF na www.alef.com.

Bezpečnostní vzdělávání v roce 2018

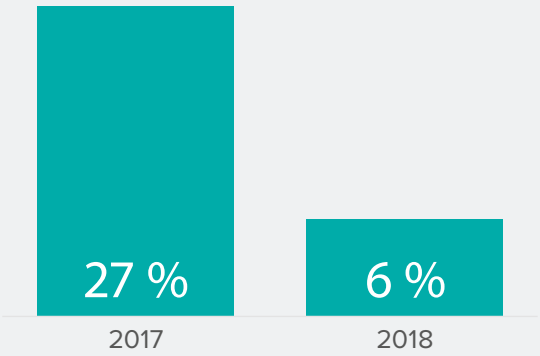
34 %

Dle odpovědí respondentů v průzkumu ALEF nezajišťovalo v roce 2018 více než 34 % dotazovaných organizací žádnou formu bezpečnostního vzdělávání svých zaměstnanců.

38 %

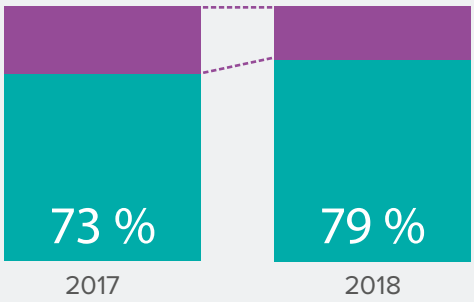
Téměř 38 % dotazovaných organizací realizovalo v roce 2018 phishingové testy svých zaměstnanců.

Vývoj zájmu o bezpečnostní služby spojené s GDPR



Zájem o bezpečnostní služby spojené s GDPR v roce 2018 citelným způsobem poklesl. V roce 2017 tvořily tyto služby přes 27 % všech poptávaných bezpečnostních služeb, v roce 2018 pak pouze tvořily necelých 6 % z nich.

Automatické transparentní šifrování e-mailu



Z dostupných dat z e-mailových bran vyplývá, že v roce 2018 došlo k rozšíření podpory oportunistického TLS šifrování. Zatímco v roce 2017 bylo s pomocí TLS šifrováno necelých 73 % příchozích zpráv, v roce 2018 to bylo již téměř 79 %.

Z dat společnosti Cisco týkajících se globální bezpečnostní situace vyplývá, že 62% phishingových simulací realizovaných organizacemi vedlo k získání přihlašovacích údajů alespoň jednoho uživatele.

Dle dat společnosti F5 využívají útočníci phishing podstatně častěji v období předcházejícím vánočním svátkům – v roce 2018 byly počty detekovaných phishingových útoků v posledním kvartálu o více než 50% nad průměrem.

Trust the Strong
www.alef.com

ALEF

Mr. Jan KOPŘIVA
Coordinator – Computer Security Incident Response Team (CSIRT), ALEF NULA, Czech Republic

Jan Kopřiva is the team leader of ALEF CSIRT, a professional security incident response team within ALEF NULA. Before joining ALEF, Jan worked in both academia and commercial sector and was involved with projects focused on implementation and testing of applications, proprietary hardware development and information security. His main focus lies in security monitoring and incident response, penetration testing and other areas of security which traditionally fall within the purview of "purple" teams. He is an author of a number of research papers and articles focused on different aspects of cyber security and he regularly speaks at security conferences, both domestic and international. He is also an Incident Handler in the renowned SANS Internet Storm Center.

ICS accessible from the Internet = bad (and very common) practice
Although connecting ICS systems directly to the Internet is generally recognized as inappropriate and dangerous, this practice is relatively common. ALEF CSIRT periodically monitors the number of internet-connected ICS devices, both on global scale as well as in specific countries. In this presentation, we will go over the trends in the numbers of ICS devices connected to the internet in Czech Republic and in other countries of the world and we'll take a look what specific Industrial Control Systems are, or were, out there and discuss what a successful attack on these devices could potentially result in. We will also take a look at how easy it is to discover ICS devices on the internet using commonly accessible tools.

Assoc. Prof. Zdeněk LOKAJ
Academic Expert, Czech Technical University in Prague, Czech Republic
Moderator: Industry 4.0 – Connected World, Mobility and IoT; Connected World – technical, business and legislative aspects - PANEL DISCUSSION

Col. Daniel MIKLÓS
Fire Rescue Service of the Czech Republic, Czech Republic

Involve IOT technologies into Civil Protection Services

Mr. Pavel MINAŘÍK
Chief Technology Officer, Flowmon Networks, Czech Republic

As Chief Technology Officer at Flowmon Networks, Pavel Minarik is responsible for research and university cooperation, product strategy and long term technology roadmap as well as technical support and customer projects worldwide. With background in theoretical informatics Pavel works in the area of network traffic monitoring & cyber security since 2006. He has participated in several research projects (2007-2010) as a senior researcher of Institute of Computer Science of Masaryk University. He is the author of more than ten publications in the domain of behavior analysis and several algorithms for traffic processing and anomaly detection summarized in PhD thesis "Building a System for Network Security Monitoring".

Network monitoring and anomaly detection in ICS/SCADA
Operational Technology (OT) and Information Technology (IT) are merging. OT systems have lived for years totally isolated and now they should be connected to enterprise networks or the internet. The lack of security measures in this environment, where availability and integrity will return us back in time, means we will have to deal with the very same issues that experienced IT professionals solved 20 years ago. The OT environment is very fragile and placing invasive monitoring or security tools such as intrusion prevention systems or antiviruses is close to impossible. Therefore, security measures are usually limited to firewalls being deployed on the perimeter of the OT environment leaving all the internal traffic as a blind spot. Main focus of the presentation is to show how passive network monitoring can be adopted and utilized in ICS/SCADA environment to provide in-context and in-depth understanding of both normal traffic and network anomalies in terms of incident magnitude, impact and root cause.

Mr. Tomáš MÜLLER
President, AFCEA Czech Chapter, Czech Republic
Moderator: Opening Session

Welcome Speech
ICS (SCADA) Security for MILINT - WORKSHOP
Protect our business against SCADA attacks - WORKSHOP
Closing Remarks

Mr. Dušan NAVRÁTIL
Director, National Cyber and Information Security Agency, Czech Republic

Opening Speech

Můžete být SCADA, můžete být i **bezpeční!**

Je zřejmé, že s každou technologickou platformou nebo konceptem často zapomínáme na základy. Každý odborník na informační bezpečnost ví, že základními pilíři jeho snažení jsou důvěrnost, dostupnost a integrita. Pokud se zaposloucháme do některých přednášek o bezpečnosti ve světě ICS/SCADA, třeba na letošní konferenci, zjistíme, že některé „nové" pohledy tento přístup opouštějí. Že by byl zastaralý? Není.

Základem ochrany jakýchkoliv procesů nebo služeb je vždy to samé. Na ose událostí, vedoucí od prevence přes různé více či méně bolestivé peripetie k obnově, je třeba vždy pečovat o naše tři známé: důvěrnost, dostupnost a integritu.

Svět SCADA systémů není výjimkou. Důvěrnost dat o architektuře, procesech, zranitelnostech, některých protokolech, ochrana vlastního obsahu, a podobně – to jsou všechno informace, které je třeba klasifikovat, monitorovat, řídit jejich životní cyklus. Je to těžké? Je. Je to možné? Ano, je. Často jde o data, jejichž významu většinou běžný IT expert ne zcela rozumí. Svět důvěrnosti dat v řídících a dohledových systémech je komplikovaný a často má nepříznivý dopad na další z oněch tří pilířů, kterým je dostupnost.

Dostupnost se na planetě SCADA bohužel týká nejen informací, statických nebo dynamických dat, ale i dostupnosti procesů, služeb, znalostí, lidí a dalších aktiv. Proto je dostupnost dat součástí balíčku „must have" a je často stavěna nad důvěrnost a integritu. Skutečný problém nastává, pokud útočník udeří na zranitelnost důvěrnosti dat a následně využije získané informace k útoku na jejich integritu. Třetí pilíř – dostupnost – pak většinou spadne sám. Pokud nespadne, vzdá se ho řízeně uživatel systému v reakci na nedůvěryhodnost výstupů a neschopnost systému věřit.

Útok na integritu může mít dopady ne první pohled neviditelné. Parametrické úpravy, drobné úpravy konstant nebo zavlečení nových členů do algoritmů mohou způsobit, že vybraný ovládací prvek provádí požadované akce se zpožděním, chybným počtem opakování, nebo jen neposkytne o jejich provedení informaci.

Současný tlak na plnou automatizaci bezpečnosti ICS/SCADA je pochopitelný. Většina plně automatizovaných detekčních systémů však cílí dominantně pouze na jednu část triády důvěrnosti/integrita/dostupnost. Některé jsou navíc konceptuálně založené na fikci snadného a trvalého bezpečného oddělení OT a IT prostředí. Existuje řada solidních bezpečnostních SCADA technologií, avšak žádná z nich nefunguje tak, že se „zaklapne" do racku nebo na lištu a provoz se přepne na bezpečnost.

Testovali jsme a testujeme řadu průmyslových bezpečnostních technologií. Všechny, i ty nejlepší z nich jsou k ničemu, pokud není jejich nasazení správně navrženo, provedeno a jejich provoz řízen v kontextu správy všech aktiv organizace.

Svět SCADA může být bezpečný. Nikdy ale nebude bezpečný v organizaci, která neřídí svou bezpečnost komplexně. Pravděpodobně nikde na světě neexistuje firma nebo instituce, která by byla schopna zajistit bezpečnost svých SCADA aktiv jako bezpečného ostrova uprostřed moře improvizace a intuitivních rozhodnutí.

Můžete být SCADA, můžete být i bezpeční. Nemůžete ale být „SCADA ONLY" bezpeční. My bezpečnosti rozumíme. Rádi pomůžeme i Vám jí porozumět.

Martin Uher
CyberG Europe, a.s.

Mr. Lukáš OBOŘIL
Head of Control Systems Department – Software, IC Energo, a.s., Czech Republic

Expert Session Opening

Mr. Petr OČKO
Deputy Minister, Ministry of Industry & Trade, Czech Republic

Opening Speech

Mrs. Barbora PÁLKOVÁ
CNP & Strategy Dept., Fire Rescue Service of the Czech Republic, Czech Republic

Protect our business against SCADA attacks - WORKSHOP

Mr. Miloslav PAVELKA
O2 Czech Republic / TeskaLabs, Czech Republic

C-ITS security solution in C-ROADS Czech Republic project

Mr. Jaroslav PEJČOCH
Vice Chairman, Czech Cyber Security Working Group, Czech Republic
Moderator: Protect our business against SCADA attacks - WORKSHOP

Mr. Tomáš PLUHAŘÍK
Czech Republic

How to make 5G trustworthy technology

Dr. Josef PROKEŠ
Vice Chairman, Data Protection Office of the Czech Republic, Czech Republic

Connected World – technical, business and legislative aspects - PANEL DISCUSSION

Mr. Tomáš PŘIBYL
CEO, Corpus Solutions, a.s., Czech Republic

- Founder and CEO of Corpus Solutions a.s. (in 1992);
- has been involved in cyber security since 1996;
- founder of the first training cyber arena in the Czech Republic (Israeli concept);
- Member of AFCEA (Member of Cyber Security Working Group);
- Member of the competition committee of the secondary school cyber competition seeking new talent in the cybersecurity area;
- Member of the 21st Century Security Platform for Cyber Security;
- lecturer on cyber defense at international conferences organized by AFCEA.

General Partner Speech
Current and Future Cyber Threats – protect your SCADA system - PANEL DISCUSSION
ICS (SCADA) Security for C-Level - WORKSHOP

Mr. Vladimír ROHEL
Security Director, National Agency for Communication and Information Technology, Czech Republic

What will be the critical infrastructure of tomorrow?

Awareness of operational technology (OT) and critical infrastructure system security is rising

OT refers to the hardware and software used to run industrial control systems (ICS), such as SCADA, that serve as the foundation of various areas of critical infrastructure. This includes industries that are essential to public safety and well-being, including power plants, manufacturing, water utilities, healthcare, transit, and more. OT differs from traditional IT systems due to the processes and systems that must be incorporated to effectively manage production and resource development systems, including engines, valves, sensors, and even robotics, that are common to critical infrastructure environments but may be absent from traditional IT stacks. While IT and OT have been managed separately since their inception, there has been a growing movement toward the convergence of these two systems.

IT / OT Convergence and Cybersecurity

This IT/OT convergence can affect the cybersecurity posture of critical infrastructure, especially given the impact that downtime caused by a cyberattack can have on the economy, health, and productivity of the nation. And worse, the potential safety risks to workers and even local communities should a critical system be compromised.

OT system managers are rightly concerned about the impact of IT/OT convergence, which is one of the reasons why OT networks were historically air-gapped in the first place. Such an approach limited attack surface concerns, since the OT environment didn't extend to external networks. OT environments converged with IT are not only highly susceptible to traditionally IT-focused cyberattacks but also vulnerable to basic IT functions like the active scanning of network devices, which can disable a primitive device or, worse, bring an entire system down.

The proper approach to securing OT environments, therefore, is to build security directly into the network architecture to ensure that the preservation of safety and system availability are paramount. While this resembles a traditional security strategy approach, it requires specialized solutions and strategies adapted to OT's unique requirements.

Layered Segmentation with a Multi-Factor Authentication

To control access, organisations needs to implement layered segmentation with a multi-factor authentication scheme, which is crucial, especially in a critical manufacturing domain where the network architecture spans multiple lines of production. This approach defeats the ability to cause harm, either directly or indirectly, through malware propagation to any areas outside of the immediate zone of control.

How to address OT Threats

Implementing an active network defense is critical, not only to defend against bad actors but to also protect delicate, high-valued infrastructure from accidental damage caused by normal IT activities. It includes three steps:

1 - Address known and reasonably expected threats by applying secure gateways at the edges of the OT network, and then implementing signature-based solutions to recognize and stop known threats. However, care must be taken to identify and implement solutions that are fluent with or support OT protocols, applications, devices and processes.

2 - Address unknown threats begin by defining the attack surface and baselining normal activity in order to detect behaviors that are either zero-day, existing malware you've not seen before, operator errors or coerced actions by a trusted operator.

3 - Trust assessments need to occur in real-time that enables the detection and analysis of malicious behaviors before they can affect live operations.

At-speed Recognition and Real-Time Network Security Analysis

Across any OT network architecture, accomplishing at-speed recognition of any known malicious code, unknown code or irregular instruction is imperative. The ability to detect, analyze and neutralize any potential threat depends upon real-time analysis of all the instructions that are being executed.

Real-time event analysis affords consistent protection regardless of intent. It is impartial and affords detection through at-speed analysis that protects against well-orchestrated attacks, as well an operator who carelessly commits an error while executing OT processes. This approach disregards assumed trust and instead seeks to protect the highly valued assets of the OT system and the enterprise.

Understandably, awareness of operational technology (OT) and critical infrastructure system security is rising. The journey to protect and secure OT systems is well under way but requires both vigilance and the recognition of the need to build in security. The ability to implement security solutions that deliver visibility, control and real-time situational awareness are the differentiators enabling safe and more efficient operations.

Author: FORTINET, Jan Vaclavik, Systems Engineer, CEE

Mr. Petr ROUPEC

CEO, Bohemia Market CZ, Czech Republic

Petr holds a degree in Industrial Automation from the EIT Institute Australia and has worked in several roles within the automation business.

He had assignments that ranged from small machinery automation up to designing and commissioning control systems for refineries and power stations.

With several decades of hands-on experience, he led an international team that designed the electrical & controls systems for a Nuclear Power station in Europe from 2009 to 2015.

Petr has ample experience with Distributed Control Systems and related underlying technologies, such as networking.

His skills and experience in engineering management and running an industrial service organization allowed him to build his own company, Bohemia Market, that provides comprehensive engineering services for customers around the world.

Pioneers on the power generation industry have trusted Petr and Bohemia Market on providing state of the art support to the existing industrial facilities, which suffer from poor OEM support and to attenuate the high costs that come with fast electronic products obsolescence.

This obsolescence of high-value operational control systems and the current cybersecurity threads led him to design the Bohemia Market cybersecurity handbook for industrial facilities.

One way data transfer. Entirely secure. Unlimited Tags.

Connecting any strategic infrastructure to the Internet makes it vulnerable to security threats. Learn how to establish the cybersecurity perimeter out of a single box.

Mr. Vladimír SEDLÁČEK

Technical Director, GREYCORTEX, Experienced Developer, Analyst, Certified Ethical Hacker, Certified Livewire Investigator, Czech Republic

Vladimír Sedláček is an experienced developer, analyst, and administrator who has worked on a broad array of projects, including connecting diverse systems and developing a secure web platform and infrastructure for more than 100 million clients. His passion for electronics, cyber-security and hacking has led him, among other things, to pass the Certified Ethical Hacker and Certified Livewire Investigator exams. He brings this experience to GREYCORTEX, where he works as CTO, and leads the development department.

New approaches to detection of SCADA threats

Modern control systems include more and more digitally interconnected devices, covering an ever larger area. This infrastructure increasingly uses elements borrowed from IT networks; not only for data collection, but also for precision tasks. Originally, systems were secure because they didn't connect to the Internet. Today, systems are open to, and communicate across the Internet; but equipment and transmission security is treated as secondary to core functionality. Detecting and combating modern threats in control systems is a multi-layered challenge, connecting the world of OT and IT.

Mr. Tobias SCHROEDEL

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 and is working for the German Chamber of Commerce as an auditor of soon to be IT -specialists for over a decade.

Heartbeat to hell

The story of hacking a pacemaker. Two IT security specialists analyzed pacemakers and found some vulnerabilities. Tobias has received first hand information on this attack and is going to share them with us in his presentation. No matter, if you have a pacemaker or not. your pulse will rise, when you see, what's possible - and what the prupose behind the research finally was.

ICS (SCADA) Security for C-Level - WORKSHOP

Mr. Ladislav STRAKA

Managing Consultant at Service & Support, Czech Republic

Ladislav serves as a Managing Consultant at Service & Support, specializing in Systems and Security Management solutions. For more than 20 years of his professional career he managed teams designing and implementing enterprise scale management systems aiming to bring real business value to its customers. Long term collaboration with Utility customers also brought him a lot of challenges in field of Security & Operation for SCADA systems. Receiving itsmF and CACIO awards last years confirms his innovative approach trying to solve actual issues today's CIOs are fighting with.

Big Data in ICS

Splunk for IoT and SCADA systems

SCADA systems used to be a closed platform up until the recent past. That is not the case now as these systems are no longer separated

Samsung Electronics Manufactures End-to-End 5G Hardware Systems

-Security is at Samsung's Core-

For more than 35 years, Samsung has been a leader across the mobile industry, from chipsets to network solutions to smartphones. Over the past decade, the company's dedication to pushing boundaries has paved the way to the development of the world's first end-to-end 5G solution. Samsung designs and manufactures all the parts integral to 5G: chips, network equipment, access units, CPE's and hand held devices—all with industry-leading security. Because of Samsung's controlled design and manufacturing environment it can deliver unrivaled equipment interoperability and security assurance. No other company can deliver this end to end, secure 5G ecosystem with a trusted global supply chain. Guaranteeing trust in its products and services is Samsung's top priority, and the company is committed to working with its business partners and governments customers around the world to maintain leadership in this area.

The need for increased mobility and connectivity raises threats to security and data protection, and Samsung is committed to assuring the security of its products that government customers rely upon to execute their important missions. Ensuring a high-level of protection for devices and information is crucial. SAMSUNG KNOX™, an unrivaled industry-leading security platform, is deployed on all our 5G products and across all connected devices. SAMSUNG KNOX™ provides defense-grade, government certified security for even the most demanding requirements, and is flexible to accommodate users from any industry. Only Samsung has complete security architecture for hardware, OS and application layers, and is verified as the highest-level security solution by governments and organizations (GSMA, Gartner, MDFPP, etc.) worldwide. Samsung is also in close collaboration with the security research community, and collaborates with the most advanced security intelligence companies in the world to provide unrivaled secure communication networks.

Samsung has the expertise to develop custom solutions for our government customers, and can provide the right speed, distance, form factor, mobility features and power ranges to meet many specialized needs. Samsung is committed to building customer trust through open partnership with the security industry and close collaboration with its business partners. As the recognized worldwide leader in 5G ecosystem solutions, Samsung will work with governments and in-country partners to create secure, 5G network solutions that meet their needs.

SAMSUNG

from other networks. SCADA is being linked with other information systems within the same organisation, with systems of contractors and with systems outside of the reach of SCADA administrators. A topic very closely connected to this fact is the Security of SCADA systems. SCADA systems are typically highly customized with many proprietary elements, subsystems, specific means of data transfer and processing.

It is therefore crucial that the SIEM itself is easily customizable and able to ingest, process and evaluate a wide range of data types coming from the many proprietary systems. Splunk as a platform operating on the principle of "Data-to-Everything" natively meets these requirements, being a Big Data solution right from the start. Splunk is thanks to its openness in terms of processing both structured and unstructured input data an ideal platform for IoT. Due to its robustness and highly scalable nature it is able to ingest vast amounts of data. This makes it fully involved in Industry 4. 0.

Splunk integrates previously separate areas – Operations, Security and Business. Various forms of data processing, evaluation, visualization and subsequent actions are used according to specific needs of individual departments of the organization.

Assoc. Prof. Radomír ŠČUREK
Deputy Head, Department of Security Services, Faculty of Safety Engineering, Technical University of Ostrava, Czech Republic

Protect our business against SCADA attacks - WORKSHOP

Mr. Jozef ŠEREG
The Prague Public Transit Co. Inc., Czech Republic

Mr. Aleš ŠPIDLA
President, ČIMIB, Czech Republic
Moderator: Current and Future Cyber Threats – protect your SCADA systems; Current and Future Cyber Threats – protect your SCADA systems - PANEL DISCUSSION

Mr. Kamil TICHÝ
Ministry of Defence of the Czech Republic, Czech Republic

Current and Future Cyber Threats – protect your SCADA system - PANEL DISCUSSION

COL (RET.) Martin UHER
CEO and Chairman of the Board, CyberG Europe a.s., Czech Republic

He successively studied measurement and automation technology, communication, and pedagogy. During his army service he worked in the field of specialized electronics. He later dedicated his career to electronic devices construction and worked subsequently as cyber security manager and diplomat. He is ranked among the founders of European Cyber Security Excellence Center and keeps lecturing at various universities.

Moderator: New Technological Trends in ICS Security

Opening Speech – New addictions as a source of new threats - PANEL DISCUSSION

Connected World – technical, business and legislative aspects - PANEL DISCUSSION

Mr. Jan VÁCLAVÍK
Systems Engineer, Fortinet, Czech Republic

Jan Václavík graduated in Technical Cybernetics at FEE-CTU in Prague and currently works for Fortinet as Systems Engineer for CEE region. He has been working in the area of computer network security for more than 8 years and has gained a lot of theoretical and practical experience. His extensive knowledge of network security and pre-sales support is appreciated by many customers and partners. In his work he focuses, among other things, on the general presentation of the importance of the concept of computer network security.

SCADA Systems as Target of Cyber Attacks

Current and Future Cyber Threats – protect your SCADA system – PANEL DISCUSSION

Mr. Jan VYKOUKAL
Head of Department, Ministry of Interior, Czech Republic

Protect our business against SCADA attacks – WORKSHOP

GREYCORTEX MENDEL

Pokročilá ochrana operačních technologií

Ing. Vladimír Sedláček
Technický ředitel GREYCORTEX

Proč je potřeba se zabývat bezpečností OT sítí?

Útočníci mohou napadením řídících systémů ve veřejné infrastruktuře, průmyslu a energetice (Operational technology, OT) způsobit obrovské škody například tak, že neplánovaně vypustí přehradu, způsobí blackout nebo převezmou ovládání průmyslového robota, který pak někomu ublíží.

Co pro zabezpečení OT dokáže GREYCORTEX udělat?

V době, kdy jsme začínali s vývojem našich produktů, neexistoval nástroj schopný detekovat napadení například skrze sociální inženýrství, ani “insider threats”. Tak jsme ho vyrobili. MENDEL dokáže velmi dobře analyzovat veškerý provoz v síti a maximalizovat viditelnost do sítě. Tím umožňuje síťovým analytikům provést hlubokou forenzní analýzu sítě a odhalit veškeré hrozby ať už známé, neznámé či pokročilé přetrvávající hrozby. Dokáže detekovat anomálie a vidí i to, co jiné nástroje odhalit v síti neumí nebo objeví příliš pozdě - když malware čeká na akci, my ho už monitorujeme. Využili jsme tedy těchto předností naší technologie a přenesli je ze světa IT také do světa operačních technologií. U našich zákazníků jsme zjistili, že IT a OT sítě mohou být úzce provázané, čehož se snažíme využít.

Jak takový produkt vypadá?

GREYCORTEX poskytuje pokročilé řešení pro analýzu síťového provozu, detekci hrozeb, sledování výkonu, forenzní analýzu a především hlubokou viditelnost do sítí. Jedná se o přehledný a snadno použitelný produkt, určený pro síťové analytiky a opravdové profesionály v oblasti síťové infrastruktury a bezpečnosti, kterým pomáhá rychle a detailně se dostat k původu anomálií a potenciálních hrozeb. MENDEL je ideální produkt pro střední a větší společnosti a instituce. Díky němu máte naprostý přehled o dění v IT i OT síti a pořádek v tom, co se vlastně ve vaší síti nachází. Tento nástroj navíc poskytuje prostor pro snadnou a přehlednou spolupráci mezi IT, OT a bezpečnostním týmem.

Jak je možné, že MENDEL řeší viditelnost do IT i OT sítí?

Původní automatizace byla provozována po desetiletí izolovaně, ale z technických a ekonomických důvodů, a také pro větší komfort, jsou dnes téměř všechna provozovaná zařízení propojována do IP sítí (I v IP znamená Internet), což je vystavuje vysokému riziku útoku.
Sice je teoreticky možné donést do rozvodny USB klíč, ale to je poměrně nepraktické a navíc jej někdo musí do něčeho zapojit. A to něco je zase počítač, ať už vypadá jakkoli. I když nejsou připojeny přímo k Internetu, “vzduchotěsné” systémy dnes prakticky neexistují, protože izolované zařízení nelze dálkově kontrolovat, diagnostikovat a spravovat. Tedy to není vhodné ani pro manažery. Bezpečnost je jako cibule a útočníci ji loupou slupku po slupce, proto je dobré o útocích vědět co nejdříve.

Čím je zabezpečení SCADA/OT od společnosti GREYCORTEX výjimečné?

Používáme v nástroji umělou inteligenci - MENDEL je schopen se sám učit vzorce typického chování v síti a model přizpůsobuje aktuální hodině v daném dni a týdnu (například v pátek v 15:00). MENDEL dokáže v síti přesně detekovat a vyznačit, kdo s kým komunikuje, kdy a s jakou časovou frekvencí. Dále vytváří modely pro všechna zařízení v síti, každou službu i subnet. V rámci SCADA sítí modeluje každou komunikaci mezi jednotlivými zařízeními a dokáže odhalit jejich anomálie. MENDEL samozřejmě pracuje také se specifickými signaturami známých útoků včetně našich vlastních detekčních metod, a dokáže tak bezpečně odhalit asi 400 typů útoků na zařízení OT.

Jaké technologie GREYCORTEX podporuje?

Zabýváme se zajištěním bezpečnosti a spolehlivosti především pro zařízení, pro která neexistují antiviry a často ani aktualizace. To je dnes velká část zařízení připojených do sítí a snad všechna průmyslová zařízení. Pro chytrý toustovač si ale naše řešení dnes nikdo nepořídí, proto se zaměřujeme na kritickou infrastrukturu. Ale v podstatě jde o veškerá zařízení využívající SCADA protokoly ve výrobě a přepravě produktů, látek, energie nebo v medicíně.

Jakým směrem se společnost GREYCORTEX v operačních technologiích dívá?

Tak jako u jiných technologií jde vývoj směrem vesmír - armáda - průmysl - konzumenti. GREYCORTEX přeskočil vesmír (aby se k němu později vrátil) a na úroveň armádních systémů je dnes stavěna také kritická infrastruktura. Aktuálně tedy směřujeme především do průmyslu 4.0, nicméně obecně lze odpovědět, že působíme všude tam, kam se zaměřují pokročilí útočníci a kde mají naši zákazníci co chránit.

Conference Partners

CORPUS SOLUTIONS a.s.

Štětkova 1638/18
140 00 Praha 4
+420 241 020 333
sales@corpus.cz
www.corpus.cz

Corpus Solutions je konzultační a technologickou společností, která se specializuje na oblast aplikované kybernetické bezpečnosti. Zákazníky systematicky vedeme k tomu, aby se naučili rozumět kybernetickým hrozbám, které ohrožují jejich business a dokázali na ně správně reagovat. Naše hodnota leží ve vysoce profesionálních službách, které se opírají o praktické zkušenosti z náročných prostředí a jsou poskytovány odborníky s dlouholetou historií v oblasti kybernetické bezpečnosti.

Corpus Solutions is a consulting and technology company specialising in applied cyber security. We systematically encourage our customers to understand and respond to cyber threats that endanger their businesses. Our value lies in the highly professional services that are delivered based on practical experience collected from diverse demanding environments by our experts with an extensive history in cyber security.

GENERÁLNÍ PARTNER / GENERAL PARTNER

FORTINET, organizační složka

Bucharova 2641/14, 158 00 Praha 13
+420 221 228 600
csr_sales@fortinet.com
www.fortinet.com

Fortinet (NASDAQ: FTNT) poskytuje zabezpečení největším podnikům, poskytovatelům služeb a státním institucím na celém světě. Vybavuje zákazníky inteligentní, vysoce účinnou ochranou proti všem druhům hrozeb, která je schopná vyhovět neustále rostoucím nárokům na výkon v neohraničených sítích – dnes i do budoucna. Pouze bezpečnostní architektura Fortinet Security Fabric dokáže poskytovat zabezpečení bez kompromisů na ochranu proti nejzávažnějším bezpečnostním rizikům v síťovém, aplikačním, cloudovém i mobilním prostředí. Společnost Fortinet je největším světovým výrobcem bezpečnostních zařízení z hlediska počtu dodaných kusů. Na její řešení spoléhá při ochraně svých podniků více než 415 000 zákazníků. Další informace naleznete na stránkách http://www.fortinet.com, v blogu Fortinet Blog a stránkách laboratoří FortiGuard.

Fortinet (NASDAQ: FTNT) secures the largest enterprise, service provider, and government organizations around the world. Fortinet empowers its customers with intelligent, seamless protection across the expanding attack surface and the power to take on ever-increasing performance requirements of the borderless network - today and into the future. Only the Fortinet Security Fabric architecture can deliver security without compromise to address the most critical security challenges, whether in networked, application, cloud or mobile environments. Fortinet ranks #1 in the most security appliances shipped worldwide and more than 415,000 customers trust Fortinet to protect their businesses. Learn more at http://www.fortinet.com, the Fortinet Blog, or FortiGuard Labs.

HLAVNÍ PARTNER / MAIN PARTNER

CHECK POINT SOFTWARE TECHNOLOGIES s.r.o.

Pobřežní 620/3
186 00 Karlín
+420 222 311 495
info_ee@checkpoint.com
www.checkpoint.com

Check Point Software Technologies Ltd. (www.checkpoint.com) je přední poskytovatel kyberbezpečnostních řešení pro vlády a organizace po celém světě. Chrání zákazníky před kyberútoky 5. generace prostřednictvím unikátních řešení, která nabízí bezkonkurenční úspěšnost zachycení malwaru, ransomwaru a jiných pokročilých cílených hrozeb. Check Point nabízí víceúrovňovou bezpečnostní architekturu, Infinity Total Protection s pokročilou prevencí hrozeb 5. generace, a tato kombinovaná produktová architektura chrání podnikové sítě, cloudová prostředí a mobilní zařízení. Check Point navíc poskytuje nejkomplexnější a nejintuitivnější nástroje pro správu zabezpečení. Check Point chrání více než 100 000 organizací všech velikostí.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading provider of cyber security solutions to governments and corporate enterprises globally. Its solutions protect customers from cyber-attacks with an industry leading catch rate of malware, ransomware and other types of attacks. Check Point offers a multilevel security architecture that defends enterprises' cloud, network and mobile device held information, plus the most comprehensive and intuitive one point of control security management system. Check Point protects over 100,000 organizations of all sizes.

GENERÁLNÍ PARTNER / GENERAL PARTNER

SAMSUNG ELECTRONICS

GLBLGOVinfo@samsung.com
www.samsung.com

Samsung Electronics is a worldwide leader in secure 5G and mobile solutions. We design, manufacture and deliver a complete 5G and mobile equipment ecosystem in a secure environment and controlled supply chain. Samsung partners with government agencies and enterprises globally to deliver secure hardware/software solutions to help achieve their critical missions.

HLAVNÍ PARTNER / MAIN PARTNER

BOHEMIA MARKET CZ, s.r.o.

Světlice 118
396 01 Humpolec
Czech Republic
+420 565 533 729
sales@bohemiamarket.com
bm.company

Firma Bohemia Market poskytuje komplexní inženýrské služby zákazníkům po celém světě. Od aktualizace a modernizace HMI systémů, až po návrh a dodání sofistikovaných

CYBER SECURITY

Do you think your Power Plant is protected because you have firewalls? **Think again.**

We live in a world of automation and data exchange. IIoT and Industry 4.0 are hot topics right now, but the most basic affair remains: as more and more things get connected, the risk of a security breach increases.

Talking about operation technology systems (OT), the question is how to secure them against cyber security threats without the need to completely modify them and how to achieve a full understanding between security rules for Information Technology (IT) & for OT. In short, cyber security for OT differs from cyber security for IT.

> **"The greater risk for a non-secure control system is being vulnerable to threats like enabling outsiders to take control over the Power Plant."**

The role of the OT computer systems is to keep the plant safe, functional, and highly available. Industrial assets have several systems in place with roles that are clearly defined to protect and control processes that gather data for maintenance, billing, and other business-related purposes.

But what happens when a *one-fits-all* solution is applied for security?

RECIPE FOR DISASTER

In the same way that IT firewalls are not efficient for OT, when IT Policies are applied to OT systems, we have a recipe for disaster.

Let's take the example of the IT security rules for setting a password. We are all familiar with the strong password rules: at least 8 characters, both upper and lower case, adding special characters and non-consecutive numbers.

This layer of security might be suitable for preventing unauthorised access to a business system but in the Control Room things are different.

If the operator is locked out of the control system this could have serious consequences in terms of availability of the Power Plant and safety.

And of course, **the last thing you want in a Power Plant is to lose control.**

THE SOLUTION

It is essential to have a clear view of the differences between IT and OT security measures to be able to implement rules that work on each environment.

To achieve this, it is imperative to find a partner that has experience with operational technology systems to prevent the erroneous implementation of IT cyber security rules into OT systems.

At Bohemia Market, we have over 18 years' experience working with OT systems. We understand the security requirements for Power Plants and are able to establish the cyber security perimeter out of a single box.

Our **PEDRONEL ONE** is a data diode solution that blocks unauthorised connections and eliminates cyber threats. It enables the data to travel securely from the Power Station to any offsite location in the world, eliminating the risk of hackers taking control of your Power Plant.

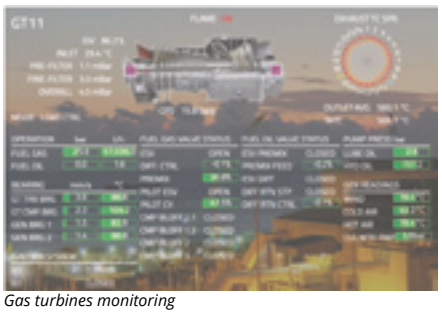
It includes a revolutionary **Historian** that goes beyond data collection, it gets information out of the data and enables you to make critical decisions faster.

The tag searching feature saves you time when viewing your complete plant history and makes reporting a breeze.

We are disrupting the industry with a unique **Unlimited Tags Model** that gives you all of the process data points you need without restrictions and included in a one-time fee.

The web-based visualisation system is available on desktop, mobile and video walls to display your data directly from OPC UA servers.

Coal fired plant monitoring



Gas turbines monitoring

Solar plants monitoring

One way data transfer. Entirely secure and with unlimited tags to keep you competitive on the grid.

Talk to us about your Power Plant security needs today.

Learn more at **bm.company**

dálkových monitorovacích center. Jsme schopni pokrýt celé spektrum, abychom vám zajistili konkurenční výhodu na trhu. Za více než 18 let naší působnosti jsme si získali důvěru vizionářů v elektrárenském průmyslu z různých koutů světa, protože máme odvahu nacházet netradiční řešení tam, kde si ostatní netroufají. Pro více informací navštivte naše stránky bm.company.

At Bohemia Market we provide comprehensive engineering services for customers around the world. From upgrade of HMI systems, to design and delivery of sophisticated Remote Monitoring Centres. We cover the whole spectrum to give you the competitive edge on the grid. With more than 18 years' experience, we have earned the trust of visionaries in the Power Generation Industry worldwide because we dare to find solutions where others don't venture. Learn more at bm.company

COLSYS AUTOMATIK

COLSYS - AUTOMATIK, a.s.

Huťská 1294
272 01 Kladno
Czech Republic
+420 312 285 312
www.colaut.cz

Inženýrská společnost poskytující služby v oborech průmyslová automatizace, průmyslová komunikace, řízení a optimalizace energetiky. Společnost COLSYS – AUTOMATIK, a.s., se ve svém portfoliu věnuje již více než 20 let návrhu, projektovaní, nasazení, dodávkám a servisu průmyslových komunikačních sítí. V drtivém procentu se jedná o kritickou komunikační síťovou infrastrukturu v průmyslovém prostředí.

Engineering company providing services in the fields of industrial automation, industrial communication, power management and optimization. For more than 20 years COLSYS - AUTOMATIK, a.s. has been designing, deploying, supplying and servicing industrial communication networks. It is an overwhelming percentage of critical communication network infrastructure in an industrial environment.

FLOWMON NETWORKS a.s.

Sochorova 3232/34
616 00 Brno
Czech Republic
www.flowmon.com

Flowmon
Driving Network Visibility

Česká společnost Flowmon Networks pomáhá firmám spravovat a zabezpečovat jejich síťovou infrastrukturu prostřednictvím moderní technologie monitorování a analýzy chování počítačových sítí na bázi datových toků (NetFlow/IPFIX). Díky řešení Flowmon získávají IT profesionálové po celém světě kontrolu nad síťovým provozem, zvyšují výkonnost aplikací a chrání své systémy před moderními kybernetickými hrozbami, které obchází tradiční bezpečnostní prvky.

Flowmon Networks empowers businesses to manage and secure their computer networks confidently. Through our high performance network monitoring technology and lean-forward behavior analytics, IT pros worldwide benefit from absolute network traffic visibility to enhance network & application performance and deal with modern cyber threats. Driven by a passion for technology, we are leading the way of NetFlow/IPFIX network monitoring that is high performing, scalable and easy to use. The world's largest businesses, internet service providers, government entities or even small and midsize companies rely on our solutions to take control over their networks, keep order and overcome uncertainty. With our solution recognized by Gartner, recommended by Cisco, Check Point and IBM, we are one of the fastest growing companies in the industry.

GREYCORTEX s.r.o.

Purkyňova 127
612 00 Brno
Czech Republic
+420 511 205 216
info@greycortex.com
www.greycortex.com

GREYCORTEX

GREYCORTEX využívá pokročilé metody umělé inteligence a strojového učení, které pomáhají společnostem a organizacím po celém světě, aby jejich sítě byly bezpečnější a spolehlivější. MENDEL, produkt společnosti GREYCORTEX, je pokročilým řešením pro analýzu síťového provozu, detekci hrozeb, sledování výkonu a hluboké viditelnosti sítí pro místní a národní úřady, armádu, justici, kritickou infrastrukturu, zdravotnické, výzkumné a finanční instituce a podniky všech velikostí. Chrání jejich budoucnost, citlivá data, sítě, tajemství a pověst.

GREYCORTEX uses advanced artificial intelligence, machine learning, and data mining methods to help organizations make their IT and OT network operations secure and reliable. MENDEL, from GREYCORTEX, gives professionals the security of knowing what's hiding in their IT and SCADA networks, at any time. Using network traffic analysis, it helps corporations, governments, and the critical infrastructure sector protect their futures by detecting cyber threats to sensitive data, networks, trade secrets, and reputations, which other traditional network security tools miss.

VERACOMP, s.r.o.

Šafaříkova 201/17
120 00 Praha
+420 724 647 785
info@veracomp.cz
www.veracomp.cz

veracomp

Veracomp Česká republika je VAD - to je zkratka pro „Value Added Distributor", což si můžeme vyložit tak, že jenom neprodáváme, ale poskytujeme přidanou hodnotu na poli konzultací, školení a technického poradenství. Zní to hrozně složitě, ale vlastně tomu tak není: Z povahy distribučního modelu, který ctíme, neprodáváme na koncový trh, ale přes naše obchodní partnery.Jsme součástí Veracomp Group - lídra v distribuci s přidanou hodnotou (VAD - Value Added distribuce) v oblasti ICT řešení. Společně působí ve 17 zemích střední a východní Evropy.
V našem portfoliu naleznete hned několik proslulých značek:
Fortinet - přední světový dodavatel integrovaných síťových bezpečnostních řešení pro poskytovatele připojení, datová centra, podniky a pobočkové sítě. Společnost Fortinet je držitelem 320 patentů a dalších 258 návrhů má v patentovém řízení. Pro své produkty získala více certifikátů než kterýkoli jiný dodavatel bezpečnostních zařízení.
Nozomi Networks - světová jednička ve svém oboru, se zabývá kybernetickou bezpečností v oblasti průmyslových sítí (tzv. ICS – Industrial Control Networks). Řešení Nozomi Networks poskytuje kompletní visualizaci prostředí a datového provozu uvnitř sítě.
Extreme Networks - patří mezi lídry v oblasti jak pevných, tak bezdrátových síťových technologií. Řešení Extreme Networks stojí na konceptu inteligence ve správě. To mimo jiné znamená, že zákazníkům poskytuje v síti detailní viditelnost a kontrolu nad provozem tak, aby věděli, co se v síti děje, kdo, kdy, kde a s jakým zařízením se připojuje a jaké aplikace a s jakou kvalitou používá.

Veracomp Czech Republic is a VAD - this stands for „Value Added Distributor", which we can interpret as not just selling, but providing added value in consulting, training and technical consulting. It sounds terribly complicated, but it is in fact very simple: By the nature of the distribution model we honor, we do not sell to the end market, but through our business partners.
We are part of the Veracomp Group - leader in Value Added Distribution (VAD) in ICT solutions. Together we operate in 17 countries of Central and Eastern Europe.
In our portfolio you will find several renowned brands:
Fortinet - the world's leading supplier of integrated network security solutions for connectivity providers, data centers, enterprises and branch networks. Fortinet holds 320 patents and has 258 other patent applications pending. It has received more certificates for its products than any other security device supplier.
Nozomi Networks - the world leader in its field, is engaged in cyber security in area of industrial networks (so-called ICS - Industrial Control Networks). Nozomi Networks provides complete visualization of environment and data traffic within the network.
Extreme Networks - is a leader in both fixed and wireless networking. Extreme Networks solutions are based on the concept of intelligence in management. This means, among other things, providing customers with detailed visibility and control over the network so they know what is happening on the network, who, when, where and with what device they are connecting, what applications and quality they use.

Media Partners

SERVICE & SUPPORT spol. s r. o.

Zvonařka 16, 617 00 Brno
Česká republika
www.sands.cz

Service & Support spol. s r.o. byla založena v roce 2003 s hlavním cílem poskytovat služby a podporu v oblasti řízení a rozvoje firemní ICT infrastruktury. Společnost se brzy stále více podílela na tvorbě integrovaných bezpečnostních systémů se zaměřením v pozdějších letech na řešení Big Data, v současné době je certifikovaným Elite partnerem Splunk v České republice. Převážná část našich integračních projektů je zaměřena na oblast bezpečnostních řešení a optimalizace IT Operations. Významnou část poskytovaných služeb tvoří oblast IOT, konkrétně prostředí SCADA, kde se podílíme na zajištění bezpečnosti SCADA systémů – a to od analýz rizik, tvorby politik bezpečnosti, přes dodávku a provoz systémů, až po systémy pro dohled IT služeb, resp. business služeb s systémy pro dohled a řízení bezpečnosti – SIEM.

Service & Support spol. s r.o. was established in 2003 with the main aim of providing services and support in the field of management and development of corporate ICT infrastructure. The company soon became increasingly involved in the field of integrated security systems creations, focusing in the later years on Big Data solutions, currently being a certified Elite Partner of Splunk in the Czech Republic. Most of our integration projects focus on security solutions and IT Operations optimization. A significant part of the provided services is in the area of IoT, namely the SCADA environment, where we participate in ensuring the security of the SCADA systems – from risk analysis, security policies definition, system delivery and operation to IT and business operations monitoring and security information and event management (SIEM).

ALEF NULA, a.s.

Pernerova 691/42
186 00 Praha 8
Czech Republic
+420 225 090 111
cz-recepce@alef.com
www.alef.com

Společnosti ALEF patří mezi největší dodavatele informačních technologií v České republice, na Slovensku, v Maďarsku, Slovinsku, Chorvatsku a Srbsku. Specializujeme se na technologie Cisco, NetApp a Meraki, se kterými máme více než 20 let zkušeností. Specialisté ALEF neovládají pouze teoretická specifika technologií, která jsou důležitá pro školení. Mají zároveň bohaté praktické zkušenosti, což jim umožňuje pohotově reagovat na jakékoliv technologické výzvy a problémy. Výsledkem je bezkonkurenční šířka i hloubka technického know-how.

ALEF is a reliable supplier of information technologies since 1994. We became one of the largest and strongest distributors in the Eastern Europe – with offices in Croatia, Czech Republic, Hungary, Serbia, Slovakia and Slovenia. ALEF strongly specialize in technology. Our expert center with extensive number of engineers allow us to provide full range of presales and postsales services, including certified trainings, professional, consulting and managed services as well as operating ALEF's own CSIRT. ALEF has direct contracts with Cisco, NetApp, Meraki, F5 Networks Flowmon, Thycotic, Arris, KEPM, Libelium and some minor vendors. ALEF is constantly growing company with current annual revenue over 150M EUR employing more than 220 professionals.

CyberG Europe, a.s.

Pobočná 1395/1
Praha 4
Czech Republic
info@cybergeurope.com
www.cybergeurope.com

Našim klientům poskytujeme ucelený vzdělávací program v oblasti bezpečnosti, kybernetické bezpečnosti a kybernetické obrany. Navrhujeme a dodáváme strategické i detailní studie vzdělávání, obsah edukačních programů, ale také workshopy, audity, poradenství a tvorbu strategií. Navíc disponujeme vlastním elitním týmem hackerů a kybernetických vyšetřovatelů. Všichni se osvědčili a vydobyli si zkušenosti při ochraně průmyslových podniků, finančních institucí, zpravodajských služeb a řadě dalších oblastí.

We offer our clients comprehensive educational program in the fields of security, cyber-security and cyber-defense. We design and deliver strategical and detail educational studies and analyses, educational programs' content, but also workshops, audits, consultation services and strategy formulations. Furthermore, we have our own elite team of ethical hackers and cyber professionals and investigators. They all have proven their worth and earned experience while protecting and safeguarding industrial companies, financial institutions, security agencies, and many other fields.

SPLUNK® FOR INDUSTRIAL DATA AND THE IoT

New insights from sensors, devices and industrial control systems

- **Gain real-time insight** from sensors, devices and industrial and operational technologies
- **Collect, manage and analyze** the velocity, volume and variety of data
- **Complement and integrate** with existing operational technologies

Disparate and deployed industrial assets and connected devices can provide the enterprise a unique touch point to real-world operations and conditions. But collection, storage and insight of the machine data generated by the Operational Technology (OT) and the Internet of Things (IoT) can be a challenge.

Splunk software collects, analyzes and visualizes real-time and historical machine data from any source—including operational technology, connected assets and products—enabling you to improve operations, ensure safety and compliance, perform predictive maintenance and better manage the uptime and availability of industrial assets. Use Splunk to harness the power of the machine data generated by devices, control systems, sensors, SCADA systems, networks, applications and end users connected by industrial networks.

Connecting Splunk to Industrial Data and the IoT

Optimate Integrator for PI System to Splunk

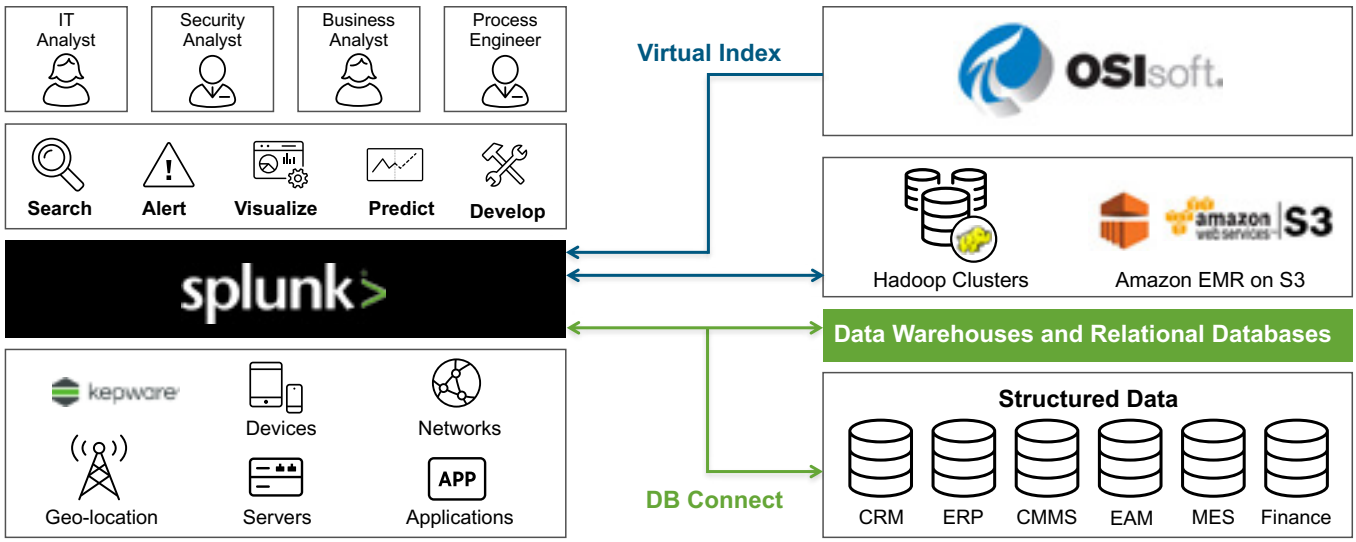
Make OSIsoft PI System data available in Splunk through a read-only query to PI, accessible within Splunk through a Splunk Search Processing Language (SPL) query

Kepware Industrial Data Forwarder for Splunk

Get real-time data collection from over 150 open and proprietary industrial data protocols common in energy, manufacturing, and oil and gas environments

HTTP Event Collector (HEC) and Modular Inputs

Use Splunk's HEC API and token-based authentication or modular input apps for MQTT, COAP, AMQP and JMS to access real-time data from industrial IoT devices and applications



Why Splunk for Industrial Data and the IoT?

Monitoring and Diagnostics

Ensure that equipment in the field operates as intended. Monitor and track unplanned device or system downtime. Understand the cause of failure on a device to improve efficiency and availability. Identify outliers and issues in device production or deployment.

Security, Safety and Compliance

Help protect mission-critical assets and industrial systems against cybersecurity threats. Gain visibility into system performance or set points that could put machines or people at risk and satisfy compliance reporting requirements.

Predictive Maintenance

Gain real-time insight into asset deployment, utilization and resource consumption. Recognize patterns and trends, and use operational data to proactively approach long-term industrial asset management, maintenance and performance.

Asset Performance Management

Gain real-time insights into the health and performance of your industrial assets. Use machine learning to detect anomalies and deviations from normal behavior to take corrective action—improving uptime, reliability and longevity.

Splunk Integrates With Leading Cloud IoT Platforms and Services

As businesses build and deploy connected devices, they are also deploying a new generation of commercial IoT platforms and services. These platforms and services enable device connectivity, visibility and simple provisioning and remote device management. They act as both a gateway to device operations and provide a platform for interaction with remote device operations and performance.

Splunk software enables powerful machine data analytics for the IoT and eliminates the need to build them from the ground up. Leading IoT platforms including Xively by LogMeIn, Citrix Octoblu and AWS IoT are already integrated with Splunk software, enabling fast time to value for developers and end users.

Download Splunk for free or explore the online sandbox. Whether cloud, on-premises or for large or small teams, Splunk has a deployment model that will fit your needs. Learn more about how Splunk customers like Bosch and Myriad Genetics are realizing value from industrial data and the IoT.

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com

FUTURE FORCES FORUM

POLICY

DIPLOMACY

DEFENCE

SECURITY

R & D

ACADEMIA

INDUSTRY

www.future-forces-forum.org