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

Bezpečnostní konference

SCADA SECURITY

Součástí Future Forces Forum

15. května 2025

Policejní akademie České republiky v Praze

Hlavní partner konference

COLSYS AUTOMATIK

Coffee break partner

ALEFNULA

Partneři konference

ROHDE&SCHWARZ

GREYCORTEX

cloudfield

FUTURE FORCES FORUM

Partneř FFF pro vědu a výzkum

Univerzita obrany

Generální partner Future Forces Forum

CSG Czechoslovak Group

Partner Future Forces Forum

RESCUE TRAILER

COLSYS AUTOMATIK

HIRSCHMANN
A BELDEN BRAND

PRŮMYSLOVÉ KOMUNIKAČNÍ SYSTÉMY PRO KRITICKOU INFRASTRUKTURU

Analýzy rizik, analýzy zadání.
Konzultace.
Inženýring.
Řešení pro průmyslovou bezpečnost.
Dokumentace a projekty.
Dodávky kompletních řešení komunikací.
Zprovoznění a oživení.
Analýzy síťového provozu, audity provozu.
Technická podpora.
Další služby související s průmyslovými komunikačními systémy.

Sledujte náš YouTube kanál
COLSYS – AUTOMATIK, a.s.

www.colaut.cz **obchod@colaut.cz**

Společnost COLSYS – AUTOMATIK, a.s., je česká inženýrská společnost. Od roku 1998 jsme partnerem HIRSCHMANN Automation And Control, GmbH, v oblasti kompletních řešení, dodávek a technické podpory řešení.

Vážené dámy, vážení pánové, příznivci a přátelé kybernetické bezpečnosti,

vítám vás opět na konferenci SCADA SECURITY 2025, která slaví svůj pátý ročník. Tentokrát se setkáváme v prostorách Policejní akademie ČR, kde je samotná bezpečnost snad nejvíce doma, kde si lze představit.

A je opět nač se těšit – tradičně konference pokrývá témata od oblastí klasického IT až po sféru výrobních průmyslových systémů a jejich (nejen) bezpečnosti.

On komplexní pohled na celou bezpečnost je, nejen a zejména pak v průmyslu, velmi důležitý parametr úspěchu v případě situace, která není právě standardní. Legislativa ukazuje dobrý návod na zajištění základních bezpečnostních požadavků pro standardní IT systémy. U systémů průmyslových je na rady mírně chudší, což je ale dáno velkou různorodostí dotčených systémů. Navíc, řada průmyslových systémů svoji bezpečnost řeší a zajišťuje i bez potřeby regulační legislativy – prostě proto, že samy firmy vnímají (čím dál více) potřebu zabezpečit to, co je živí – tedy výrobní procesy a jejich životaschopnost.

A zde vstupuje v průmyslu do hry nutná znalost systému u každého jednotlivého správce, rozhled nad provozem systému jako celku a zajištěním jeho integrity, důvěrnosti, dostupnosti, provozovatelnosti a obnovitelnosti.

V této souvislosti zmíním i důležitost osvěty a vzdělávání – nejen – správců systémů. A v této věci může dnešní konference jistě přispět svým dílem.

Doufám tedy, že dnešní konference přinese tyto informace a bude pro všechny přínosem.

Těším se na setkání s každým z vás…

Jiří Kasner
Předseda představenstva
COLSYS – AUTOMATIK, a.s.

Ani v roce 2025 nelze zabezpečení technologických a řídicích systémů považovat za vyřešený problém

Bezpečnost technologických prostředí, průmyslových řídicích systémů (ICS) a dalších specifických zařízení a OT infrastruktur zůstává i nadále jednou z nejproblematičtějších oblastí kybernetické bezpečnosti. Přestože se situace postupně zlepšuje – zejména díky rostoucímu povědomí o specifických hrozbách a lepší dostupnosti technických nástrojů, standardů i rámců – každodenní provozní realita ukazuje, že jsme i v roce 2025 daleko od stavu, který by bylo možné označit za uspokojivý.

Aktuální útoky, při nichž škodliví aktéři kompromitují přístupové mechanismy mezi IT a OT, stále potvrzují, že klíčovým problémem zůstává nedostatečné oddělení těchto dvou světů. Bezpečnostní opatření v OT prostředích navíc bývají často nastavována reaktivně, bez systematického posouzení stavu bezpečnosti podle odborných standardů, jako je například IEC 62443. Právě takové posouzení přitom může představovat velmi dobrý výchozí bod pro definici měřitelné, efektivní a smysluplné bezpečnostní strategie.

Pro letošní ročník konference SCADA Security jsme proto připravili přednášku zaměřenou právě na problematiku posuzování bezpečnosti OT prostředí, a to nejen s využitím rozdílové analýzy vůči požadavkům vybraných norem, ale také pomocí modelování hrozeb a rámce MITRE ATT & CK. Jelikož samotná implementace bezpečnostních opatření požadovaných odbornými normami a rámci však nezaručuje jejich efektivitu, zaměříme se rovněž na možnosti realizace smysluplných bezpečnostních testů a na specifická omezení, která je v OT prostředí nutné při jejich provádění dodržovat, aby nedošlo k narušení provozu.

Zajištění bezpečnosti OT systémů není možné bez kombinace kvalitních procesů, vhodně zvolených technologií a – především – kompetentních odborníků. Věřím, že i letošní ročník konference SCADA Security přispěje k rozvoji všech tří těchto pilířů.

Jan Kopřiva
Senior Security Consultant
ALEF NULA, a.s.

Vážení účastníci konference SCADA Security,

společnost Rohde & Schwarz již více než 90 let vyvíjí, vyrábí a prodává elektronické produkty pro profesionální aplikace na světovém trhu. Rohde & Schwarz disponuje rozsáhlou prodejní a servisní sítí a je přítomna ve více než 70 zemích světa, především prostřednictvím vlastních dceřiných společností. V České republice je značka Rohde & Schwarz známá již téměř 40 let.

Dceřinou společnost Rohde & Schwarz - Praha, s.r.o. založil a slavnostně otevřel zakladatel společnosti Rohde & Schwarz GmbH & Co. KG., Dr. Hermann Schwarz, jako první samostatnou dceřinou společnost v zemích střední a východní Evropy v roce 1995.

Dlouhá desetiletí byla naše společnost synonymem pro špičkovou testovací a měřící techniku v oblasti elektromagnetického spektra. Dále synonymem pro radiostanice pro profesionální použití, televizní vysílače, radiomonitoring, v poslední době i satelitní monitoring a zpracování signálu

V posledních několika letech rozšířila naše společnost své portfolio i o kryptografickou techniku a produkty pro cyber security a síťové produkty dceřiné společnosti LANCOM.

V prezentaci na konferenci SCAD se zaměřím především na dvě produktové řady certifikovaných kryptografických prostředků a na jejich potenciál nejen pro ochranu utajovaných informací, ale i v oblasti kritické infrastruktury nebo ochrany průmyslového know-how.

Konkrétně se jedná o prostředek ELCRODAT 7-FN a jeho potenciál pro národní použití i ve světle dokumentu „Národní politika kryptografické ochrany utajovaných informací v České republice“ z loňského roku.

Druhým tématem je potenciál certifikovaného kryptografického prostředku pro L2 vrstvu v OSI modelu SITLIneETH pro ochranu kritické infrastruktury. Nejedná se pouze o problematiku ochrany dat před zcizením, ale i o integritu dat.

Pavel Kotyk
Sales Engineer
ROHDE & SCHWARZ – Praha, s.r.o.

Vážení účastníci konference SCADA Security,

je mi ctí vás přivítat na letošním ročníku této odborné akce, která se v čím dál složitějším světě kybernetických hrozeb stává důležitou platformou pro výměnu zkušeností, sdílení osvědčených postupů a propojování odborníků napříč oblastmi IT, OT i bezpečnosti.

Ochrana kritické infrastruktury, zejména v oblasti průmyslových řídicích systémů, dnes vyžaduje mnohem více než jen robustní technologii. Je třeba rozumět provozu, mít přehled o komunikaci v sítě, dokázat rychle reagovat a především spolupracovat. Proto vítám zaměření letošní konference nejen na technologické trendy a nové hrozby, ale i na krizové řízení, legislativu a praktické zkušenosti s implementací směrnice NIS2.

Ve společnosti GREYCORTEX se dlouhodobě věnujeme vývoji nástroje Mendel, který pomáhá nejen průmyslovým podnikům i státním organizacím získat přehled nad sítí, odhalovat hrozby a chránit klíčové systémy bez zásahu do provozu. Věřím, že moderní nástroj může výrazně přispět k bezpečnosti – pokud je používán v rámci promyšlené strategie, jasně nastavených procesů a spolupráce napříč týmy.

Jsem rád, že se letos do programu aktivně zapojuje i můj kolega Ondřej Hubálek, který se účastní panelové diskuze věnované krizovému řízení a kontinuitě podnikání. Věřím, že jeho praktické postřehy z oblasti síťového monitoringu přispějí k širší debatě o ochraně provozu a odolnosti průmyslových systémů.

Přeji vám přínosný a podnětný den, který posílí odolnost nejen vašich systémů, ale i celé společnosti.

Petr Chaloupka
CEO
GreyCortex s.r.o.

Vážení účastníci,

kybernetická bezpečnost dnes není jen o ochraně dat – je o ochraně kontinuity společnosti, veřejné infrastruktury a důvěry. S rostoucí digitalizací průmyslu se i dříve izolované technologie stávají součástí otevřenějších systémů, a tím i cílem stále sofistikovanějších útoků.

V Cloudfieldu věříme, že prevence začíná u pochopení reálných hrozeb – nejen těch technických, ale i organizačních. Právě proto jsme vytvořili dceřinou společnost Comma0, která se věnuje výhradně oblasti kybernetické bezpečnosti a chrání jak moderní cloudová prostředí, tak průmyslové a státní systémy. Zaměřujeme se na návrh bezpečnostních architektur, provoz vlastního SOC týmu, simulaci reálných útoků a implementaci GRC rámců v souladu s NIS2, DORA či ISO27001.

Jedním z našich největších technologických přínosů v této oblasti je Triagator – automatizovaný framework, který pomáhá SOC týmům zvládat desítky incidentů denně bez nutnosti neustálé lidské přítomnosti. Triagator je odpovědí na současnou realitu: útočníci nečekají na pracovní dobu.

Velmi si vážíme možnosti být součástí SCADA Security Conference 2025. Těšili jsme se, že budeme moci sdílet naše zkušenosti a zároveň se inspirovat přístupy dalších odborníků, kteří – stejně jako my – věří, že bezpečnost začíná u strategie a končí u precizního provedení.

Děkujeme, že chráníte to, na čem opravdu záleží.

Lucia Belková
CEO
Cloudfield, a.s.

Hlavní partner konference

COLSYS AUTOMATIK

Coffee break partner

ALEFNULA

Partneři konference

GREYCORTEX

cloudfield

Pod záštitou a za podpory

Národní úřad pro kybernetickou a informační bezpečnost

Hospodářská komora České republiky

Ministerstvo průmyslu a obchodu

Univerzita obrany

Centrum kybernetické bezpečnosti

ictunie

ČIMIB

Mediální partneři

CZDEFENCE Czech Army and Defence Magazine

Cyber Security Review

Network News

ICT Network News

IT Systems www.SystemOnLine.cz

katalogakci.cz

AUTOMA

Program konference

čtvrtek 15. května 2025 — Policejní akademie České republiky v Praze

9.00	Zahájení **Petr JIRÁSEK** – moderátor	
9.10	Úvodní slovo **Tomáš KREJČÍ**, NÚKIB	NÚKIB
9.25	*Úvodní vystoupení:* Nové výzvy pro provozovatele kritických informačních systémů **Bohuslav ZŮBEK**, Ministerstvo Vnitra ČR	MINISTERSTVO VNITRA ČESKÉ REPUBLIKY
9.50	*Vystoupení hlavního partnera:* Design, bezpečnost a nasazení kritické komunikační infrastruktury – krok za krokem… **Jiří KASNER**, COLSYS Automatik	COLSYS AUTOMATIK
10.20	Diskuze	
10.45	*Coffee break*	

KRIZOVÉ ŘÍZENÍ A KONTINUITA PODNIKÁNÍ, diskuzní panel

11.30	Úvodní slovo **Jaroslav PEJČOCH** – moderátor	
11.40	Úvodní slovo **David PATRMAN**, Generální ředitelství Hasičského záchranného sboru	
11.50	Moderovaná diskuze: • **David PATRMAN**, GŘ HZS • **Jan DUSPĚVA**, ČEPRO, a.s. • **Ondřej HUBÁLEK**, GREYCORTEX • **Radek JANSKÝ**, ŠKODA AUTO • **BG Petr ŠNAJDÁREK**, AČR	GREYCORTEX
12.50	*Oběd*	

Bezpečnost řídicích systémů:
zabezpečení infrastruktury, na níž stojí moderní společnost

Průmyslové a další řídicí systémy dnes tvoří jeden z klíčových pilířů fungování moderní společnosti. Jsou základem provozu energetiky, dopravy, zdravotnictví, výroby i dalších kritických oblastí. Spolehlivá funkce těchto systémů je nezbytná pro zajištění základních služeb, stability i národní bezpečnosti. S rostoucí digitalizací však roste i jejich zranitelnost.

Technologická prostředí (OT) a systémy typu ICS jsou vystavovány stále sofistikovanějším hrozbám – od kompromitace přístupových bodů mezi IT a OT, přes zneužití nedostatečně zabezpečených komponent, až po cílené útoky zaměřené na narušení provozu. Dopady souvisejících incidentů mohou být extrémně vysoké nejen z pohledu výroby či konkrétního postiženého procesu, ale i z hlediska bezpečnosti osob či fungování celé moderní společnosti.

Společnost ALEF Nula se proto dlouhodobě věnuje problematice kybernetické bezpečnosti specifických systémů a prostředí a disponuje v této oblasti špičkovými odbornými kapacitami. Naši specialisté, držitelé prestižních mezinárodních certifikací, pomáhají zákazníkům v celé šíři činností spojených se zajištěním kybernetické bezpečnosti OT systémů – od implementace preventivních bezpečnostních mechanismů po praktické ověření úrovně zabezpečení.

Nabízíme mimo jiné:

- Bezpečnostní testování OT prostředí, ICS systémů a specifických zařízení včetně pasivní analýzy zranitelností a technického hodnocení rizik.
- Modelování hrozeb pro specifická technologická prostředí.
- Konzultace pro vývojáře řídicích a dalších specifických systémů zaměřené na bezpečný návrh a architekturu.
- Implementaci procesních a technologických opatření dle norem z řady IEC 62443 i souvisejících legislativních požadavků.
- Budování systémů řízení kybernetické bezpečnosti (CSMS) šitých na míru konkrétním provozním podmínkám.
- Posouzení zabezpečení OT s využitím rozdílových analýz oproti požadavkům odborných standardů i legislativy.

Ve spolupráci se společností Nettles Consulting navíc realizujeme specializovaná školení zaměřená na různé aspekty OT bezpečnosti, určená jak pro provozní či implementační specialisty, tak pro bezpečnostní role v rámci organizace.

Bezpečnost řídicích systémů si žádá více než jen technologická řešení. Vyžaduje porozumění konkrétnímu prostředí, hluboké odborné zkušenosti a schopnost aplikovat bezpečnostní opatření bez negativního dopadu na provoz. Právě tyto přístupy tvoří základ našich služeb.

Pokud Vás naše nabídka zaujala, rádi Vám kteroukoli z našich služeb představíme detailněji – neváhejte nás kontaktovat na e-mailu cz-sales@alef.com.

NOVÉ TECHNOLOGICKÉ TRENDY V OBLASTI BEZPEČNOSTI ICS

Petr JIRÁSEK – moderátor

13.30 *Partnerské vystoupení:*
Certifikované kryptografické prostředky jak pro ochranu UI, tak pro kritickou infrastrukturu
Pavel KOTYK, ROHDE & SCHWARZ

14.00 *Odborné vystoupení:*
Bezpečnost v době kvantové
Walter PAVLIŠ, DATERA

14.30 *Coffee break*

AKTUÁLNÍ A BUDOUCÍ KYBERNETICKÉ HROZBY A JEJICH ŘEŠENÍ, ZKUŠENOSTI Z IMPLEMENTACE EVROPSKÝCH SMĚRNIC

15.00 Úvodní slovo
Jan DIENSTBIER – moderátor

15.05 *Partnerské vystoupení:*
Odolnost pod palbou: Reakce na incidenty a zajištění kontinuity provozu v oblasti kritické infrastruktury
Michaela UHRÍKOVÁ, CLOUDFIELD

15.25 *Partnerské vystoupení:*
Posuzování zabezpečení OT: Od IEC 62443 po MITRE ATT & CK
Jan KOPŘIVA, ALEF NULA

15.50 *Odborné vystoupení:*
OT systémy v kontexte riešenia kybernetického incidentu
Lukáš HLAVIČKA, IstroSec

16.20 *Odborné vystoupení:*
NIS2 a povinností subjektů kritické informační infrastruktury státu
Petr KOPŘIVA, **Klára HUMPOLÍKOVÁ**, NÚKIB

17.00 *Závěr konference*

GREYCORTEX MENDEL

Kyberbezpečnostní dohled průmyslových sítí

- **PROVOZNÍ SPOLEHLIVOST VE VÝROBĚ**
- **PŘEHLED AKTIV V INFRASTRUKTUŘE**
- **POKROČILÁ DETEKCE HROZEB V IT A OT**
- **SLEDOVÁNÍ EXTERNÍCH PŘÍSTUPŮ**

Spolehlivá ochrana IT a OT ve výrobních podnicích

Výrobní a zpracovatelské podniky čelí rostoucím hrozbám, které ohrožují kontinuitu provozu. Komplexní a segmentované sítě ztěžují dohled nad infrastrukturou, což zvyšuje riziko výpadků způsobených chybami, přetížením nebo útoky. Situaci dále komplikuje využití zastaralých technologií bez moderní ochrany.
Řešením je nasazení neinvazivního nástroje, který pracuje pasivně a nezasahuje do provozu sítě.

Právě takový je GREYCORTEX Mendel, který nabízí ucelený pohled na komunikaci v celé infrastruktuře a umožňuje včasné odhalení hrozeb bez narušení provozu. Díky podpoře průmyslových protokolů a pasivnímu provozu představuje ideální řešení pro zabezpečení moderní výrobu.

Mendel umožňuje detekci známých i pokročilých útoků, kontrolu přístupů dodavatelů i dohled nad souladem s předpisy. Pomáhá chránit klíčové systémy jako ICS nebo ERP a zároveň podporuje IT i OT týmy díky přizpůsobitelným přehledům a auditním funkcím.

Díky dlouhodobému uchování dat a integraci s dalšími bezpečnostními nástroji zvyšuje Mendel odolnost výrobních provozů a pomáhá čelit výzvám spojeným s kybernetickými útoky v prostředí průmyslu 4.0.

Zajistěte si audit vašeho IT i OT prostředí pomocí GREYCORTEX Mendel.

www.greycortex.com

COLSYS AUTOMATIK

HIRSCHMANN
A BELDEN BRAND

KRITICKÁ INFRASTRUKTURA

Neviditelná páteř průmyslu i společnosti

V době digitalizace a automatizace nabývá pojem kritická infrastruktura zcela nového významu. Výrobní závody, energetika, doprava nebo vodní hospodářství – všechny tyto segmenty jsou závislé na systémech, které musí fungovat nepřetržitě, bezpečně a bezchybně. COLSYS – AUTOMATIK, a.s. přináší řešení pro bezpečný a spolehlivý provoz průmyslových komunikací v kritické infrastruktuře.

Kybernetická bezpečnost jako nutnost

Se zvyšujícím se propojením provozních technologií (OT) s informačními systémy (IT) roste i riziko kybernetických útoků.

COLSYS – AUTOMATIK, a.s., proto nabízí nejen robustní komunikační a dohledové systémy, ale také komplexní řešení kybernetické bezpečnosti v průmyslu – od analýzy rizik až po implementaci bezpečnostních prvků v souladu s platnou legislativou.

Sledujte náš YouTube kanál
COLSYS – AUTOMATIK, a.s.

Spolehlivý partner pro náročná řešení

Díky dlouholetým zkušenostem s projekty v oblasti energetiky, dopravy, vodního hospodářství i průmyslu je COLSYS – AUTOMATIK, a.s., partnerem, který rozumí specifickým potřebám kritické infrastruktury. Naše firma klade důraz na kvalitu, bezpečnost a dlouhodobou udržitelnost svých řešení.

www.colaut.cz **obchod@colaut.cz**

COLSYS – AUTOMATIK, a.s., česká technologická firma s více než 30 lety zkušeností, se specializuje na návrh, dodávku a integraci řídicích systémů a automatizace pro klíčové provozy. Naše řešení chrání nejen technologické procesy, ale i společenské funkce, které na nich závisí – od dodávek energie až po bezpečnost dopravy.

Útočníci nespí.

Vaše obrana by taky neměla.

Triagator je inteligentní SOAR framework, který automatizovaně zvládne až 80 % bezpečnostních incidentů – a to nonstop, 24/7.

S Triagatorem získáte:

Snadné nasazení

Implementace je rychlá a plně integrovaná s Microsoft Sentinel.

Automatické reakce

Triagator rozpozná útok, spustí obranné akce a funguje nonstop 24/7.

Zvýšení efektivity SOC týmu

Automatizace snižuje zátěž operátorů a eliminuje rizika spojená s únavou a lidským faktorem.

Škálovatelnost

Triagator zvládne paralelní analýzu stovek incidentů bez ohledu na velikost prostředí.

www.comma0.io
info@comma0.io

comma_0

Rohde&Schwarz Cybersecurity

R&S®SITLINE ETH NG

The main pillars of processes in companies and public authorities are digital. At the same time, data security requirements have risen due to increased cybercrime, IT security vulnerabilities and espionage. As a key element of IT security, layer-2 encryption provides basic protection for network communications between different locations.

Analog paperwork security, especially in the environment of public authorities, must be replaced by digital security. Unlike paperwork, digital documents move on paths that are faster but more difficult to control. Certified solutions are needed that meet the highest demands for security, efficiency and performance.

Security made in Germany – 30 years of certified cryptographic competence

R&S®SITLine ETH NG is a solution approved by the Federal Office for Information Security (BSI) up to VS-NfD (RESTRICTED), NATO RESTRICTED and RESTREINT UE/EU RESTRICTED classification level. These Ethernet encryptors provide "Security Made in Germany". With 30 years of cryptographic competence, Rohde&Schwarz Cybersecurity is one of the pioneers in the field of network encryption. We offer state-of-the-art cybersecurity with advanced cryptographic methods and standards (elliptic curves, AES-256, X.509 certificates and QKD – Quantum Key Distribution). A special feature is that the entire hardware and software production process is in the hands of Rohde&Schwarz Cybersecurity.

ROHDE&SCHWARZ

Make ideas real

Programový výbor konference

Jan DIENSTBIER, exprezident, Český institut manažerů informační bezpečnosti, Předseda

Petr JIRÁSEK, Místopředseda Výkonného výboru ENISA European Cyber Security Challenge Čestný předseda

Členové

Petr HRŮZA, Univerzita obrany

Jiří KASNER, Předseda představenstva, COLSYS – AUTOMATIK a.s.

Jan KREJČÍ, Univerzita J. E. Purkyně, Ústí nad Labem

Jaroslav PEJČOCH, Člen představenstva, ICT Unie

Tomáš PŘIBYL, CEO, Corpus Solutions a.s.

Michal ZEDNÍČEK, Cyber Expert, Alef Security

Bohuslav ZŮBEK, Oddělení kybernetické bezpečnosti, Ministerstvo vnitra ČR

Řečníci

Ondřej Hubálek
Cyber Security Presales Engineer, GREYCORTEX

IT profesionál s téměř dvacetiletou v oblasti síťové infrastruktury a kybernetické bezpečnosti. Srdcem je síťař, ale uvědomuje si klíčovou roli kybernetické bezpečnosti. V rámci řešení GREYCORTEX Mendel obě tyto oblasti znalostí propojuje a nadále rozvíjí.

Z pohledu komplexního přístupu k problematice kybernetické bezpečnosti je zastáncem nových trendů v oblasti budování kyberbezpečnostních ekosystémů a robustních XDR platforem, zvláště pak pokud obsahují potřebný kamínek skládačky, NDR systém GREYCORTEX Mendel.

Radek Jánský
SO/2 – ŠKODA AUTO Corporate Security

Zkušený profesionál v oblasti korporátní a informační bezpečnosti s více než 20 lety praxe v mezinárodním prostředí.

V současnosti působí na manažerské pozici ve společnosti Škoda Auto a.s., kde se věnuje problematice informační bezpečnosti a krizovému řízení. Zastánce komplexního přístupu k řízení rizik, konvergence bezpečnostních agend a jejich propojení s byznysovými potřebami.

Jiří Kasner
Předseda představenstva, COLSYS – AUTOMATIK, a.s.

Jiří Kasner je absolventem FEL ČVUT Praha, obor kybernetika – výpočetní technika.

V současné době předseda představenstva a společník ve společnosti COLSYS – AUTOMATIK, a.s. Odborně se zaměřuje na komplexní návrh bezpečných komunikačních systémů v průmyslu (rizika, design, konfigurace, dokumentace, analýzy), dále pak analýzy toků dat a komunikací v průmyslových systémech a řízení projektů v této oblasti vč. konzultací. Oblast kritické komunikační infrastruktury a jejích zákoutí přednáší v rámci zvaných přednášek například na VUT v Brně i na různých konferencích.

Jan Kopřiva
Senior Security Consultant, ALEF NULA

Jan Kopřiva je specialistou na kybernetickou bezpečnost s dlouhou praxí a širokými zkušenostmi.

V současnosti působí mimo jiné jako konzultant ve společnostech Alef Nula a Nettles Consulting a také jako jeden z bezpečnostních odborníků ve světoznámém sdružení SANS Internet Storm Center. Profesně se zaměřuje mj. na bezpečnostní analytiku, reakci na incidenty, analýzu malware a další aspekty tzv. „modré“ bezpečnosti, ale také oblasti penetračních testů, red teamingu a ofenzivní bezpečnosti obecně. Je autorem řady bezpečnostních kurzů, odborných výzkumů a článků zaměřených na různé aspekty kybernetické bezpečnosti a pravidelně přednáší na domácích i zahraničních odborných konferencích.

Pavel Kotyk
Rohde & Schwarz - Praha, s.r.o., Sales Engineer

Absolvent oboru FEL ČVUT obor technická kybernetika a doktorandského studia oboru biokybernetika a umělá inteligence.

V letech 1995-2003 pracoval na technických pozicích u útvaru s celostátní působností Policie ČR. Poslední zařazení jako technický náměstek útvaru.

V roce 2003 nastoupil do společnosti Rohde & Schwarz - Praha, s.r.o., kde pracuje jako prodejní inženýr se specializací na zabezpečené radiokomunikační systémy, celotělové skenery a kryptografickou techniku

Partneři konference

COLSYS – AUTOMATIK, a.s.

Huťská 1294, 272 01 Kladno
+420 312 285 312
obchod@colaut.cz
www.colaut.cz

Jsme od založení v roce 1998 ryze česká inženýrská společnost, která poskytuje služby a dodávky v oblasti kritické komunikační infrastruktury (KKI) v průmyslu, dále v oblasti systémů pro řízení a dohled nad energetickými celky a konečně v oblasti automatizovaných systémů pro řízení technologií. V oblasti průmyslové KKI se zabýváme analýzou a hodnocením rizik, analýzou provozu, návrhy a doporučeními (nejen) pro povinné subjekty a celkovým návrhem koncepce, konfigurace i provozu celé KKI až k realizaci a servisu.

HLAVNÍ PARTNER KONFERENCE

ALEF NULA, a.s.

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

ALEF působí na trhu již od roku 1994. Ctíme hodnoty jako dlouhodobá spolupráce, prozákaznický přístup a odborné kompetence. Poskytujeme dodávky a služby moderního a funkčního ICT řešení, založeného na elitních značkách v oboru, profesionálním přístupu a bohatých zkušenostech. Naše služby pokrývají celý životní cyklus ICT projektů – od předběžné analýzy, přes navržení a implementaci řešení, školení a certifikaci, až po údržbu, podporu a financování. Tyto služby jsou dostupné pro široké spektrum klientů, od malých a středních podniků až po velké mezinárodní korporace.

V oblasti technologií se zaměřujeme především na produkty a služby od společností jako Cisco, NetApp, F5, Splunk, Flowmon, Microsoft a AWS. Naše odborné znalosti zahrnují nejen teoretické aspekty těchto technologií, ale i praktické zkušenosti z reálných zákaznických projektů, což nám umožňuje efektivně minimalizovat rizika spojená s řízením ICT. Velmi si zakládáme na expertní úrovni technických znalostí, což z nás činí důvěryhodného partnera v oblasti ICT řešení.

COFFEE BREAK PARTNER

ROHDE & SCHWARZ – Praha, s.r.o.

Hadovka Office Park
Evropská 2590/33c
160 00 Praha 6
+420 234 749 101
office.rscz@rohde-schwarz.com
www.rohde-schwarz.com

Rohde & Schwarz je společnost s mezinárodní působností zabývající se vývojem, výrobou a prodejem širokého spektra elektronických zařízení pro profesionální aplikace, Rohde & Schwarz - Praha letos slaví 30 let od svého založení.

Nabízí výrobky a služby v těchto oblastech:

- testování a měření;
- bezpečné komunikační systémy;
- kybernetická bezpečnost;
- monitoring a testování sítí;
- broadcast a média

PARTNER KONFERENCE

GREYCORTEX, spol. s r.o.

Purkyňova 649/127
612 00 Brno
+420 733 601 442
info@greycortex.com
www.greycortex.com

GREYCORTEX je jedním z hlavních poskytovatelů bezpečnostního řešení NDR (Network Detection and Response) pro IT i OT (průmyslové) sítě. Zajišťuje jejich bezpečnost a spolehlivost. Produkt GREYCORTEX Mendel je řešení pro monitorování síťové bezpečnosti v IT i průmyslových (OT) sítích. Kombinací pokročilých metod detekce analyzuje síťový provoz a upozorňuje na škodlivé aktivity, běžné i neznámé moderní hrozby a provozní problémy sítě. Dokonale vizualizuje síťovou komunikaci na úrovních uživatelů, zařízení i aplikací a umožňuje systémovým analytikům a správcům sítě rychle a efektivně řešit bezpečnostní i provozní incidenty.

PARTNER KONFERENCE

Cloudfield a.s. / Comma0, s.r.o.

Na Poříčí 1047, 110 00 Praha 1
info@cloudfield.cz; info@comma0.io
www.cloudfield.cz / www.comma0.io

V Cloudfield od roku 2020 pomáháme firmám i veřejným institucím zvládat nároky moderní doby pomocí cloudových řešení, agilního vývoje softwaru a inovativního využití dat a AI. Sledujeme aktuální technologické i bezpečnostní trendy a rychle reagujeme na potřeby našich zákazníků.

Rostoucí počet kybernetických hrozeb a zpřísňující se legislativa, jako jsou směrnice NIS2 nebo DORA, nás přivedly k založení dceřiné společnosti Comma0, která se specializuje výhradně na kybernetickou bezpečnost.

V Comma0 se zaměřujeme na návrh bezpečnostních architektur, provoz bezpečnostních operačních center (SOC), implementaci GRC rámců a testování odolnosti systémů prostřednictvím aktivit Red Team a Purple Team.

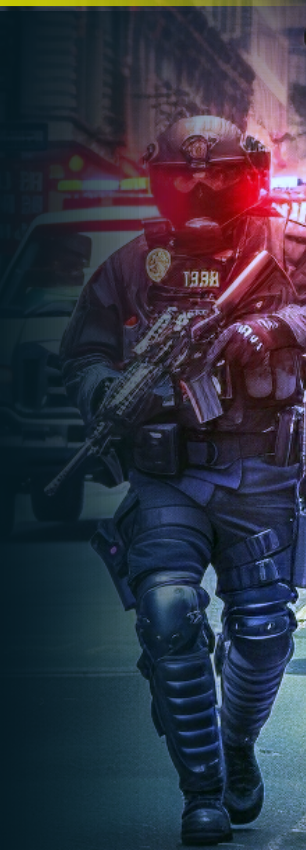
Věříme, že moderní bezpečnost musí být praktická, adaptivní a efektivní – ať jde o ochranu průmyslových technologií, cloudového prostředí nebo tradiční IT infrastruktury.

PARTNER KONFERENCE

Future Forces
EXHIBITION & FORUM

21. – 23. 10. 2026 | PRAHA

Mezinárodní setkání
odborné komunity,
prezentace technologií
a řešení pro bezpečnost
a obranu



FUTURE FORCES FORUM

www.FFF.global

generální partner

CSG Czechoslovak Group