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

Bezpečnostní konference

SCADA SECURITY

Součástí Future Forces Forum

25. března 2026

Policejní akademie České republiky v Praze

Hlavní partneři konference

SYNERIQ FORTINET

Partneři konference

GREYCORTEX cloudfield TAKTIK

KRUGEL EXIM CZ SecureAnyBox 5

FUTURE FORCES FORUM

Partner FFF pro vědu a výzkum

Univerzita obrany

Generální partner Future Forces Forum

CSG Czechoslovak Group

Partner Future Forces Forum

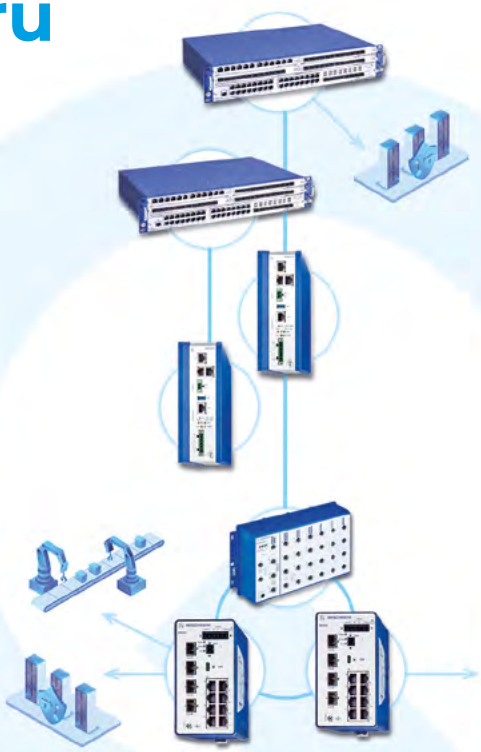
RESCUE TRAILER

SYNERIQ

JISTOTA V KAŽDÉM SPOJENÍ

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.



Společnost SYNERIQ 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.

HIRSCHMANN
A BELDEN BRAND

info@syneriq.cz

www.SYNERIQ.cz

Vážené dámy, vážení pánové,

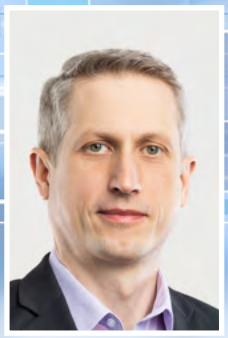
konference SCADA Security má již letitou tradici a stala se místem, kde se setkávají příznivci a odborníci z průmyslových oblastí, kterým není bezpečnostní problematika lhostejná či cizí.

Jsem rád, že i letos se můžeme na této konferenci setkat u zajímavých přednášek v průběhu celého dne. Věřím, že obsah a informační hodnota všech příspěvků bude pro posluchače tradičně přínosem.

Věřím také, že obecně se začne více a více dostávat bezpečnost na světlo zájmu nás všech (a nejen ta kybernetická, ale i ty ostatní „bezpečnosti"). Budeme se o to společně snažit.

Přeji všem maximálně užitečný a přínosný zážitek z konference a těším se se všemi na viděnou či osobní setkání.

Jiří Kasner
Předseda představenstva
SYNERIQ, a.s.



Průmyslové sítě čelí stále sofistikovanějším kybernetickým útokům, které mohou narušit výrobu, ohrozit provoz, bezpečnost i lidské životy.

Digitalizace, automatizace a propojení výrobních technologií přinášejí vyšší efektivitu, ale zároveň otevírají nové cesty pro útočníky. Podle společnosti Fortinet bude kyberkriminalita v následujících letech dále sílit a promění se v plně organizované odvětví založené na automatizaci, specializaci a využití umělé inteligence.

Útočníci budou schopni narušit provoz rychleji a snadněji než kdykoli dříve. Zatímco v minulosti rozhodovaly především nové techniky útoků, v roce 2026 bude klíčovým faktorem rychlost reakce – tedy jak rychle dokáže organizace proměnit informace v konkrétní obranné kroky.

Další vývoj kybernetické bezpečnosti bude záviset na tom, jak efektivně dokážou lidé, procesy a technologie fungovat jako adaptivní systém. Organizace, které propojí inteligentní analýzu, automatizaci a lidskou odbornost do jednoho dynamického celku, získají zásadní výhodu.

Pozitivním trendem je, že podniky začínají brát zabezpečení provozních technologií (OT) mnohem vážněji. Odpovědnost za řízení rizik OT se stále častěji přesouvá na úroveň vrcholového managementu. Tento posun odráží skutečnost, že útok na OT infrastrukturu není jen IT problém – může mít přímý dopad na výrobu, bezpečnost zaměstnanců i kontinuitu dodavatelských řetězců.

*V naší přednášce vám ukážeme, jak **Fortinet OT Security Fabric** propojuje detekci hrozeb, segmentaci a bezpečný přístup v OT prostředí, aby kritické systémy zůstaly chráněné bez výpadků. Praktický pohled na řešení této výzvy pomůže posluchačům pochopit, jak propojit kybernetickou bezpečnost s provozními potřebami průmyslu.*

Těšíme se na setkání a odborné diskuze s vámi na konferenci SCADA SECURITY 2026.

Jan Václavík
Systems Engineering Team Lead
FORTINET

Vážení účastníci konference SCADA Security,

dovolte mi, abych vás jménem společnosti GREYCORTEX přivítal na konferenci SCADA Security 2026. Toto setkání vnímám jako důležitou platformu pro výměnu zkušeností v oblasti, kde se digitální technologie přímo potkávají s fyzickým provozem a průmyslovou výrobou.

S narůstající komplexností řídicích systémů a jejich propojováním s vnějšími sítěmi roste i jejich zranitelnost. Jako ředitel společnosti, která se dlouhodobě věnuje ochraně náročných síťových prostředí, vnímám znepokojivý trend: útočníci jsou v poznání vašich vlastních sítí často o krok napřed. Zatímco se provozní týmy soustředí na kontinuitu výroby, sofistikovaní aktéři využívají „slepých míst" v infrastruktuře k tichému mapování slabin. Tento asymetrický vztah, kdy útočník vidí víc než správce, představuje pro kritickou infrastrukturu největší bezpečnostní riziko.

Právě na tento problém se zaměříme v našem letošním příspěvku s názvem „Proč útočníci vidí vaše ICS dřív než vy". Pevně věřím, že hloubková viditelnost je naprostým základem účinné obrany – nemůžete totiž chránit to, o čem nevíte, ani reagovat na anomálie, které v reálném čase nevidíte. Můj kolega Ondřej Hubálek vám představí, jak tyto principy přenášíme do praxe prostřednictvím našeho řešení GREYCORTEX Mendel. Ukážeme vám, jak pomocí pokročilé analýzy síťového provozu získat nad ICS prostředím nepřetržitý přehled a eliminovat hrozby dříve, než stihnou ovlivnit integritu vašich systémů.

Věřím, že informace a postupy, které zde zazní, budou pro vaši práci přínosné a pomohou vám lépe chránit technologické celky, za které zodpovídáte. Přeji vám produktivní účast na konferenci a podnětné diskuse.

Petr Chaloupka
CEO
GREYCORTEX

Vážení účastníci konference SCADA Security!

Ani v roce 2026 nelze zabezpečení IoT a průmyslových řídicích systémů (ICS/OT) považovat za vyřešený problém. Počet připojených zařízení roste exponenciálně, konvergence IT/OT/IoT se prohlubuje a útočníci stále častěji cílí přímo na zařízení, která nejsou vidět – shadow IoT, legacy PLC, RTU, průmyslové senzory, kamery nebo 5G modemy. Právě tato „neviditelná" zařízení představují jedno z největších rizik současnosti: bez přesné asset visibility nelze efektivně aplikovat segmentaci, detekci anomálií, ani principy Zero Trust.

Ve společnosti TAKTIK se dlouhodobě věnujeme aktivní osvětě této problematiky. Upozorňujeme provozovatele kritické infrastruktury a průmyslových podniků na to, jak velkou část jejich zařízení a attack surface ve skutečnosti nevidí, a jak vážné důsledky to může mít při cíleném útoku. Zároveň jako zkušení implementátoři pomáháme tato rizika systematicky snižovat pomocí moderních technologií pro viditelnost a kontrolu.

*Na konferenci SCADA Security 2026 představíme v přednášce „**Efektivní zabezpečení IoT a ICS v praxi: Jak ochránit to, co nevidíte**" praktický pohled na reálná nebezpečí IoT zařízení. Ukážeme, jak takové útoky v praxi vypadají, proč je mnoho zařízení „neviditelných" pro tradiční bezpečnostní nástroje, a jaká konkrétní opatření mohou organizace přijmout, aby získaly plnou přehlednost a efektivně se proti těmto hrozbám chránily – včetně využití pokročilých řešení pro automatickou detekci a behaviorální analýzu, jako je Palo Alto Networks Device Security. Věříme, že skutečná bezpečnost OT a IoT vzniká především kvalitní osvětou, pochopením reálných rizik a následnou praktickou implementací.*

Těšíme se na setkání s vámi, na otevřenou diskusi a na společné projekty, které posunou bezpečnost české kritické infrastruktury vpřed.

Lukáš Březina
Chief Technical Officer – Security
TAKTIK, a.s.

Vážení účastníci konference SCADA Security,

je mi velkým potěšením, že vám mohu představit naši ***společnost Krugel Exim CZ****, která působí na českém trhu již téměř 30 let jako distributor s přidanou hodnotou (VAD) v oblasti pasivní infrastruktury.*

Mezi stěžejní produkty v rámci našeho portfolia pak patří kvalitní strukturovaná kabeláž ***Reichle De-Massari****, která je základním stavebním kamenem vysoce spolehlivého a bezpečného spojení mezi počítači, WiFi přístupovými body, servery, internetem a dnes vlastně již téměř vším (IoT, OT, MaR…). Následně pak díky možnosti rozšíření instalace o* ***inteligentní management*** *získává uživatel dokonalý visuální přehled o síti a tím zvyšuje efektivitu a úroveň zabezpečení včetně eliminace nejrůznějších bezpečnostních rizik, a to i z pohledu směrnice NIS2.*

Velmi zajímavou informací pak je, že i analytici společnosti Gartner pravidelně informují o podceňování kvality a bezpečnosti u „první vrstvy" z hlediska OSI modelu, a to téměř u všech organizací. V souvislosti s tímto se pak těšíme, že vám budeme schopni ukázat jednu z možných cest, jak tuto problematiku efektivně vyřešit.

Přeji příjemný den plný inspirativních podnětů.

Jiří Netuka
Business Development Director
KRUGEL EXIM CZ

Vše, co jsme kdy v oblasti bezpečnosti navrhli, vyvíjíme a dodáváme zákazníkům do celého světa má společného jmenovatele - Z opatrnosti nedůvěřujeme osobě správce. SecureAnyBox je čistě kryptografický design - žádná ACL, žádné přiřazení nebo odejmutí přístupu správcem. Žádné master heslo, žádné vtípky typu rozbijte bezpečnostní sklíčko. To ale není všechno. Důležitý je i Enterprise styl správy - nový uživatel, uživatel přecházející na jinou pozici. odcházející uživatel. Přidělení přístupu tím, kdo za data/tajemství nese odpovědnost. Ne správcem, ne automaticky. Vše děláme tak, aby to odolalo i nám. Nedokážeme nikomu, kdo zapomněl přístupový klíč, pomoci. Ani tajné službě. Dokážeme Vám ale ukázat, jak systém konfigurovat tak, aby týmy data sdílely a nic důležitého se Vám neztratilo. SecureAnyBox dokáže chránit data nejen ve své databázi ale i na serveru, hostingu nebo v cloudu. Můžete sdílet citlivé soubory/data na druhou polokouli nebo se sousedem. Projekty, výzkum, právní i obchodní tajemství.

My sami nejsme cloud. Umíme vám říci, proč ne. SecureAnyBox si můžete instalovat ve svém prostředí nebo ho pro Vás může hostovat váš oblíbený partner.

Naše technologie je součástí mnoha NIS2 projektů a nevykazuje žádnou závislost na vašem prostředí. Jsme kompatibilní s Active Directory, Entra ID., eDirectory a obecnými LDAP zdroji. Server je čistá Java s pohodlnou a automatickou instalací pro Windows a Linux. Je jedno, jakou verzi čeho máte na straně serveru a na počítačích uživatelů.

Audit, SIEM, notifikace, sledování, archivace, měření entropie s využitím slovníků a mooreova zákona, plně konfigurovatelný generátor hesel, sledování a reportování compliance.

Vyvinuli jsme vše, co my sami a naši zákazníci využívají denně. Žijeme bezpečností a myslíme to vážně. Děláme i autentizaci. Opravdu dvoufaktorovou. Ne přihlášení certifikátem. Ale ta sama o sobě vaše data neochrání. Na to potřebujete:

SecureAnyBox!

Ing. Václav Šamša
CEO & CTO
TDP, s.r.o. / SecureAnyBox

Hlavní partneři konference

SYNERIQ

FORTINET

Partneři konference

GREYCORTEX

cloudfield

TAKTIK

KRUGEL EXIM CZ

SecureAnyBox 5

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

ict unie

ČIMIB

Mediální partneři

CZ DEFENCE Czech Army and Defence Magazine

Cyber Security Review

CCTV Czech Cyber TV

Network News

ICT Network News

AUTOMA

IT SYSTEMs

katalogakci.cz

Program konference

09.30 Zahájení konference
Petr JIRÁSEK

09.40 Úvodní slovo
zástupci **MPO ČR, NÚKIB**
Strategické a koncepční pohledy na rozvoj kybernetické bezpečnosti, ochranu kritické infrastruktury a připravenost České republiky na nové regulační a bezpečnostní výzvy.

09.55 Bezpečnost, design a rozumné provozování kritické komunikační infrastruktury
Jiří Kasner, Předseda představenstva, SYNERIQ, a.s.
Přednáška se zaměří na vazby mezi legislativním rámcem a praktickými kroky, které vedou k bezpečnému a spolehlivému provozu komunikační infrastruktury v kritických aplikacích v průmyslu. Pozornost bude věnována provázání různých typů bezpečnosti, dostupnosti, integrity, obnovitelnosti a provozuschopnosti a konkrétním postupům, které pomáhají těchto cílů dosahovat.

10.25 Hackeři a škodlivý kód v síti průmyslového řízení: OT Security Fabric je připraven je zastavit
Jan Václavík, Systems Engineering Team Lead, FORTINET
Průmyslové sítě čelí stále sofistikovanějším útokům, které mohou ohrozit výrobu, provoz, bezpečnost i lidské životy. Ukážeme, jak Fortinet OT Security Fabric propojuje detekci hrozeb, segmentaci a bezpečný přístup v OT prostředí, aby kritické systémy zůstaly chráněné bez výpadků. Praktický pohled na řešení této výzvy pomůže posluchačům pochopit, jak propojit kybernetickou bezpečnost s provozními potřebami průmyslu.

10.55 *Přestávka s občerstvením*

Kybernetická bezpečnost průmyslu a OT / SCADA – aktuální hrozby a trendy

11.20 Proč útočníci vidí vaše ICS dřív než vy: viditelnost jako základ ochrany kritické infrastruktury
Ondřej Hubálek, Cyber Security Presales Engineer, GREYCORTEX
Přednáška ukáže, proč je síťová viditelnost a včasná detekce anomálií zásadní pro bezpečnost průmyslových řídicích systémů a pro snižování provozních rizik. Součástí bude i pohled na to, jak tyto principy v praxi naplňuje řešení GREYCORTEX Mendel.

11.40 inteliPhy – bezpečnost, přehlednost a zvýšení efektivity pasivní infrastruktury
Jiří Netuka, Business Development Director, KRUGEL EXIM CZ
Jak získat plnou kontrolu nad provozem pasivní infrastruktury – od fáze plánování, přes monitorování v reálném čase až po dlouhodobou správu a optimalizaci provozu.

12.00 Od viditelnosti k automatizované obraně: Zero Trust architektura pro IoT/ICS
Lukáš Březina, CTO Security, TAKTIK
V éře rostoucích kybernetických hrozeb se zaměříme na využití strojového učení pro precizní identifikaci a profilování každého zařízení v síti. Ukážeme si, jak můžeme transformovat pasivní monitorování v aktivní vynucování Zero Trust politik pro IoT a OT systémy. Prezentace nabídne praktický pohled na prevenci známých i neznámých hrozeb dříve, než stihnou ovlivnit kritické procesy.

12.20 Události a trendy kyberprostoru v roce 2026
Stanislav Novotný, CZECH CYBER TV
Rok 2026 přinesl řadu událostí, které ukazují, jak rychle se kybernetický prostor proměňuje – a jak se mění i chování útočníků, jejich motivace a používané postupy. V této přednášce nabídnu stručný přehled nejvýznamnějších kybernetických incidentů a trendů roku 2026 a zasadím je do širšího kontextu vývoje hrozeb v digitálním prostředí.

12.45 *Oběd*

Krizové řízení a kybernetická připravenost organizací

13.30 *Odborný keynote:*
zástupce **MV ČR**

13.50 *Panelová diskuse:*
*moderátor **Jaroslav Pejčoch***
- ***Jiří Kasner***, Syneriq
- ***Miroslav Lukeš***, specialista na krizové řízení
- ***Aleš Špidla***, CEVRO Univerzita
- zástupce ***MV ČR***

14.50 *Přestávka s občerstvením*

Regulace a nové povinnosti: NIS2, AI Act a ochrana komunikace

15.15 Rizika AI v praxi: co hrozí při implementaci a jak je řídit
Vilém Markovič, vCISO / Cyber Security Architect, Comma0
Prezentace se zaměří na praktická rizika spojená s implementací AI aplikací v celém jejich životním cyklu – od práce s daty, přes výběr a provoz modelů až po jejich začlenění do existující IT infrastruktury a byznysových procesů. Ukáže nejčastější chyby firem v praxi, limity tradičních bezpečnostních a governance přístupů a představí principy řízení rizik pomocí AI governance, bezpečné architektury, kontrol v CI/CD pipeline, monitoringu chování modelů a jasného rozdělení odpovědností mezi IT, bezpečnost, právní a byznysové týmy. Součástí bude i pohled na dopady regulace, zejména AI Act, na reálné nasazení AI v organizacích.

15.45 Jak splnit požadavky NIS2 v praxi: bezpečná autentizace strojů a služeb
Václav Šamša, CEO & CTO, SecureAnyBox
Přednáška se zaměří na bezpečnější autentizaci strojů a aplikačních účtů v prostředí organizací. Ukáže možnosti více-faktorové autentizace pro programy a služby, přístup k rotaci hesel účtů služeb, plánovaných úloh a aplikačních poolů v prostředí Microsoft a jejich vztah k požadavkům směrnice NIS2.

16.15 NIS2 v České republice – aktuální stav a výhled
zástupce **NÚKIB**
Shrnutí klíčových požadavků směrnice NIS2, praktické dopady na organizace a aktuální informace k národní implementaci.

17.00 *Závěr konference*
Petr Jirásek

Stav OT bezpečnosti v roce 2025:
vyšší vyspělost, menší dopady incidentů a tlak na konsolidaci bezpečnostních architektur

Globální průzkum Fortinetu mezi více než 550 odborníky z klíčových průmyslových odvětví potvrzuje, že organizace začínají přistupovat k ochraně provozních technologií systematičtěji a s větší odpovědností. Zpráva o stavu OT bezpečnosti za rok 2025 ukazuje posun směrem k vyšší vyspělosti, lepší připravenosti a efektivnějšímu řízení rizik v prostředí, kde kybernetické útoky stále častěji zasahují přímo do fyzických procesů.

Rostoucí odpovědnost a zvyšující se vyspělost OT bezpečnosti

Organizace napříč průmyslem deklarují výrazný nárůst odpovědnosti za OT bezpečnost na úrovni vedení. Kybernetická bezpečnost se přesouvá pod CISO nebo jiné výkonné role, což z ní činí téma strategického významu. Tento posun se odráží i v tom, že více organizací samo uvádí vyšší úroveň vyspělosti OT bezpečnosti a lepší schopnost zvládat méně sofistikované útoky, jako je phishing či kompromitace přístupových údajů.

Vyspělejší organizace zároveň hlásí nižší počet úspěšných narušení nebo menší dopady incidentů. Trend je jednoznačný: investice do OT bezpečnosti se přímo promítají do provozní odolnosti.

Klíčová zjištění průzkumu

- **Bezpečnost OT se stává tématem představenstev** — odpovědnost se přesouvá na nejvyšší úroveň řízení, což zvyšuje prioritu důležitosti.
- **Vyspělost OT bezpečnosti snižuje dopady incidentů** — organizace významně zvýšili vyspělost, a tak s pokročilejšími procesy a nástroji zaznamenávají méně úspěšných útoků a rychleji reagují.
- **Osvědčené postupy mají měřitelný efekt** — základní kybernetická hygiena, školení, zpravodajství o hrozbách a konsolidace bezpečnostních řešení vedou k poklesu incidentů, zejména v oblasti kompromitace firemní e mailové komunikace.
- **Konsolidace dodavatelů zvyšuje efektivitu** — sjednocené bezpečnostní platformy zlepšují viditelnost, snižují složitost a umožňují rychlejší reakce.

Osvědčené postupy pro posílení OT bezpečnosti

Zpráva zdůrazňuje několik klíčových kroků, které mají největší dopad na snížení rizik v OT prostředí:

- **Kompletní viditelnost nad OT aktivy:** Organizace potřebují mít přehled o všem, co je v jejich OT sítích, a rozumět tomu. Identifikace zařízení, jejich chování a zranitelností je základ pro jakoukoli další ochranu. Kompenzační kontroly, analýza protokolů a monitorování koncových bodů pomáhají zabránit kompromitaci.
- **Segmentace sítí:** Snížení počtu průniků vyžaduje zabezpečené prostředí OT se silnou kontrolou síťových zásad na všech přístupových bodech. Tento druh obranyschopné architektury začíná vytvořením síťových zón nebo segmentů. Týmy by také

měly vyhodnotit celkovou složitost správy řešení a zvážit výhody integrovaného nebo platformového přístupu s možnostmi centralizované správy.

- **Integrace OT do bezpečnostních operací (SecOps) a plánování reakcí na incidenty:** OT musí být součástí incident response procesů, protože narušení provozních technologií má přímý dopad na výrobu a bezpečnost. Společné postupy IT, OT a výroby zlepšují reakční schopnosti.
- **Platformový přístup k bezpečnostní architecture:** V reakci na rychle se vyvíjející hrozby pro provozní technologie a zvětšující se plochu útoků, mnoho organizací sestavilo širokou škálu bezpečnostních řešení od různých dodavatelů. Výsledkem je příliš složitá architektura, která omezuje viditelnost a zároveň zvyšuje zátěž omezených zdrojů bezpečnostního týmu. Přístup k zabezpečení na jedné platformě může organizacím pomoci konsolidovat dodavatele a zjednodušit jejich architekturu. Robustní bezpečnostní platforma se specifickými funkcemi pro IT sítě i OT prostředí může zajistit integraci řešení pro zvýšení účinnosti zabezpečení a zároveň umožnit centralizovanou správu pro zvýšení efektivity. Integrace může také poskytnout základ pro automatizované reakce na hrozby.
- **Zpravodajství o hrozbách specifické pro OT:** Zabezpečení provozních technologií stojí na rychlé dostupnosti kvalitních informací o hrozbách a na přesné analýze rizik, která mohou ovlivnit provoz. Moderní bezpečnostní architektura proto musí využívat pokročilé nástroje založené na umělé inteligenci, které dokážou detekovat a blokovat útoky téměř v reálném čase, včetně nových variant a neznámých zranitelností. Současně je nezbytné, aby organizace pracovaly se spolehlivými zdroji zpravodajství o hrozbách, které obsahují detailní a aktuální informace specifické pro OT prostředí, a tyto informace integrovaly do svých bezpečnostních procesů a služeb.

Průzkum zahrnuje organizace z odvětví, kde je OT klíčovou součástí provozu: výroba, logistika, zdravotnictví, těžba ropy a plynu, energetika, chemický průmysl a vodárenství. Tato odvětví sdílejí společný problém — rostoucí tlak na zajištění provozní kontinuity v prostředí, kde se kybernetické hrozby stále více prolínají s fyzickými procesy.

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

Jiří KASNER, Předseda představenstva, SYNERIQ a.s.

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

Jaroslav PEJČOCH, Tajemník, The International Emergency Managers Society

Tomáš PŘIBYL, CEO, Corpus Solutions a.s.

Michal ZEDNÍČEK, Cyber Expert, Alef Security

Bohuslav ZŮBEK, Oddělení kybernetické bezpečnosti, Ministerstvo vnitra ČR

Řečníci

Lukáš Březina
CTO Security, TAKTIK

Lukáš vede ve společnosti Taktik technický tým kyberbezpečnosti a zodpovídá za ochranu kritické infrastruktury ve státním i komerčním sektoru.

Specializuje se na architekturu a aktivní správu řešení od lídrů trhu, jako jsou Palo Alto Networks, Thales či Recorded Future.

S více než 10 lety praxe pokrývá jeho tým celý životní cyklus bezpečnosti – od návrhu odolné sítě až po dohled nad SLA a řešení incidentů.

Jako Certifikovaný Etický Hacker (CEH) a Threat Hunter propojuje v krizovém řízení manažerský nadhled s hlubokou znalostí technologií.

Ondřej Hubálek
Cyber Security Presales Engineer, GREYCORTEX

IT profesionál s 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.

Ing. Jiří Kasner, MBA
Předseda představenstva, SYNERIQ, a.s.

Absolvent FEL ČVUT v Praze (Ing.) a VUT v Brně (MBA).

Autorizovaný inženýr ČKAIT pro obory technologická zařízení staveb a technika prostředí staveb – elektrotechnická zařízení.

Zabývá se konzultacemi, koncepčním řešením, designem a celkovým návrhem a provozem komunikačních systémů v kritickém průmyslu. Tato témata přednáší v rámci expertních přednášek na ČZU v Praze a VUT v Brně.

Vilém Markovič
vCISO / Cyber Security Architect, Comma0

Vilém Markovič je zkušený bezpečnostní architekt s téměř 30 lety praxe v IT bezpečnosti v bankovním sektoru, z toho 15 let v roli hlavního bezpečnostního architekta v České spořitelně a.s. Je držitelem certifikací OWASP a členem ISACA.

Odborně se specializuje na cloudovou bezpečnost (IaaS/PaaS/SaaS), správu identit a přístupu (IdP/IdM, federované služby), PKI/HSM infrastrukturu a DevSecOps. Během své kariéry v České spořitelně zastával mimo jiné roli architekta cloudové bezpečnosti a partnera týmů OpsRisk, Compliance a Legal, architekta AI bezpečnosti (Azure OpenAI, ChatGPT) a vedl stream DevSecOps a Identity bezpečnost v agilním prostředí. Byl rovněž architektem síťové bezpečnosti se znalostí SASE, IDS/IPS a SIEM (SOC).

V současnosti působí jako vCISO a bezpečnostní architekt ve společnosti Comma0 s.r.o., kde se věnuje konzultacím v oblasti návrhu bezpečnostních architektur, designům implementace CNAPP/XDR/NDR platforem, cloudové správy a AI a shody s NIS2, ISO 27001, ZKB a AI Act. Souběžně zastává pozici CIO ve společnosti Global Cyber Security s.r.o., specializující se na praktický výcvik bezpečnostních specialistů formou simulací reálných kybernetických útoků a krizových situací na unikátním polygonu (dle metodiky CyberGym Izrael).

Jiří Netuka
Business Development Director, KRUGEL EXIM CZ

Zkušený profesionál s mnohaletou praxí v oblasti networikngu se zaměřením na pasivní infrastrukturu a související kybernetickou bezpečnost.

Aktuálně se v Krugel Exim CZ věnuje především komplexním řešením z hlediska zabezpečení pasivní infrastruktury v návaznosti na potřeby partnerů. V rámci kybernetické bezpečnosti je pak zastáncem praktického a pragmatického přístupu, který partnerům umožňuje efektivní přístup k aplikování požadovaných technologií, a to nejen ve vztahu k aktuálním potřebám ale i těm budoucím.

Ing. Václav Šamša
CEO & CTO, TDP / SecureAnyBox

Ing. Václav Šamša vede od roku 1987 tým, který navrhl, vyvinul a udržoval projekty informačních systémů a IT nástrojů pro domácí i světové zákazníky. Od roku 2000 a 2008 se soustředíme na bezpečnost s produkty SecureAnyBox a KeyShield SSO. Václav mj udržuje intenzivní a pravidelný kontakt s významnými zákazníky a partnery po celém světě a získané zkušenosti převádí se svým týmem do obou produktů.

„Autentizace je prima, ale vaše data neochrání“

Jan Václavík
Systems Engineering Team Lead, FORTINET

Jan Václavík vystudoval obor Kybernetika a řídicí technika na FEL-ČVUT v Praze a nyní působí ve společnosti Fortinet v týmu systémových inženýrů. V oblasti bezpečnosti počítačových sítí se pohybuje už od roku 2008 a za tu dobu nasbíral řadu teoretických i praktických zkušeností. Jeho široké znalosti z oblasti síťové bezpečnosti a předprodejní podpory oceňují mnozí zákazníci i partneři. V rámci své pracovní činnosti se zaměřuje mimo jiné i na obecné prezentace důležitosti pojmu bezpečnosti počítačových sítí.

SYNERIQ

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.

SYNERIQ 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.

SYNERIQ 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.

SPOLEHLIVÝ PARTNER PRO NÁROČNÁ ŘEŠENÍ

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

SYNERIQ 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.

HIRSCHMANN
A BELDEN BRAND

info@syneriq.cz

www.SYNERIQ.cz

SecureAnyBox

Technické účty jako přehlížená slabina i v prostředích, ve kterých byly proinvestovány značné prostředky v oblasti bezpečnosti.

Jen tam ještě chybí SecureAnyBox.

Téměř všude najdete účty, které se naposledy změnily dříve, než současný správce nastoupil do práce. Nikdo se neodvažuje na ně byť jen sáhnout, protože jsou využívány různými automatickými i poloautomatickými službami a programy, bez kterých se prostě nelze obejít. Správci vědí, že za slabou bezpečnost je nikdo nevyhodí, potažmo se na ni ani nepřijde. Ale pokud neproběhne proces a ráno chybí data, všichni to vidí. A nakonec zjistí, že to způsobil správce, který z pilnosti změnil dvacet let staré šestiznakové heslo technického účtu na nové. Asi také i delší a lepší, ale hlavně nové. Takže už ho sto jeho kolegů a předchůdců neví.

V praktickém životě správce prostředí, postaveném na technologiích Microsoft, to je také o účtech pro:

- PRIVILEGED LOCAL USER (Admin)
- AUTOLOGON
- SYSTEM SERVICE
- SCHEDULED TASK
- IIS APP POOL

Nejde o to, zda máte nějaký doplněk, který správcům ve jménu vyšší bezpečnosti komplikuje přístup k výše uvedenému. Jde o to, že tak to prostě je. A že mnoho produktů, které běžný zákazník využívá, je v kategorii LEGACY nebo dokonce OBSOLETE. Že jsou to skripty vytvořené najatým konzultantem a spouštěné každou noc. Nejen NIS2, ale i zdravý rozum velí hesla těchto účtů rotovat. Zamezit tomu, že je někdo "ví" a že je ví již léta a že už dávno odešel jinam.

Na konferenci prezentujeme řešení SecureAnyBox, které nabízí kompletní řešení pro rotaci všech technických účtů. Všeho, co je vyjmenováno výše. I účtů, které potřebuje programátor použít, ale Vy nechcete, aby je měl v kódu nebo konfiguračním souboru.

Uděláme při prezentaci maximum, ale představit celé řešení trvá několik hodin. Nejde to zvládnout za pár minut. Uděláme maximum, ale přesto - ozvěte se nám na sales@tdp.cz. Budeme se Vám věnovat. Nebo Vám doporučíme někoho z našich odborných partnerů. Nebo se budeme věnovat vašemu oblíbenému dodavateli, od kterého bude chtít řešení všeho výše uvedeného.

TAKTIK

MODERNÍ A BEZPEČNÁ IT ŘEŠENÍ

INFRASTRUKTURA NEJEN PRO DATOVÁ CENTRA

Hyperkonvergovaná infrastruktra s možností volby HW platformy i hypervisoru

Datová úložiště pro produkční i sekundární účely s nekompromisním výkonem, rozšiřitelností i zabezpečením

KYBERBEZPEČNOST

Firewally nové generace, ochrana koncových stanic, kontejnerů či cloudu

Šifrování datových linek a propojení na úrovni armádních bezpečnostních standardů

Threat Intelligence platforma s rozsáhlou databází aktuálních i historických bezpečnostních hrozeb

REFERENČNÍ PROJEKTY V PROSTŘEDÍ VELKÝCH ZÁKAZNÍKŮ

www.taktik.cz

KRUGEL EXIM CZ

www.krugel.cz

INOVACE

Krugel Exim CZ přináší efektivní a inovativní řešení přizpůsobené specifickým potřebám uživatelů. Vícero produktů vyvinul a certifikoval mezi prvními na světě a zasloužil se tak o rozšíření cenově dostupných a pokrokových řešení.

KONTROLA KVALITY

Nezávislé akreditované zkušebny FORCE Technology, 3P a GHMT vykonávají pravidelný audit výrobních zařízení, kontrolu kvality a shody s mezinárodními normami klíčových komponentů.

CERTIFIKOVANÍ PARTNEŘI

Partnerský program zabezpečuje koncovému uživateli rychlou dostupnost produktů, jejich odborné nainstalování a dlouholetou systémovou záruku.

25 LETÁ SYSTÉMOVÁ ZÁRUKA

Na všechny instalace strukturované kabeláže, realizované certifikovaným partnerem, po auditu zkušebních protokolů, poskytuje výrobce systémovou záruku 25 let.

FUTURE OF CYBER KONFERENCE

21.–23. října 2026

PVA EXPO PRAHA

GREYCORTEX MENDEL

Viditelnost ICS jako základ ochrany kritické infrastruktury

Průmyslové řídicí systémy jsou stále častěji propojeny s externími sítěmi, aniž by organizace měly přehled o skutečné komunikaci v OT prostředí.

Útočníci využívají skryté služby, nezabezpečené protokoly a nezdokumentovaná zařízení, která tradiční IT bezpečnostní nástroje neodhalí.

GREYCORTEX Mendel mění pravidla hry. Poskytuje detailní vhled do komunikace průmyslových zařízení, identifikuje anomálie v reálném čase a pomáhá předcházet incidentům dříve, než ovlivní kontinuitu provozu. Bezpečnost ICS pro nás není jen o ochraně dat, ale o stabilitě celého výrobního procesu.

SPRÁVA AKTIV

Přehled o všech zařízeních v síti, včetně těch nezdokumentovaných.

DETEKCE ANOMÁLIÍ

Včasné varování před kyberútoky i technickými závadami v reálném čase.

VIDITELNOST OT PROTOKOLŮ

Rozumíme OT protokolům jako Modbus, IEC 104, PROFINET a další.

PLYNULÝ PROVOZ

Pasivní monitoring bez rizika ovlivnění nebo zpomalení kritické infrastruktury.

Pomáháme vám vidět hrozby dřív než útočníci

→ **www.greycortex.com**

Partneři konference

SYNERIQ, a.s.

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

FORTINET

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

Fortinet je hnací silou vývoje kybernetické bezpečnosti a konvergence síťových a bezpečnostních technologií. Jejím posláním je zabezpečit uživatele, zařízení a data na všech místech. Poskytuje tak kybernetickou bezpečnost všude tam, kde ji uživatelé potřebují, a to díky nejrozsáhlejšímu a nejucelenějšímu portfoliu řešení zahrnujícímu více než 50 produktů podnikové třídy. Řešením společnosti Fortinet, která patří k nejrozšířenějším, nejčastěji patentovaným a nejlépe ověřeným na trhu, důvěřuje přes půl milionu zákazníků.

HLAVNÍ 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.

www.cloudfield.cz / www.comma0.io

Comma0 s.r.o., dceřiná společnost Cloudfieldu, je poradenská firma specializující se na kybernetickou bezpečnost a IT architekturu pro různé druhy zákazníků včetně regulovaného prostředí. Zaměřuje se na návrh a posuzování bezpečnostních architektur v oblastech cloud security (Azure IaaS/PaaS), identity a access managementu, PKI/HSM a DevSecOps, SOC.

Firma poskytuje expertní konzultace při výběru a implementaci bezpečnostních řešení – od CNAPP (XDR, CSPM) platforem přes SIEM a NDR až po compliance s regulatorními rámci NIS2 a ISO 27001. Díky hlubokým zkušenostem z bankovního sektoru a kritické infrastruktury dokáže Comma0 překládat mezi technickou hloubkou a business potřebami klienta – ať už jde o strategické rozhodnutí v oblasti bezpečnosti nebo podporu nebo hands-on security design.

PARTNER KONFERENCE

TAKTIK

TAKTIK, a.s.

Ohradské náměstí 2826/6
155 00 Praha 5
+420 222 703 900
taktik@taktik.cz
www.taktik.cz

Taktik je moderní a dynamická IT firma se zaměřením na bezpečnost a infrastrukturu.

V týmu jsou certifikovaní profesionálové s dlouholetými a prokazatelnými zkušenostmi, kteří se starají o kritickou infrastrukturu zákazníků velkých firem i veřejné správy. Kromě obchodní a technické podpory nabízí možnost vyzkoušení nabízených řešení ve vlastním prostředí i pomoc s pilotními projekty.

Taktik se specializuje na netradiční a novátorská řešení, která přinášejí velkou přidanou hodnotu při maximálním využití vynaložených prostředků.

PARTNER KONFERENCE

KRUGEL EXIM CZ

KRUGEL EXIM CZ

Na návsi 6/19
620 00 Brno – Holásky
+420 545 232 258
info@krugel.cz
www.krugel.cz

KRUGEL EXIM CZ patří mezi významné české VAD distributory v oblasti pasivní infrastruktury. Již téměř 30 let spolupracujeme s předními výrobci strukturovaných kabeláží a pomáháme partnerům i koncovým zákazníkům budovat kvalitní a spolehlivé sítě. Odbornost, osobní přístup a dlouhodobé vztahy s našimi partnery pak vnímáme jako základní stavební kámen firemní filosofie, která nám pomáhá zdárně řešit i ty na první pohled nejkomplikovanější situace.

PARTNER KONFERENCE

SecureAnyBox 5

TDP, s.r.o. / SecureAnyBox

Bohúňova 1336/13
149 00, Praha - Chodov
sales@tdp.cz
www.tdp.cz

Značka Továrna na Dokonalé Programy, založená v roce 1989, se napříč svou existencí zabývala nespočtem odvětví ve světě informačních technologií – od tvorby informačních systémů, přes budování síťových prostředí a záchranu dat až po vývoj softwaru.

Na vývoji bezpečnostních produktů, jako jsou SecureAnyBox a KeyShieldSSO, pracujeme od začátku století dodnes. Díky výsledkům naší práce se můžeme pyšnit partnery napříč pěti světovými kontinenty.

PARTNER KONFERENCE

Future Forces
EXHIBITION & FORUM

21. – 23. 10. 2026 | PRAHA

Mezinárodní veletrh
a odborné fórum
o trendech, technologiích
a řešeních v oblasti
obrany a bezpečnosti

V rámci

FUTURE FORCES FORUM

www.FFF.global

Generální partner

CSG Czechoslovak Group