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

Bezpečnostní konference

SCADA SECURITY

Součástí Future Forces Forum

27. dubna 2023

Mladá Boleslav, Škoda Auto Museum

Hlavní partner konference

COLSYS AUTOMATIK

HIRSCHMANN
A BELDEN BRAND

Partneři konference

ALEFNULA

GREYCORTEX

Bohemia Market.cz

Progress Flowmon

Barracuda

BDO

ŠKODA

FUTURE FORCES FORUM

Partneři FFF pro vědu a výzkum

ČVUT ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Univerzita obrany

Generální partner Future Forces Forum

LOCKHEED MARTIN

Partner Future Forces Forum

RESCUE TRAILER

COLSYS
AUTOMATIK

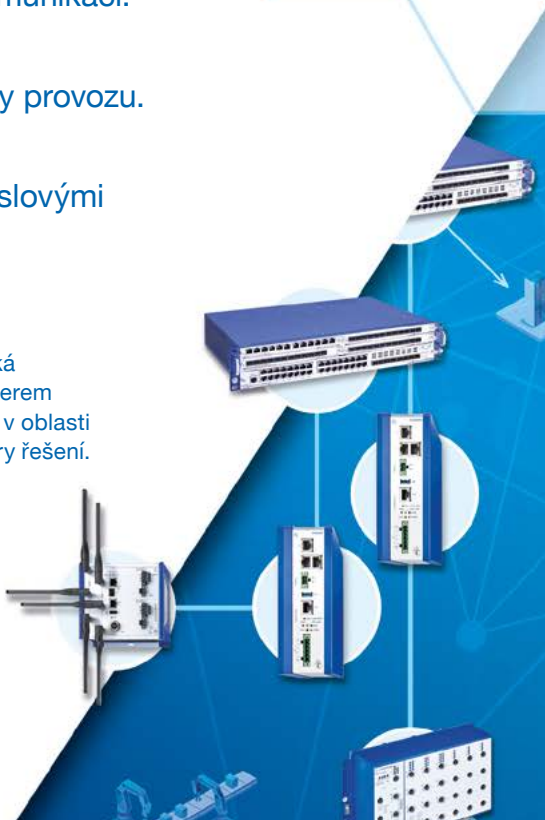
HIRSCHMANN
A BELDEN BRAND

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.

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.

Podívejte se na náš YouTube kanál
COLSYS – AUTOMATIK, a.s.



www.colaut.cz
obchod@colaut.cz

Odborný programový garant

AFCEA

Záštita a odborná garance

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

Úřad pro ochranu osobních údajů

Hospodářská komora České republiky

Ministerstvo průmyslu a obchodu

ict unie

Univerzita obrany

ČIMIB

Centrum kybernetické bezpečnosti

Jsem rád, že mohu moderovat takovouto konferenci. Jsem u elektroniky a softwaru už mnoho let, zažil jsem i první legrační viry na PC, ale teď je to o něčem jiném. Naše totální závislost na informační infrastruktuře, systémech a informacích nás nutí je chránit jako oko v hlavě a to nejen na technické, ale i na procesní úrovni. Všechno je propojeno se vším a je stále obtížnější hlídat rizika a chránit se před úmyslnými i neúmyslnými selháními, které mohou mít zejména v kritické infrastruktuře pro společnost fatální důsledky.

Vítám proto každou možnost, kdy se mohou sejít odborníci a prezentovat a diskutovat své zkušenosti, poznatky a názory. Věřím, že to, o čem budou mluvit naši řečníci, nás posune dopředu ve vnímání reality a inspiruje k vytváření budoucnosti.

Jaroslav Pejčoch
Člen představenstva
ICT UNIE

Vážení přátelé a příznivci kybernetické bezpečnosti,

jsem velmi rád, že se vám dostává do ruky tento katalog konference „SCADA Security 2023“.

Oblast kybernetické bezpečnosti je jednou z těch, kterým se v poslední době dostalo velké pozornosti a důležitosti. Je jasné, že tato všeobecná pozornost souvisí zejména s okolnostmi let posledních, ale i tak je téma bezpečnosti systémů, zejména v průmyslových a kritických aplikacích, tématem již letitým.

Bohužel, zvýšená všeobecná pozornost často nejde úplně ruku v ruce s porozuměním tématu jako takovému. Často se tato zvýšená pozornost přetaví v „papírový“ zájem, který s sebou nese málo přemýšlení a konstruktivních úvah na základě solidních znalostí. Naopak s sebou často nese velký objem administrativní práce se značným nedostatkem znalostí a přemýšlení.

Konference „SCADA Security 2023“ se snaží odbornou formou rozšířit obzor a znalosti posluchačů, aby se vám dařilo více ve skupině první, tedy té, která má znalosti a konstruktivně přemýšlí nad tématem bezpečnosti.

Přeji vám v této věci dobré znalosti a konstruktivní přístup. To jsou základní stavební kameny jakékoliv bezpečnosti, protože nesystémový a zmatečný přístup s chabými znalostmi je velmi dobrou živnou půdou pro ty, kteří tyto vlastnosti chtějí využít (a tedy typicky zneužít).

Věřím, že pro vás bude tato konference a informace z ní přínosem.

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

Jsem potěšen, že jsme opakovaně součástí konference SCADA, na které můžeme promluvit o aktuálních tématech kybernetické bezpečnosti, jejichž důležitost roste s počtem a závažností kybernetických bezpečnostních incidentů.

Naším hlavním úkolem je řešit okamžité digitální potřeby v oblastech kybernetické bezpečnosti, digitalizace, ale také IT compliance a regulace. Právě vznikající zákon o kybernetické bezpečnosti, který vychází o evropské směrnice NIS2, sdružuje dosavadní roztříštěnou úpravu několika typů povinných osob do jedné – poskytovatele regulované služby.

Novým kritériem pro regulované služby je velikost organizace. Dramaticky se rozšiřuje počet povinných osob z celkového počtu 400 organizací odhadem na 6000. Naplnit požadavky zákona tak budou muset organizace uvedeny v příloze Vyhlášky o regulovaných službách s velikostí podniku střední nebo velké. Je také důležité zmínit, že je upraveno pravidlo sčítání velikosti podniků. Pokud je malá společnost součástí holdingu, může z ní být rázem velká. Návrh českého zákona do regulace vtahuje některé subjekty dle poskytované služby bez ohledu na jejich velikost.

V praxi to bude pro podniky mimo jiné znamenat zavedení rozsahu řízení kybernetické bezpečnosti a bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů a informování svých zákazníků, provádění protiopatření, zavedení mechanismu řízení bezpečnosti dodavatelského řetězce (v případě poskytovatelů ve vyšším režimu povinností) nebo podřízení kontrol inspektorům či dozorovému orgánu.

Při nedodržení zákonných povinností hrozí firmám pokuta až ve výši 230 milionů korun. Posílili jsme tak náš tým, abychom byli připraveni nabídnout pomoc našim klientům dosáhnout souladu se zákonem

Věřím, že na konferenci bude prostor k diskusi nejen o tomto, ale i dalších důležitých tématech. Těším se na setkání s Vámi.

Martin Hořický
Partner, Cybersecurity
BDO

Vážení účastníci konference SCADA Security,

je mi ctí napsat několik úvodních slov do sborníku této konference.

Jak sami dobře víte (a proto jste nejspíš také tady), kybernetická bezpečnost průmyslových systémů se v posledních letech stává stále palčivějším problémem. Už dávno neplatí, že IT a OT jsou oddělené světy a že průmyslové řídící systémy jsou fyzicky izolované a kybernetickými útočníky nedotknutelné. Kybernetické útoky totiž nectí hranice.

Jsme si pravděpodobně všichni vědomi rizik, která mohou mít zásadní dopady na systémy klíčové pro fungování kritických infrastruktur, ať už jde o energetické sítě, průmyslové výrobní linky, nemocnice nebo dopravní infrastruktury.

V posledních letech vidíme, jak se útoky na průmyslové systémy stávají stále častějšími. I když se jedná o reálný problém, existují technologie a postupy, které nám pomohou se těmto útokům bránit. Průmysloví hráči i vládní organizace se stále více snaží zlepšit svou kyberbezpečnost, aby zajistili bezpečnost a spolehlivost svých infrastruktur. Přispěje tomu snad i nová směrnice Evropské unie o kybernetické bezpečnosti, kterou většina z vás zná pod pojmem NIS2. Byť pro mnohé může být strašákem, který některé věci zkomplikuje, věřím, že nám přinese naopak nové příležitosti.

Ani já vás strašit nechci. Věřím totiž, že kybernetická bezpečnost (nejen) průmyslových systémů je výzva, které jsme schopni společně čelit a zajistit jejich spolehlivý a bezpečný provoz.

Je důležité, abychom se v oblasti kybernetické bezpečnosti dále rozvíjeli a neustále vylepšovali své postupy a technologie. Řečníci konference SCADA Security zajisté přinesou inspiraci i nejnovější poznatky a procesy při ochraně průmyslových systémů. Tuto konferenci vnímám jako inspirativní příležitost k výměně nápadů a řešení, která nám pomohou zlepšit kybernetickou odolnost a bezpečnost průmyslových systémů.

Přeji vám všem podnětná setkání a novou pozitivní inspiraci k vaší práci.

Petr Chaloupka
CEO, GreyCortex s.r.o.

Vážené dámy a pánové,

s rostoucí digitalizací průmyslové výroby se nové, ale i stávající, hrozby v oblasti informační bezpečnosti stávají relevantními pro stále širší oblast firem. Aktuálně zveřejněné detaily tzv. „Vulkan files" potvrzují dřívější domněnky o propojení hackerských skupin se zahraničními aktivitami vládních agentur, a proto nejen pro ŠKODA AUTO a.s. je klíčové zajistit robustní bezpečnostní opatření nejen na technické úrovni, ale i na úrovni spolupráce s ostatními subjekty kritické infrastruktury. Jsem rád, že spolupráce v rámci pracovních skupin kybernetické bezpečnosti organizace AFCEA nám umožňuje být v kontaktu s odbornou bezpečnostní komunitou v České republice.

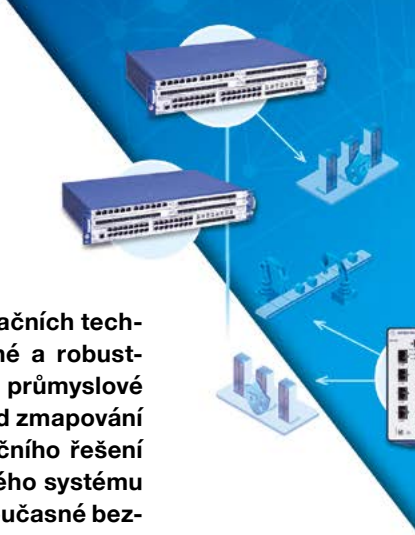
Stále platí, že bezpečnost není stav, ale proces. Kromě výměny informací si ceníme i možnosti být podporovatelem při rozšiřování povědomí o bezpečnostních hrozbách a obraně proti nim. ŠKODA AUTO a.s. investuje nemalé prostředky do implementace vícevrstvé bezpečnostní architektury, šifrované komunikace a dat, vícestupňového ověřování uživatelů a dnes tolik populárního konceptu „Zero trust", ovšem tou nejdůležitější investicí jsou pravidelná školení a osvěta reagující na aktuální hrozby.

Cílem spolupráce v rámci SCADA Security konference je být připraveni na minimalizaci dopadů kybernetických hrozeb vůči naší společnosti, ale i vůči prostředí našich partnerů a dodavatelů v automobilovém průmyslu. Rozvoj nových talentů je nedílnou součástí procesu zvyšování úrovně bezpečnosti a proto jsem rád, že mohu přivítat účastníky letošního finále ročníku středoškolské kybernetické soutěže a SCADA Security konferenci v Mladé Boleslavi v Muzeu ŠKODA AUTO. Těším se na setkání s Vámi.

Marek Hlávka
CISO ŠKODA AUTO a.s.

www.colaut.cz obchod@colaut.cz

Podívejte se na náš YouTube kanál COLSYS – AUTOMATIK, a.s.



Průmysl je v současné době zcela závislý na komunikačních technologiích. Pro spolehlivý chod je zapotřebí bezpečné a robustní prostředí. Společnost COLSYS – AUTOMATIK pro průmyslové podniky zajišťuje kompletní rozsah této oblasti, a to od zmapování aktuálního stavu včetně analýzy rizik, návrhu projekčního řešení až po kompletní konfigurační parametry a dodání celého systému včetně servisu. „Staré technologie často nezvládají současné bezpečnostní požadavky, proto je potřeba najít jiný způsob ochrany," vysvětluje Jiří Kasner ze společnosti COLSYS – AUTOMATIK, která se průmyslové komunikaci věnuje už dvacet let.

Provoz průmyslových podniků je závislý na bezpečných komunikačních systémech

Podcenění rizik stojí peníze

Spousta firem podceňuje zabezpečení průmyslové komunikace včetně kritické infrastruktury. Často si možná rizika ani neuvědomují. Výpadky a narušení pak ale značně komplikují provoz a stojí nemalé peníze. Je zásadní finanční rozdíl v tom, jestli vám nefunguje hodinu poštovní klient nebo turbína. Nechte zkušené odborníky nahlédnout do vašich průmyslových komunikačních systémů. Analýza rizik a návrhy řešení, která budou kombinovat robustnost ve smyslu záložních systémů a bezpečnost, povedou ke spolehlivému zajištění provozu. Kdo je připraven, není překvapen. Zde to platí dvojnásob.

COLSYS AUTOMATIK

HIRSCHMANN
A BELDEN BRAND

HiSecOS
Hirschmann™ Security Operating System

Program konference

27. DUBNA 2023 — Muzeum Škoda Auto, Mladá Boleslav

12.15 - 12.20	Úvodní slovo **Jaroslav PEJČOCH**, Člen představenstva, **ICT UNIE**
12.20 - 12.40	Nová směrnice EU o kybernetické bezpečnosti NIS2 **Petra LOMPEJOVÁ**, Oddělení regulace soukromého sektoru, **NÚKIB**
12.40 - 13.10	Bezpečná průmyslová komunikační infrastruktura – jak ano a jak ne… **Jiří KASNER**, Předseda představenstva, **COLSYS – AUTOMATIK**
13.10 - 13.35	OT a IT jsou si blíže, než se zdá **Pavel MINAŘÍK**, VP, Technology, **PROGRESS/FLOWMON**
13.35 - 14.00	Malé i velké výzvy a úspěchy v zabezpečení kritických OT aktiv **Marnix JANSE**, Oddělení OT security research, **GREYCORTEX**
14.00 - 14.20	IT bezpečnost ve výrobě **Erik ZAPLETAL**, Architekt kybernetické bezpečnosti pro oblast výroby, **ŠKODA AUTO**
14.20 - 14.45	přestávka
14.45 - 15.10	Kybernetická bezpečnost – „Jsme docela v bezpečí“ – Opravdu!? **Petr ROUPEC**, CEO & Prezident, **BOHEMIA MARKET**
15.00 - 15.35	Modelování hrozeb (nejen) pro průmyslová prostředí **Jan KOPŘIVA**, Cybersecurity Consultant, **ALEF NULA**
15.35 - 16.00	Řízení rizik dodavatelského řetězce, standardy pro Manufacturing, hodnocení jeho rizik a modelování hrozeb **Martin HOŘICKÝ**, Partner, Digital Services, **BDO**
16.00 - 16.25	Polygon operačních technologií na NÚKIB **Jan ZDRHA**, Oddělení bezpečnosti operačních technologií, **NÚKIB**
16.25 - 16.50	Kybernetická bezpečnost železnic **Jakub JANČÍK**, Account Manager CEE, **BARRACUDA**
16.50 - 17.00	Prostor pro dotazy a závěrečné slovo **Jaroslav PEJČOCH**, člen představenstva, **ICT UNIE**

moderuje: Jaroslav Pejčoch, člen představenstva, ICT Unie
Změny v programu vyhrazeny.

Jste si jisti, že víte, co se děje ve vaší síti?

Síť představuje společného jmenovatele v jinak heterogenním prostředí systémů SCADA, které se liší nejen napříč obory, ale dokonce i mezi jednotlivými podniky. Detekce nežádoucího chování v síti je nutným a univerzálním způsobem, jak výrazně posílit zabezpečení SCADA systémů.

Zabezpečení průmyslových sítí a systémů je dnes výzvou pro všechny operátory SCADA/ICS. Již dávno totiž neplatí, že bezpečnost průmyslových kontrolních 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.

Většina zařízení v prostředí SCADA/ICS nebyla v minulosti navrhována na to, aby byla bezpečná. Dlouho těžila z toho, že byla jen oddělena od tradičních počítačových sítí, což ji dostatečně chránilo proti klasickým počítačovým útokům. Většina zařízení v prostředí ICS totiž nevyžaduje ověření ani nedisponuje správou přístupu ke kritickým částem systému. Často chybí také logy a záznamy, které by bylo možné zpětně využít v rámci detekce nebo sledování proběhlých událostí.

V současnosti se kromě silného zabezpečení systémů SCADA/ICS vyžaduje také jejich interoperabilita a přenositelnost. Důvody jsou nasnadě, těžit z agregace dat, vzdálené správy nebo se lépe rozhodovat se znalostí kontextu.

Progress Flowmon – klíčem je viditelnost

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. Byl distribuován pomocí klasických phishingových aktivit prostřednictvím sociálního inženýrství a způsobil vážné selhání v dodávkách elektrické energie pro stovky obcí. Existují však i běžnější kybernetické hrozby cílené na organizační síťovou infrastrukturu, jako jsou například botnety. Bez vhodné monitorovací technologie jako je řešení Progress Flowmon jsou podobné hrozby pro administrátory v podstatě neviditelné.

Nový přístup k zabezpečení SCADA sítí

Tradiční monitoring zastoupený protokolem SNMP 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. Řešení spočívá v monitorování provozu datové sítě a nasazení technologie NDR (Network Detection and Response) prostřednictvím řešení Flowmon. To využívá k odhalení podezřelého chování v síti strojové učení, heuristiku a pokročilou analytiku a je tak je schopno odhalit i nové nebo dosud neznámé hrozby a útoky. Klíčovou vlastností a konkurenční výhodou je pokrytí jak oblasti OT, tak i IT (včetně hybridního prostředí organizace) jediným řešením, které dokáže reagovat na hrozby napříč firemní infrastrukturou. Navíc předkládá administrátorům užitečné a srozumitelné informace v oblasti provozního i výkonnostního monitoringu, tedy nejen bezpečnosti.

Shrnutí

Absence šifrované komunikace, chabý autentifikační mechanismus, zastaralé systémy i postupné propojování OT a IT prostředí činí průmyslové sítě a řídící systémy značně zranitelné vůči současným kybernetickým hrozbám. Sbližování prostředí OT a IT tak kromě nesporných výhod přináší i nové výzvy.

www.flowmon.com

Programový výbor konference

Petr JIRÁSEK
Předseda pracovní skupiny kybernetické bezpečnosti, AFCEA ČP
Předseda

Doc. **Josef POŽÁR**, CSc.
Emeritní prorektor, Policejní akademie České republiky v Praze
Čestný předseda

Členové

Jan DIENSTBIER
Víceprezident, ČIMIB

plk. **Petr HRŮZA**
Prorektor, Univerzita obrany

Jaroslav PEJČOCH
Člen představenstva, ICT Unie

Tomáš PŘIBYL
Místopředseda pracovní skupiny kybernetické bezpečnosti, Česká pobočka AFCEA

Vladimír ROHEL
Bezpečnostní ředitel, Národní agentura pro komunikační a informační technologie

Tomáš TRÁVNÍČEK
FIG/2 Řízení informační bezpečnosti, ŠKODA AUTO a.s.

Bohuslav ZŮBEK
Oddělení kybernetické bezpečnosti, Ministerstvo vnitra ČR

Tisíce firem budou muset povinně investovat do své kyberbezpečnosti

Zejména střední a velké podniky by měly zbystřit v souvislosti se vznikajícím zákonem o kybernetické bezpečnosti. Nově mohou totiž spadat pod jeho regulaci. Smyslem zákona je zlepšení odolnosti digitální infrastruktury proti narůstajícím kybernetickým útokům, a to na půdě celé Evropské unie. Ostatně i vznikající zákon, jehož účinnost je očekávána od poloviny roku 2024, vychází z evropské směrnice NIS2, která zavazuje subjekty v rámci EU, aby zajistili bezpečnost svých sítí a informačních systémů.

Vznikající zákon o kybernetické bezpečnosti, který již prochází připomínkovým procesem, sdružuje dosavadní roztříštěnou úpravu několika typů povinných osob do jedné – poskytovatele regulované služby. Poskytovatelé jsou dále regulováni dle Vyhlášky o regulovaných službách. Ta je rozděluje podle způsobu plnění zákonných povinností na poskytovatele v nižším a vyšším režimu.

Novým kritériem pro regulované služby je velikost organizace. Dramaticky se rozšiřuje počet povinných osob z celkového počtu 400 organizací odhadem na 6000. Naplnit požadavky zákona tak budou muset organizace uvedeny v příloze Vyhlášky o regulovaných službách s velikostí podniku střední nebo velké. Je také důležité zmínit, že je upraveno pravidlo sčítání velikosti podniků. Pokud je malá společnost součástí holdingu, může z ní být rázem velká. Návrh českého zákona do regulace vtahuje některé subjekty dle poskytované služby bez ohledu na jejich velikost. Zákon tak naplňuje povinné požadavky směrnice, ale je dále důrazněji specifikován. To ve skutečnosti znamená, že pokud z povahy NIS2 vaše organizace do regulace nespadala, je možné, že bude do české úpravy zákona vtažena.

V praxi to bude pro podniky mimo jiné znamenat zavedení rozsahu řízení kybernetické bezpečnosti a bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů a informování svých zákazníků, provádění protiopatření, zavedení mechanismu řízení bezpečnosti dodavatelského řetězce (v případě poskytovatelů ve vyšším režimu povinností) nebo podřízení kontrol inspektorům či dozorovému orgánu.

Při nedodržení zákonných povinností hrozí firmám pokuta až ve výši 230 milionů korun.

Pomůžeme vám

Posílili jsme náš tým a jsme připraveni nabídnout pomoc našim klientům dosáhnout souladu se zákonem. Vše bude založeno na počáteční srovnávací GAP analýze, kde zjistíme aktuální situaci vašeho podniku vůči novelizovanému zákonu. Jsme k dispozici i pro konzultace při implementaci navrhovaných změn pro dosažení souladu vaší organizace s regulací a vyhnutí se tak nemalým pokutám, vyplývajících z regulace.

martin.horicky@bdo.cz

Řečníci

Martin Hořický
Partner, BDO

Martin se připojil k BDO v roce 2005, v současné době působí na pozici Partner. Věnuje se oblasti IT a pracuje na IT auditech. Zaměřuje se na audity IT bezpečnosti, kybernetické bezpečnosti a kromě jiných oblastí také audity založené na SOC2, HIPAA, ISO 27x, NIST a CSA. Mezi jeho rozsáhlé znalosti patří zabezpečení sítě, kybernetická bezpečnost, penetrační testování, řízení rizik ICT, konzultace s vývojem SW a řízení vztahů s dodavateli v souvislosti s IT a bezpečností IT. Martin řídí zakázky v oblasti IT pro různorodé klienty mj. v oblastech IT auditu, ověřovacích zakázkách, či kybernetické bezpečnosti.

Řízení rizik dodavatelského řetězce, standardy pro Manufacturing, hodnocení jeho rizik a modelování hrozeb

Jakub Jančík
Account Manager CEE, Barracuda

Jakub Jančík se aktivně věnuje kybernetické bezpečnosti několik let, počínaje studiem na VUT v Brně, následně pracoval pro start up zabývající se kybernetickou bezpečností se zaměřením na síťový provoz a aktuálně pracuje pro Barracuda Networks, kde pomáhá tuzemským klientům s otázkou zabezpečení e-mailů, aplikací, sítí a ochranou dat.

Kybernetická bezpečnost železnic

Marnix Janse
OT Product Manager, GREYCORTEX

Jako produktový manažer je Marnix Janse ve firmě GREYCORTEX zodpovědný za výzkum a vývoj té části produktu Mendel, která zajišťuje bezpečnost průmyslových sítí. Se svým týmem vytvořil také mikrosenzor pro asset discovery. Ten zjišťuje identifikační údaje z OT zařízení, a pomůže tak s bezpečnostními audity OT sítí nebo jejich základním nastavení a posoudí zranitelnosti zařízení v síti.

Malé i velké výzvy a úspěchy v zabezpečení kritických OT aktiv

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.

Bezpečná průmyslová komunikační infrastruktura – jak ano a jak ne…

Efektivní přístup ke kybernetické bezpečnosti v průmyslových a specifických prostředích

Přes svou historii jsou moderní průmyslové a specifické (zdravotnické, dopravní…) systémy ve vybraných aspektech v současnosti již relativně často blízké klasickým informačním technologiím. Řada výrobních, kontrolních i dalších procesů, které dříve zajišťovaly úzce specializované OT technologie, je v současnosti řízena či monitorována s pomocí systémů, které poskytují interakční rozhraní v podobě webových stránek, komunikují s pomocí tradičních síťových protokolů po IP sítích, či dokonce vycházejí z koncepce internetu věcí.

Tyto moderní systémy jsou pak v produkčních prostředích nezřídka využívány paralelně s klasickými OT technologiemi, které jsou principiálně blíže tradiční automatizační a zabezpečovací technice, než světu informačních technologií.

Zejména v podobných „hybridních" průmyslových a specifických prostředích, avšak nejen v nich, je pak efektivní řízení kybernetické bezpečnosti přinejmenším netriviálním úkolem. Mimo jiné proto, že pro zabezpečení moderních a tradičních systémů je nezbytný různý přístup, ač u obou musí být zpravidla akcentována dostupnost nad zbytkem CIA triády (resp. musí být akcentovány faktory RAMS – tedy spolehlivost, dostupnost, udržovatelnost a bezpečné fungování – spíše než CIA triáda).

Obecný přístup k (nejen) kybernetické bezpečnosti založený na analýze a řízení rizik relevantních pro chráněná prostředí je samozřejmě plně využitelný, avšak musí při něm být zohledněna některá specifika průmyslových systémů. Vedle principiálních požadavků dobré odborné praxe v podobě relevantních odborných standardů (např. IEC 62443) a architektonických zásad (především PERA) je jednou z významných oblastí, v nichž je nezbytné zohlednit zvláštnosti průmyslových a specifických systémů, problematika identifikace a modelování hrozeb.

Mezi metodiky, které je možné v této oblasti efektivně využít, patří mj. STRIDE, tradiční metodika pro modelování hrozeb zejména pro SW systémy. Její použití je však vhodné především při modelování hrozeb pro jednotlivé systémy, nikoli celá průmyslová prostředí. Pro identifikaci hrozeb v rámci komplexních průmyslových a specifických prostředí (resp. „systémů systémů") pak může být vhodná mj. metodika založená na tvorbě tzv. stromů útoků.

Nad rámec výše uvedených metodik však mohou být extrémně efektivní i méně tradiční přístupy k modelování hrozeb založené na rámci MITRE ATT & CK a bezpečnostní metodice OSSTMM.

Bez použití těchto, či jiných relevantních metodik a přístupů lze relevantní rizika identifikovat pouze na základ tradičních a do jisté míry „standardizovaných" katalogů hrozeb, které jsou (nejen) pro průmyslová a specifická prostředí zpravidla nedostačující. Zejména v prostředích, v nichž není možné zajistit bezpečnost oddělením různých typů systémů plně v souladu s „Purdue architekturou" (resp. její rozšířenou variantou uvedenou na obrázku) je tak bezpochyby namístě jedno z těchto metodik pro identifikaci relevantních hrozeb využít…

„Zdroj: NIST".

Zajímá Vás toto téma více?
Kontaktujte: cz-sales@alefnula.com

Jan Kopřiva
Cybersecurity 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.

Modelování hrozeb (nejen) pro průmyslová prostředí

Mgr. Bc. Petra Lompejová
Oddělení regulace soukromého sektoru, NÚKIB

Absolvovala Filosofickou a Právnickou fakulty Masarykovy univerzity, na oddělení regulace soukromého sektoru Národního úřadu pro kybernetickou a informační bezpečnost se věnuje regulaci kybernetické bezpečnosti. Zaměřuje se především na problematiku výkladu zákona o kybernetické bezpečnosti a jeho prováděcích právních předpisů, a aktuálně se podílí se na návrzích novelizace zákona o kybernetické bezpečnosti v souvislosti s přijetím směrnice NIS2.

Nová směrnice EU o kybernetické bezpečnosti NIS2

Pavel Minařík
VP, Technology, Progress

Absolvent Fakulty Informatiky Masarykovy Univerzity v Brně. Během profesní kariéry se účastnil řady výzkumných projektů v oblasti kybernetické bezpečnosti a je autorem desítky publikací a algoritmů tzv. behaviorální analýzy shrnuté v doktorské práci “Building a System for Network Security Monitoring”. V současné době pracuje jako viceprezident pro technologie pro oblast AX (Application eXperience) ve společnosti Progress Software a zodpovídá za technologickou strategii a inovace produktů.

OT a IT jsou si blíže, než se zdá

Petr Roupec
CEO & Prezident, BOHEMIA MARKET

Vizionář a CEO společnosti Bohemia Market CZ.
Odborník na automatizaci, UNIX, sítě a I&C inženýrství.
Zkušený manažer v oblasti elektrotechniky, přístrojové techniky a řízení
Teleperm XP & T2000, T3000 – DCS systém Siemens používaný pro řízení elektráren, konfigurace, uvedení do provozu, řešení problémů, údržba.
Rozsáhlé zkušenosti v oblasti sítí (směrování, průmyslové sítě, ladění).

GREYCORTEX

Kyberbezpečnostní dohled průmyslových sítí

Komplexní přehled o síti

Detekce hrozeb a rizik

Jednotné řešení pro monitorování IT a OT

Efektivní a flexibilní monitorování průmyslové sítě

www.greycortex.com

Jak poznat svou infrastrukturu do posledního detailu

Jedním z největších problémů, kterým firmy čelí, je zahlcení množstvím produktů a regulací v oblasti kybernetické bezpečnosti. Pro majitele a ředitele firem a výrobních podniků může být obtížné se v tomto množství orientovat a najít správný produkt, který by jim pomohl zajistit bezpečnost jejich sítí a dat. Zabezpečení firemních sítí i řídících systému v oblasti průmyslu a ochrana důležitých dat jsou stále složitější a mnohdy takřka nezvladatelné úkoly. Možná vyrábíte skleněné lahve, možná jste ředitelem elektrárny a na zajištění kybernetické bezpečnosti nezbývá čas, peníze, znalosti, nebo vše dohromady.

Soustředit se na to, co je pro vás opravdu důležité, je snazší, pokud víte, že jsou vaše nejcennější aktiva v bezpečí. S jejich identifikací i se zajištěním jejich kybernetické bezpečnosti pomůže pokročilý průmyslový dohledový systém GREYCORTEX Mendel. Přehledně zmapuje celou síť, včetně všech zařízení a konfigurací, neustále ji monitoruje a detekuje jakékoliv anomálie a potenciální hrozby, bez ohledu na to, zda se nachází uvnitř organizace nebo na ni působí z vnějšku.

Navíc Mendel umožňuje dohled jak nad průmyslovou sítí, tak IT infrastrukturou. Propojení zdánlivě neslučitelných oblastí poskytuje ucelený přehled o kybernetické bezpečnosti firmy a usnadňuje tak komunikaci mezi IT a OT týmy. Čas šetří snadné nasazení, kdy první výsledky uvidíte už první den, intuitivní ovládání a samozřejmě také možnost zajištění externího dohledu nad sítí.

Podrobná identifikace všech aktiv vám umožní lépe porozumět svému prostředí, určit priority a následně posoudit stávající zabezpečení a rizika.

Pokročilá detekce hrozeb je pak nedílnou součástí zajištění bezpečného provozu.

Posuzování kybernetické bezpečnosti.
Odborník na Unix, skriptování v shellu, perlu.
Unix (Linux, SCO, HP-UX, BSD, SUN Solaris), správa sítí Windows, sítě TCP IP.
Rozsáhlá znalost jazyka SQL (Ingres, MySQL, Postgres).
Udělený evropský patent č. EP3734376 na „Systém, počítačový systém a způsob řízení distribuovaných akčních členů“, který je budoucností automatizace.
Řídící systémy pro rafinérie, jaderné elektrárny, paro-plynové elektrárny (spalovací turbíny a parní turbíny).

Kybernetická bezpečnost – „Jsme docela v bezpečí“ – Opravdu!?

Erik Zapletal
FIG - IT Security, ŠKODA AUTO a.s.

V IT Škoda Auto se pohybuje již 15. rokem. Původně začínal na pozici operátora dohledového centra, poté se přes správu Windows serverů dostal až k IT bezpečnosti. Zde se již roku 2017 věnuje rozvoji IT a OT bezpečnosti ve výrobní oblasti. V osobním životě je nadšeným „elektrobastlířem“, kutilem a otcem 2 dětí.

IT bezpečnost ve výrobě

Jan ZDRHA
Oddělení bezpečnosti operačních technologií, NÚKIB

Polygon operačních technologií na NÚKIB

Partneři konference

ALEF NULA, a.s.

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

Společnost ALEF působí na trhu již od roku 1994 a za tu dobu si vybudovala pozici spolehlivého partnera, poskytujícího moderní a funkční IT řešení, která spolu s nejlepšími značkami v oboru, profesionálním přístupem a zkušenostmi tvoří tu nejlepší možnou kombinaci. Jako jedinečnou přednost společnosti lze zmínit komplexnost nabídky od analýzy, návrhu řešení, implementace, zaškolení, certifikace až po monitorování a profesionální služby – a to jak pro malé a střední podniky, tak i mezinárodní korporace.

Specializujeme se na technologie Cisco, NetApp, Splunk, Flowmon, Microsoft a AWS. 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.

PARTNER KONFERENCE

Barracuda Networks, Inc.

The White Building, 33 King's Road
Reading, Berkshire RG1 3AR

Jakub Jančík, Account Manager
+420 737 597 499
jjancik@barracuda.com

Matyáš Franěk, Account Manager
+420 774 090 791
mfranek@barracuda.com
www.barracuda.com

Barracuda Networks je jedním z předních světových výrobců řešení pro kybernetickou bezpečnost. Svět IT se mění rychle a hrozby se vyvíjejí ještě rychleji, je nutné mít partnera, který je schopen reagovat a předcházet problémům dříve, než se stanou. Barracuda se dnes zaměřuje jak na klasické on-premise řešení, tak i na segment cloudové bezpečnosti. Barracuda je tradičně silná v oblastech e-mailové bezpečnosti, firewallů, zálohování, webových aplikačních firewallů (WAF) a IoT zabezpečení. Neopomíjíme ani důležitá témata, jako je například vzdělávání uživatelů a jejich testování phishingovými útoky.

PARTNER KONFERENCE

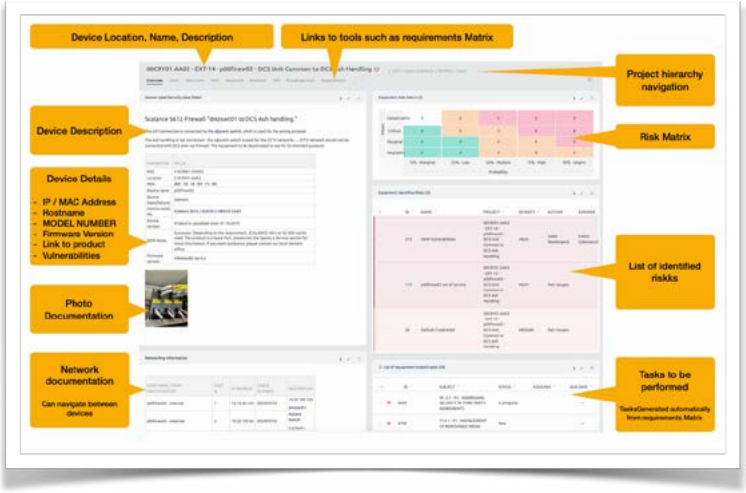
BDO Group s.r.o.

V parku 2316/12
148 00 Praha
+420 241 046 111
bdo@bdo.cz
www.bdo.cz

BDO Digital je součástí poradenské společnosti BDO. Nabízí ucelený soubor vysoce kvalitních služeb v oblasti strategického technologického a obchodního poradenství zaměřeného na střední trh. Disponujeme obchodním přehledem a rozsahem služeb potřebných k tomu, abychom vaše podnikání posunuli na vyšší úroveň, včetně vývoje digitální strategie, kybernetické bezpečnosti, modernizace technologií, řízení rizik, outsourcingu.

Náš tým spolupracující napříč obory pomáhá řešit okamžité digitální potřeby a odhalit nové příležitosti k získání konkurenční výhody. Služby poskytujeme v těchto oblastech:

Device Cybersecurity and Maintenance Datasheet



BOHEMIA MARKET
www.bm.company

BM Digital, February 2023, Rev. 1

Kybernetická bezpečnost - „Jsme docela v bezpečí“ - Opravdu!?

Kolikrát jste toto již slyšeli aneb „Compliance is not security“ čili hezky česky - věříte tomu, že ta či ona agentura zkontrolovala vámi předloženou dokumentaci, papíry, vyplnila formuláře a prohlásila, že jste z hlediska kybernetiky v bezpečí. Ano, splnili jste všechny normy, možná aktualizovali systémy. V angličtině je pro toto velmi pěkný výraz, který se nazývá „False Sense of Security“.

Takže si rozeberme, co je to „compliance“ – zde jsou jasně daná pravidla hry a jsou známá před započetím jakéhokoliv auditu. Existuje velmi dobře zdokumentovaný „formulář“ principů a požadavků. Organizace ví již dlouho předem na co se má připravit, jaké požadavky na ní jsou/budou kladeny a kdo test provede – neboli předem se ví kdo, co, jak a kde. Lze se tedy velmi dobře připravit.

Avšak realita je zcela jiná. Definujme si „Security“ – zde si nemůžeme být jistí předem kdy, kdo, jak a kde. Útočník může, a samozřejmě zaútočí kdykoliv, využije každé skulinky a s jistotou najde mnoho kreativní cest, jak se do systému dostat či ho poškodit. Toto je bezpečnost.

Je nutné se naučit a velmi dobře si zapamatovat, že „IT Compliance“ nezaručuje žádnou bezpečnost. Bohužel většina řídících pracovníků toto zatím nepochopila.

A nyní se podívejme na to, jak může pomoci naše společnost Bohemia Market.

Na základě více než 20 let zkušeností si troufáme prohlásit, že neexistuje žádná možnost, jak zabezpečit jakýkoliv systém na 100 procent. Tudíž jsme problém zanalyzovali a vytvořili „Control Systems Continuity Solutions“ neboli zajištění provozní kontinuity řídících systémů. Jedná se o program sestavený selským rozumem, který se skládá ze dvou kroků. Krok první je vytvoření seznamu zařízení, a krokem druhým je vytvoření plánů a procedur, jak daná zařízení zálohovat, obnovovat, testovat a zjištění a případně zajištění jejich dostupnosti. Výsledkem je podrobný plán pro celý řídící systém v přehledném webovém nástroji společnosti Bohemia Market.

Teprve po vytvoření tohoto plánu má smysl zabývat se „compliance“ formuláři.

KYBERNETICKÁ BEZPEČNOST; IT COMPLIANCE, REGULACE; DIGITALIZACE; TECHNOLOGICKÉ PORADENSTVÍ

BDO v České republice poskytuje služby v oblastech auditu, účetnictví, daní, práva, informačních technologií, digitalizace, finančního a transakčního poradenství či znalectví. Služby poskytuje malým a středně velkým českým firmám, rozsáhlým koncernům i pobočkám mezinárodních korporací. Je největší ryze česky vlastněnou poradenskou skupinou společností v ČR se zázemím rozsáhlé mezinárodní sítě.

PARTNER KONFERENCE

Bohemia Market CZ, s.r.o.

Holandská 878/2
639 00 Brno
+420 565 533 729
sales@bohemiamarket.com
bm.company

Firma Bohemia Market poskytuje inženýrské služby, prodlužování životnosti a údržbu řídících a DCS systémů zákazníkům po celém světě. Od aktualizace a modernizace HMI systémů, až po návrh a dodání sofistikovaných dálkových monitorovacích center. Jsme schopni pokrýt celé spektrum, abychom vám zajistili konkurenční výhodu na trhu. Za více než 20 let naší působnosti jsme si získali důvěru klíčových hráčů 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.

Jelikož je téměř nemožné ochránit starší řídící systémy z hlediska cyber security tak jsme pro naše zákazníky vyvinuli unikátní systém na vytvoření plánu na obnovu řídícího systému v případě jakýchkoliv problémů. Díky tomuto mohou naši zákazníci obnovit své řídící systémy v rámci hodin či dnů a vyhnout se vydírání či ztrátám ve výrobě či produkci.

PARTNER KONFERENCE

COLSYS – AUTOMATIK, a.s.

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

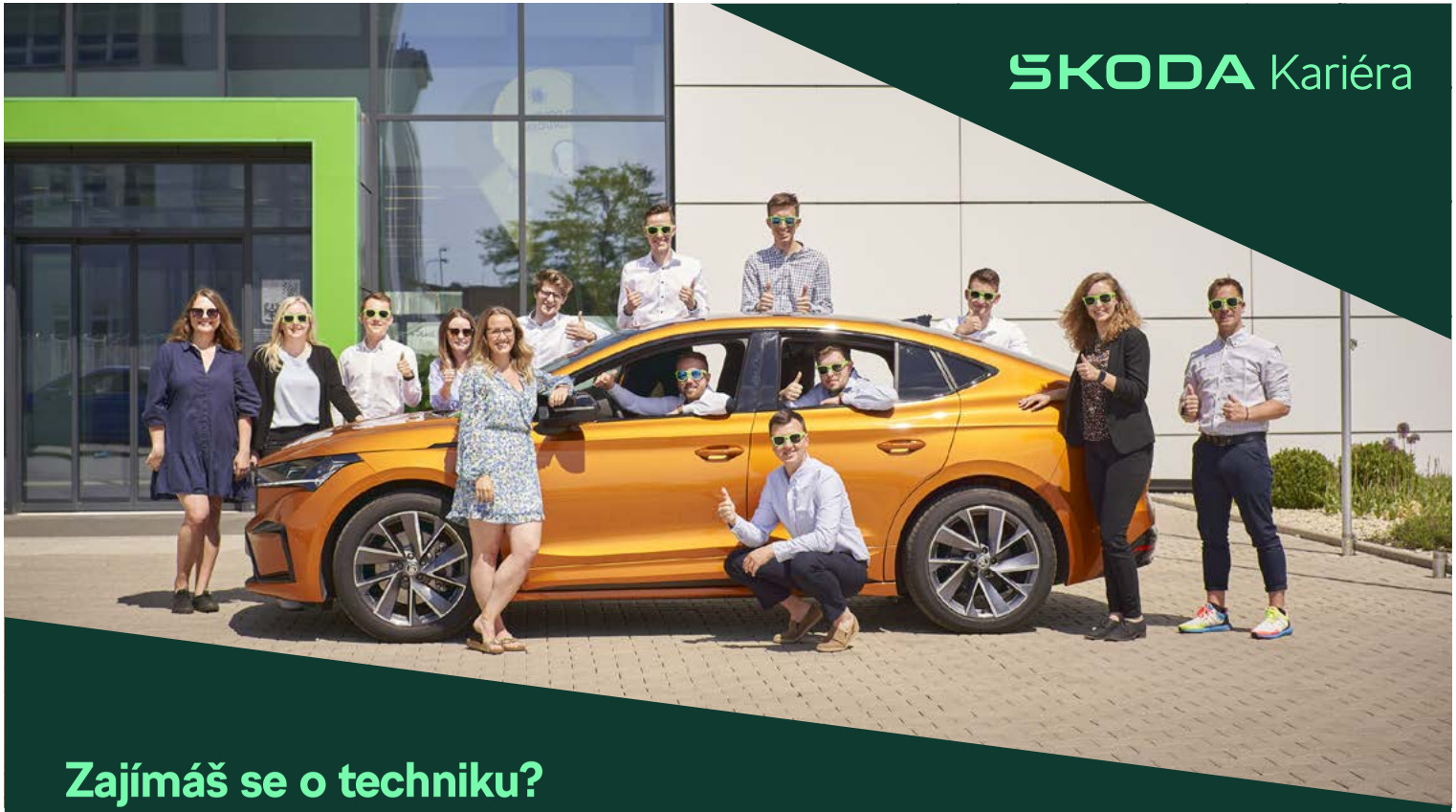
Jsme od založení v roce 1998 ryze česká inženýrská společnost, která poskytuje služby a dodávky v oblasti kritické komunikační infrastruktury (KKI) v průmyslu, dále v oblasti systémů pro řízení a dohled nad energetickými celky a konečně v oblasti automatizovaných systémů pro řízení technologií. V oblasti 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

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 mo-



ŠKODA Kariéra

Zajímáš se o techniku?

Staň se součástí Škoda Auto.

Škoda Auto Kariéra | @WeAreSKODA | Škoda Auto a.s. | Škoda Auto - Career

derní 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

Progress

Název produktu: Progress Flowmon
Škrobárenská 511/5
617 00 Brno
www.flowmon.com

Flowmon je součástí produktového portfólia Progress. Progress je předním poskytovatelem technologií pro vývoj aplikací a digital experience.

PARTNER KONFERENCE

ŠKODA AUTO a.s.

tř. Václava Klementa 869
Mladá Boleslav II
293 01 Mladá Boleslav
Infolinka +420 800 600 000
infoline@skoda-auto.cz
www.skoda-auto.cz

Jedna z nejdéle kontinuálně vyrábějících automobilek na světě, jejichž historie sahá až do roku 1895. Se strategií Next Level – Škoda Strategy 2030 a novou podobou značky má společnost v tomto desetiletí jasný plán; z tradičního výrobce automobilů se proměňuje na více elektrickou, mezinárodní a digitální automobilku.

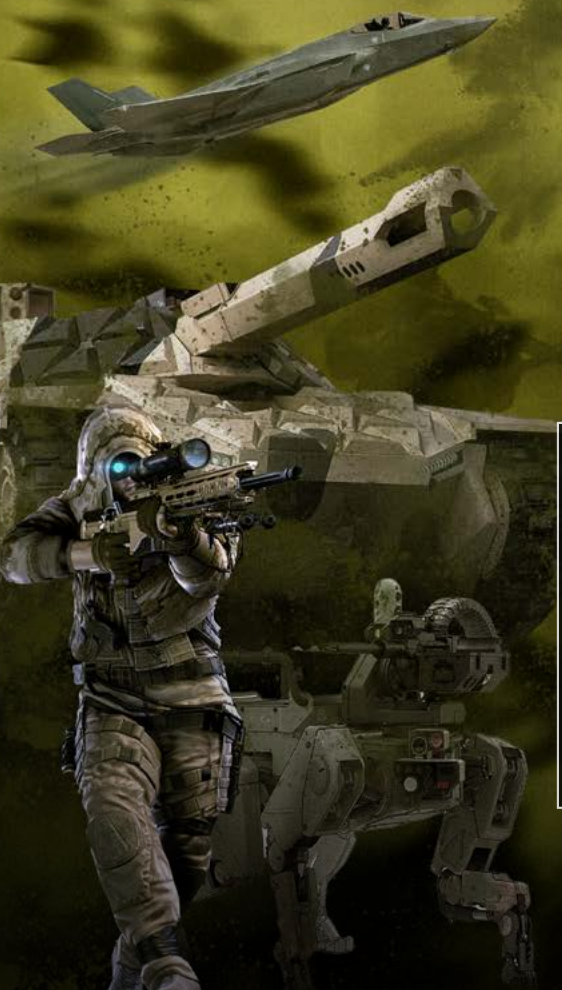
PARTNER KONFERENCE

Mediální partneři

FUTURE FORCES FORUM

Future Forces®
INTERNATIONAL EXHIBITION
www.natoexhibition.org

OBRANA A BEZPEČNOST



- VÝSTAVA
- ODBORNÉ PANELY
- NETWORKING

PŘÍŠTÍ ROČNÍK
16.–18. 10.
2024
PVA EXPO PRAHA

www.fff.global