

SCADA CONFERENCE

ZABEZPEČENIE PREVÁDZKY KRITICKÝCH SYSTÉMOV V SCADA/ICS

1. OKTÓBER 2019 SHERATON BRATISLAVA HOTEL

PROGRAM KONFERENCIE

- 8:30 - 9:00 **Registrácia**
- 9:00 - 9:05 **Otvorenie konferencie**
Marek Král, Generálny riaditeľ, SecTec
- ODBORNÁ ČASŤ**
- 9:05 - 9:30 **Legislatíva k Z. 69/2018 Z.z. a dopad na riešenie kybernetických bezpečnostných incidentov v záujmových sektoroch /podsektoroch a úloha CERT-SK v IT/OT**
Rastislav Janota, Národný Bezpečnostný Úrad
- 9:30 - 10:00 **Expect Unexpected: ICS Monitoring of the Future**
Špeciálny hosť zo zahraničia: Tomer Ben-Shalom, Senior Business Director, EMEA, Claroty
- 10:00 - 10:30 **Stories from the cyber trenches: Constant cyber attacks against critical Infrastructure in Ukraine**
Špeciálny hosť zo zahraničia Andrii Slobodyanyk, Head of Cybersecurity, BDO, Ukraine
- PRESTÁVKA S OBČERSTVENÍM**
- 11:00 - 11:30 **Osvedčené postupy pri budovaní a prevádzkovaní CSIRT/ SOC**
Špeciálny zahraničný hosť Juraj Příbyl, Head of Security Operation Center
- 11:30 - 12:00 **Auditovanie a modelovanie hrozieb v SCADA/ICS**
Martin Fábry, Critical Infrastructure Cybersecurity Consultant
- 12:00 - 12:25 **Oplatí sa Vám mať vo firme vlastný SOC?**
Ján Andraško, SOC Operations Manager, Binary Confidence s.r.o.
- 12:25 - 13:00 **PANELOVÁ DISKUSIA so spíkrami odbornej časti na tému: Aplikovateľnosť bezpečnostných opatrení a prístupov pre interoperabilný IT/OT svet**
Moderátor: Roman Čupka, Country Manager & Principal Consultant, Flowmon Networks
- 13:00 - 14:00 **OBED**

Organizátori:



Partneri:



SCADA CONFERENCE

ZABEZPEČENIE PREVÁDZKY KRITICKÝCH SYSTÉMOV V SCADA/ICS

1. OKTÓBER 2019 SHERATON BRATISLAVA HOTEL

PROGRAM KONFERENCIE

14:00 - 16:00 **TECHNOLÓGICKÁ ČASŤ**

venovaná predstaveniu integračných platforiem pre monitoring, bezpečnosť a incident manažment v prostredí SCADA/ICS

a) Efektívna správa a zabezpečenie technologických sietí, Jindřich Šavel, Obchodný riaditeľ Novicom

Anotácia: Prezentácia predstaví riešenie AddNet a jeho možnosti sieťového monitoringu, integrovanej IP správy a riadení prístupu do siete zariadení prevádzkovaných v technologických sieťach – DDI a NAC v hybridných IT/OT sieťach.

b) Zabezpečenie prevádzky IT/OT interoperabilného prostredia, Roman Čupka, Country Manager & Principal Consultant, Flowmon Networks

Anotácia: S globálnym nárastom aplikovateľnosti IoT dochádza k čoraz užšej interoperabilite medzi „klasickým“ IT a „priemyselným“ OT prostredím, čoho dôkazom je podľa jedného z renomovaných ICS CERT 30% medziročný nárast zdrojov bezpečnostných hrozieb práve z internetu. Flowmon monitoring a detailná viditeľnosť do sieťovej komunikácie a používaných aplikácií cez celé toto prostredie umožňuje predchádzať rôznym výkonnostným a prevádzkovo-bezpečnostným udalostiam.

c) Monitorovanie a bezpečnosť priemyselných riadiacich systémov, Branislav Kollar, Business Development Manager, SecTec, Martin Fábry, Critical Infrastructure Cybersecurity Consultant

Anotácia: Po prvý krát sa na Slovensku takto verejne predstaví typizované riešenie Claroty špeciálne dimenzované na monitoring a ochranu OT prostredia. 100% viditeľnosť do špecifických SCADA/ICS protokolov a sieťovej komunikácie umožňuje predchádzať funkčným problémom a efektívne rieši rôzne kybernetické bezpečnostné incidenty.

d) What hackers want? Andrej Aleksiev, Country Sales Manager, Check Point Software

Anotácia: 40% priemyselných lokalít má aspoň jedno priame spojenie s verejným internetom, 53% webových stránok má zastaralé systémy Windows, napríklad Windows XP, 69% stránok má heslá prostého textu prechádzajúce ich sieťami ICS, 57% webových stránok nemá antivírusovú ochranu, ktorá automaticky aktualizuje podpisy, 16% webov má aspoň jeden bezdrôtový access point, 84% priemyselných lokalít má najmenej jedno remote access zariadenie.

e) Forcepoint Data Guard – riadenie SCADA protokolov v oddelených sieťach a umožnenie ich bezpečnej komunikácie, Miroslav Bajgar, Sales Engineer Forcepoint

Anotácia: Management a kontrola SCADA protokolov musí rozumieť aj ich obsahu a byť schopný prepustiť iba očakávaný rozsah ich hodnôt.

f) „Incident Response Automation“ ako súčasť SOAR

Anotácia: „Start Up okienko“ – predstavíme vám sľubne sa rozvíjajúcu slovenskú technologickú platformu Synapsa pre automatizáciu a zrýchlenie procesov kombinujúcu odhaľovanie a notifikovanie kyber-bezpečnostných incidentov s ich mitigáciou v reálnom čase, ktorá by výrazne ušetrila FTE v organizáciách.