IT/OT bezpečnosť v priemysle

Michal Sekula

Digitalizácia prepája rôzne svety – IT a OT … a IoT

Kybernetický útok

Stuxnet

rok 2010

prvý známy vírus, ktorý napadol SCADA

Kybernetický útok

23. december 2015

230 000 ľudí bez elektriny až 6 hodín

Kybernetický útok / Ransomware

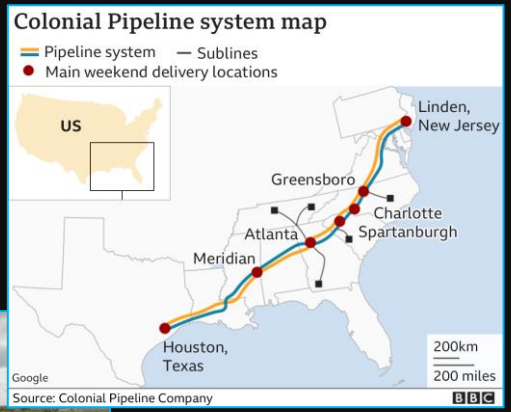
júl 2019

v nemocnici zomrelo dieťa

Kybernetický útok / Ransomware

máj 2021

výkupné 5 000 000 USD



Kybernetický útok / Ransomware

december 2019

hackeri v Česku ochromili bane, položili sieť OKD

Kybernetický útok – je toho stále viac a viac

13.03.2020 **Fakultní nemocnice v Brně**, kde se léčí lidé s koronavirem, čelí kybernetickému útoku

31.03.2020 **Psychiatrická nemocnice Kosmonosy** je bez IT systémů

07.04.2020 Další kybernetický útok v Česku. Hackeři zasáhli Povodí Vltavy

17.04.2020 Pražské letiště odvrátilo několik kybernetických útoků

17.04.2020 **FN Ostrava** se v noci stala terčem kybernetického útoku

18.04.2020 **Olomouckou fakultku** napadli hackeři

18.04.2020 Nemocnice kybernetické útoky odrážejí. Poslední atak cílil na tu **karlovarskou**

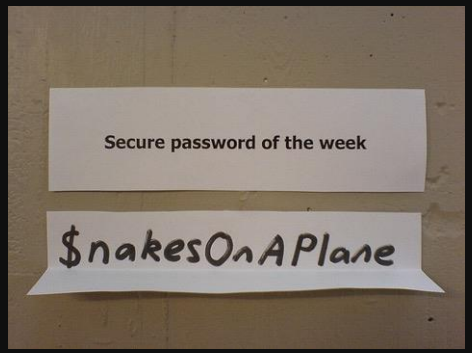
18.08.2020 Loňský kybernetický útok na **Nemocnici Rudolfa a Stefanie Benešov** způsobil škodu přes 59 milionů korun.

Prečo sa to deje?

Za všetkým hľadaj človeka

Chyba

Nedbanlivosť
Neznalosť
Nepozornosť
Únava



Úmysel

Pomsta
Vydieranie
Politické ciele
iné motivy

Atos

Rôzne ciele a potreby OT a IT

Operational Technology

Vyrába veci

Riadi veci

Monitoruje veci

Information Technology

Pracuje s dátami

Chráni dáta

Skladuje dáta

Atos

Rôzne ciele a potreby OT a IT

Operational Technology	Information Technology
Pravidelné, malé objemy dát Operácie v reálnom čase	Nepravidelné, veľké objemy dát Oneskorenie je akceptovateľné
Výpadky nie sú akceptovateľné Redundancia je vyžadovaná	Reštarty systémov sú akceptovateľné Obnoviteľné backupy sú akceptovateľné
Bezpečnosť ľudí Bezpečnosť technológií	Integrita dát Bezpečnosť dát
Špecifický hardvér Bezpečnosť nie je (nebola) prvoradá Špecifické komunikačné protokoly	Flexibilný hardvér Jednoduché bezpečnostné aktualizácie Štandardné protokoly – TCP/IP
Závislosť na špecifickom vendorovi Životnosť komponentov 10-15 rokov a viac Aktualizácie starostlivo plánované a testované	Zvyčajne viacerí štandardní vendori Životnosť komponentov 3-5 rokov Pravidelné aktualizácie a patche
1. Dostupnosť, 2. Integrita, 3. Dôvernosť	**1. Dôvernosť**, 2. Integrita, 3. Dostupnosť

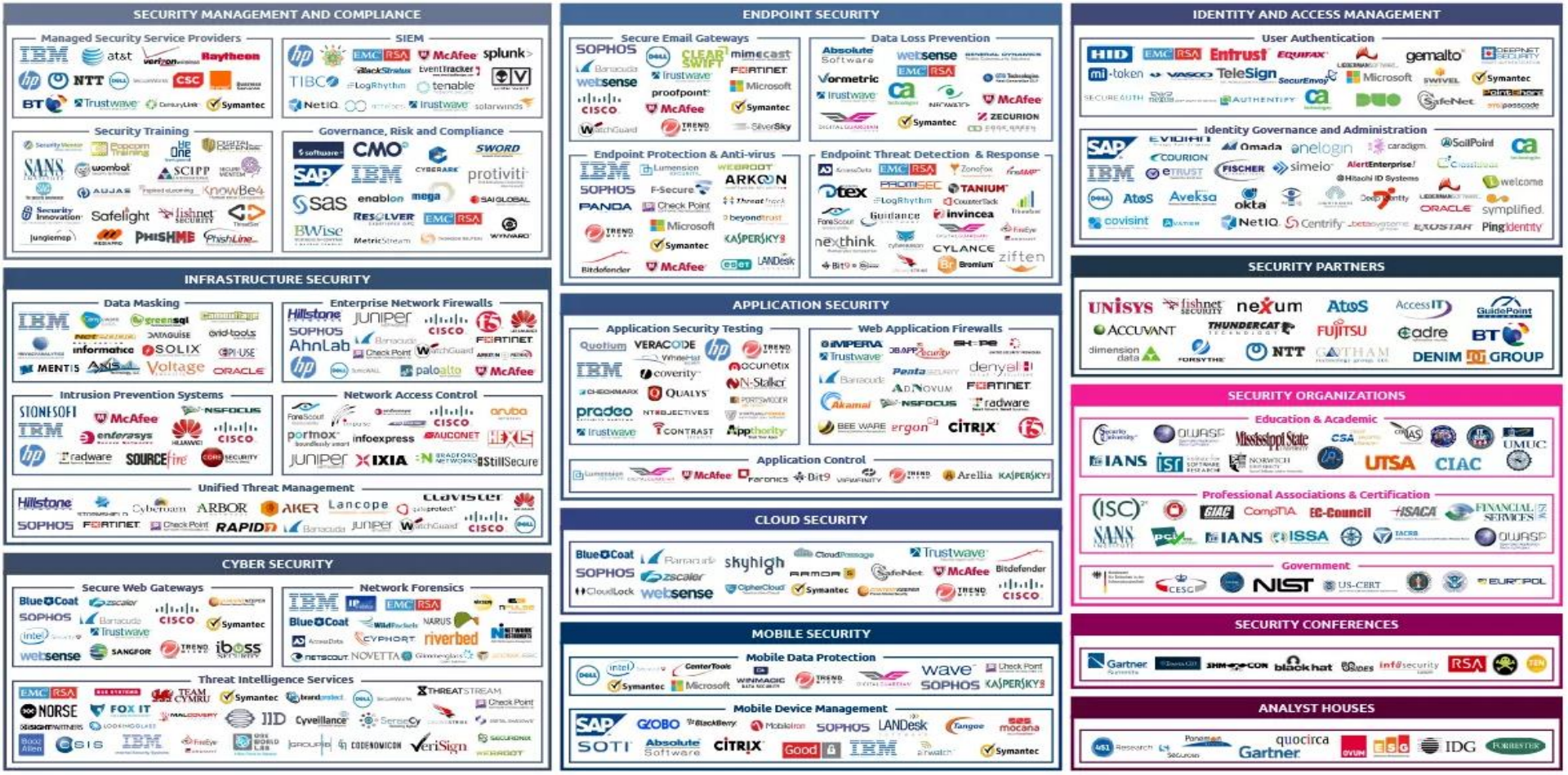
Atos

Ako sa chrániť?

Chrániť viem iba to, čo vidím, o čom viem.

Atos

Vybraní vendori riešení IT/OT Security



Ako dokáže Atos pomôcť

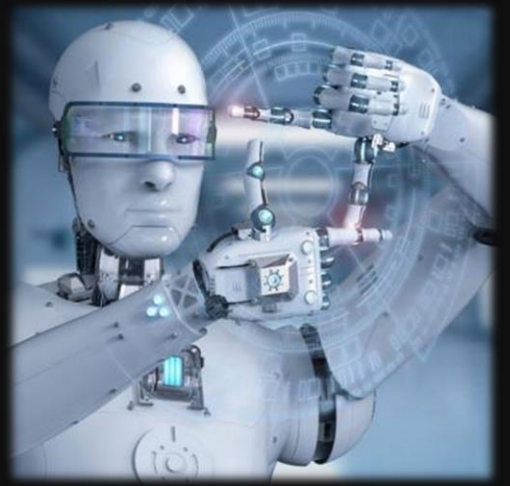
IT, OT a IoT

Základné komponenty

- Vizibilita aktív
- Mapa sítě
- Detekcia OT pripojených do internetu
- Identifikácia problémov v konfigurácii
- Detekcia hrozieb a anomálií
- Automatizované zprávy o rizikách

Volitelné položky

- Informácie o hrozbách
- Vyhodnocovanie zraniteľností
- Flexibilný reporting a dashboardy
- Segmentácia sietí



Štandardné servisné požadavky

Štandardný reporting

Nastavenie služeb

Integrácia

SIEM | SOC | ITSM

Atos

Čo tým získate?

Viditeľnosť a situačný prehľad v reálnom čase o všetkých pripojených zariadeniach (IT, IoT, OT, virtuálne, cloud)

Škálovateľnú platformu a jednotný rámec politík na minimalizáciu rizika v prepojených sieťach

Digitalizované akcie a pracovné postupy s cieľom automatizovať kontrolu a reakciu a urýchliť nápravu

Atos

Chcete vedieť viac?

michal.sekula@atos.net

+421 905 401170