BDS / HEALTHCARE

On-line seminář

Kybernetická bezpečnost ve zdravotnictví:

Odhalení skrytých slabin vaší infrastruktury

Jan Váša
Cyber Security Sales
Atos

Petr Němec
Cyber Security Consultant
Atos

Patricie Baroňová
Business Development Manager
Flowmon Networks

Dejan Laketić
Sr. Sales Engineer
Gigamon

3. prosince 2020

Agenda aneb
Co nás dnes čeká a nemine

1 Zdravotnictví v ČR z pohledu kybernetické bezpečnosti
Jan Váša | Cyber Security Sales | Atos BDS CZ & SK

2 SIEM bezpečnostní nástroje pro sběr a vyhodnocení dat
Petr Němec | Cyber Security Consultant | Atos BDS

3 Monitorování provozu a detekce hrozeb
Patricie Baroňová | Business Development Manager | Flowmon Networks

4 Sběr dat a agregace pro bezpečnostní a monitorovací nástroje
Dejan Laketić | Sr. Sr. Sales Engineer | Gigamon EMEA Central

Zdravotnictví v ČR z pohledu kybernetické bezpečnosti

Jan Váša | Atos

Atos IT Solutions and services, s.r.o.

Atos ve světě

Atos je lídrem v digitálních službách, zaměstnávající 120000+ zaměstnanců v 72 zemích a dosahuje ročního výnosu ve výši 12 miliard €

Atos Česká republika

~300 zaměstnanců
Cyber Security tým součástí divize BDS
Kvalifikace a kompetence (ISO27001, NBÚ-Tajné,…)
Provozovatel KII, VIS pro povinné subjekty dle 181/2014

Roční výnosy CZ (2019)

~ 50 mio. €

Kybernetická bezpečnost

- Specifika digitalizace našich životů přináší nejen výhody, ale i vážné problémy
- Počet bezpečnostních incidentů a kybernetických útoků roste
- Známé útoky
  - Nemocnice Benešov, FN Brno, PN Kosmonosy, FN Ostrava, …
- Proč se to děje?
  - Podcenění rizik ze strany managementu
    - Nepochopení závažnosti problematiky
  - Přenesení zodpovědnosti na IT oddělení
    - Sdílení stejných zdrojů k zajištění provozu i bezpečnosti

Problematika kybernetické bezpečnosti

- Vyřeší nákup bezpečnostních prvků situaci?

  Ano, ale…
  - Je třeba pokrýt celou řadu oblastí
    - Detekce, Monitoring, Vyhodnocování, Řízení, …
  - Dokážete zajistit kvalifikovaný personal?
    - Schopný bezpečnostní technologie reálně používat
  - Budete schopni zajistit bezpečnost nepřetržitě?
    - Je třeba fungovat 365/7/24
  - Vyplatí se vám to?

- Z ekonomického pohledu je vybudování týmu schopného se nepřetržitě postavit hackerům a odrazit kybernetický útok pro většinu organizací nereálné.

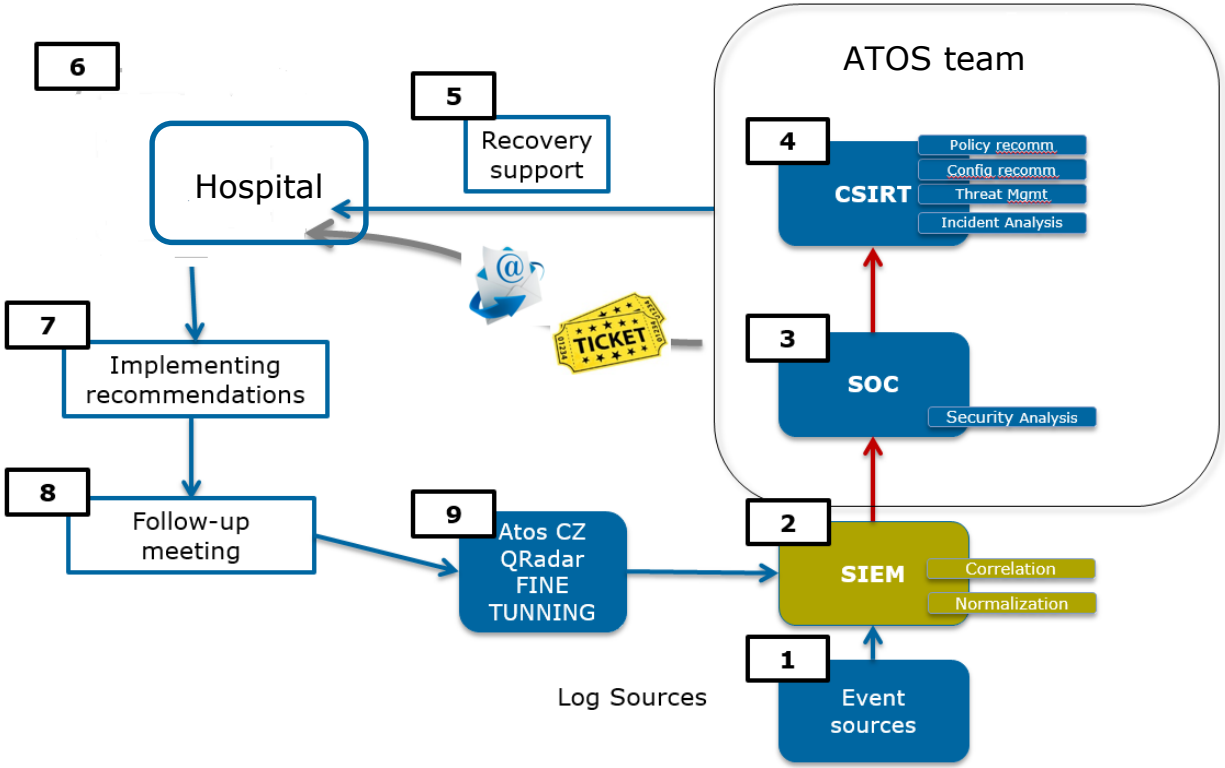
Řešení kybernetické bezpečnosti

- Sdílení specializovaných zdrojů
  - Security Operation Center - SOC

- Jaký je ten pravý SOC?
  - Dostupnost 24x7
  - Plné převzetí zodpovědnosti za řešení incidentů
  - Schopnnost kdykoliv reagovat na kybernetický útok a provádět obranné reakce nezávisle, bez součinnosti s personálem zákazníka

- Zajištění aktivní reakce SOC na incidenty lze pouze docílit sdílením nástrojů umožňujících vhled do prostředí zákazníka a řízení jeho infrastruktury

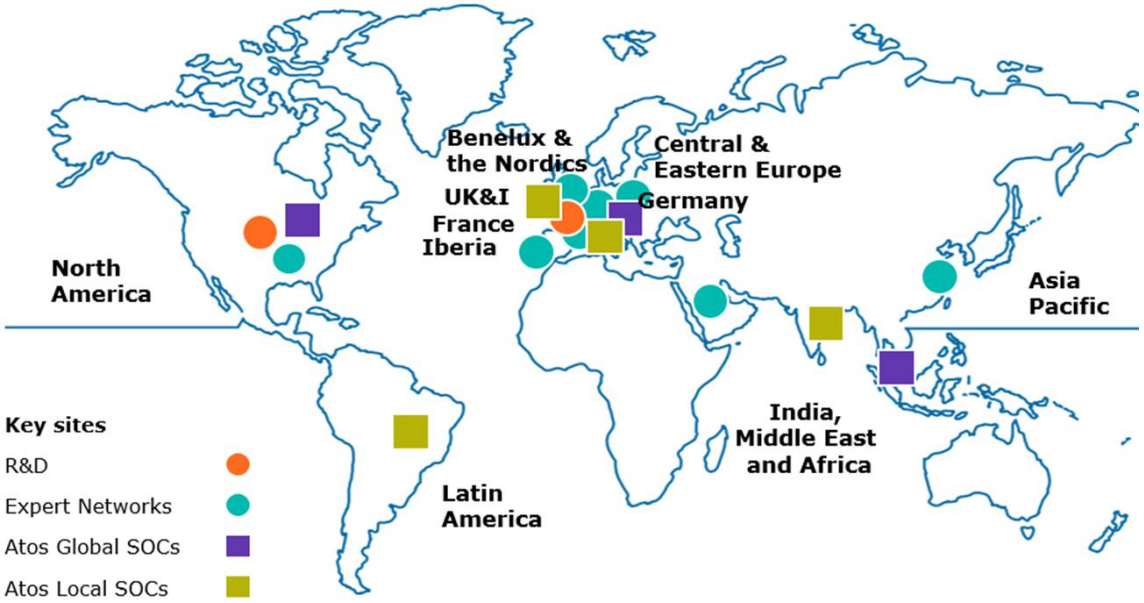
Příklad řešení SOC od Atos



Kybernetická bezpečnost od Atosu

HEALTHCARE

- Globální působnost včetně týmů specializovaných na bezpečnost ve zdravotnictví
- Sdílení informací a zkušeností i lidských zdrojů
- 15 SOC po celém světě
- Více než 6000 zkušených a certifikovaných bezpečnostních expertů



Zdravotnictví v ČR
z pohledu kybernetické bezpečnosti

- Zpráva Evropského policejního úřadu popisuje, jak kriminálníci vydělávají na koronavirové krizi. Data sbírá ze všech zemí EU. Uvádí ale **jediný příklad kyberútoků na klíčovou zdravotnickou infrastrukturu** a tím jsou **české nemocnice**. Série kyberútoků z března a dubna byla výjimečná v mnoha ohledech. Načasování na začátek nouzového stavu, zacílení na zdravotnická zařízení i důsledek v podobě paralyzované klíčové brněnské nemocnice nemají v evropském kontextu obdoby.

Kybernetická bezpečnost zdravotnictví v ČR – shrnutí faktů

- Sektor zdravotnictví je dlouhodobě podfinancovaný
- Personální kapacity jsou poddimenzované
- Na trhu práce je nedostatek kvalifikovaných odborníků s praxí
- Platy v IT oboru v komerční sféře jsou nadprůměrné a dále stoupají
- Kybernetická bezpečnost není vedením nemocnic vnímána jako priorita
- Počet kybernetických útoků narůstá a reálná hrozba napadení den ze dne roste

Kybernetická bezpečnost zdravotnictví v ČR – jak pokračovat?

- Postupné dobudování infrastruktury tak, aby byla připravena pro napojení na SOC
  - Firewally, Antiviry/Antispamy apod.
  - IdM, Monitoring Flow, DDI/NAC, Log management, SIEM, PAM
- Atos má všechny předpoklady být důvěryhodným partnerem při řešení kybernetické bezpečnosti ve vaší organizaci
- Vize dedikovaného SOCu pro zdravotnictví – hSOC
- Kde na to vzít?
  - Nové programové období 2021 – iROP

Děkuji za pozornost

Více viz:
atos.net/en/industries/healthcare/cybersecurity-in-healthcare

Atos

SIEM bezpečnostní nástroje pro sběr a vyhodnocení dat

Petr Němec | Atos

2

Monitorování provozu a detekce hrozeb

Patricie Baroňová | Flowmon

3

Sběr dat a agregace pro bezpečnostní a monitorovací nástroje

Dejan Laketić | Gigamon

Naše odpovědi na Vaše dotazy

Q1:
Dobrý den. Bude k dispozici záznam webináře, případně prezentace?
Děkuji.

Q2:
Mám dva dotazy:
1. Jaký je rozdíl když sbírám data ze sondy a z prvků?
2. Mám k dispozici i šablony reportů?
Děkuji.

Q3:
Rád bych se zeptal:
1. "Je možné pomoci Gigamonu sledovat komunikaci v rámci Vmware prostředí?"
2. "Jakým způsobem mohu monitorovat distribuované lokality"

Q4:
Dekuji za prezentaci, jelikoz jsme certifikovany IBM Qradar administrator/specialist, je toto pro mne nepodstatne. Preji hodne uspechu, Qradar umi byt i narocny, ale rozhodne souhlasim ze je to jedno z nejlepsich reseni na trhu.

HEALTHCARE

Děkujeme za Vaši účast

Pro více informací nás neváhejte kontaktovat:
M: +420 722 446 644
E: cyber.security@atos.net

Atos

Česko je pro hackery atraktivní cíl, varoval NÚKIB

Ondřej Rojčík, vedoucí oddělení strategických informací a analýz

Národní úřad pro kybernetickou a informační bezpečnost, 21. 10. 2019

*„…**řada lidí podceňuje atraktivitu Česka jako cíle pro kybernetický útok**. Upozornil, že zemi je možné chápat jako bránu do Evropské unie i do Severoatlantické aliance.*

*Kromě toho mohou mít nejčastější pachatelé kybernetických útoků i své ekonomické nebo politické zájmy v Česku, kterých by chtěli pomocí útoků dosáhnout. Dále také upozornil, že **Česko má velmi vyspělý průmysl, vědu a výzkum, což může rovněž lákat pachatele k nelegálnímu získávání informací**.*

Náklady na útoky zpravidla bývají relativně nízké, pachatele je obtížné jednoznačně identifikovat a prakticky nemožné účinně potrestat.