



# **Cacio seminář „Kybernetická bezpečnost 20!21“**

## **Význam implementace SIEM v prostředí IT systémů nemocnic**

Leoš Stránský  
Team Leader

11/03  
2021





**Tlak na zabezpečení systémů nemocnic roste.**

**AUTOCONT pomocí systému SIEM posiluje jejich kybernetickou bezpečnost.  
Jsou nemocnice v něčem jiné? Jaké služby čerpají a jaký nástroj využíváme?**

## NEMOCNICÍM NENÍ CO ZÁVIDĚT ...

<p>Dopadá na ně legislativa. <b>Provozovatelé základní služby</b> Vyhl. č. 437/2017 400 lůžek+ nebo 40 JIP+</p> <p><b>ZoKB</b> Není to jen o papíru, je nutné pořídit technologie</p>	<p>Bez nemocnic se neobejdeme. Jejich služby potřebujeme bezodkladně. Hodně toho tady o nás ví (citlivé osobní údaje).</p>	<p>Nedostatek financí na investice. IT je stále bráno jako příslušenství ke zdravotní technice. Bohužel se už ale stihly do značné míry digitálně transformovat.</p>	<p>Je zde rozsáhlé protředí IoT s dopadem na pacienta. Personál není dostatečně vyškolený a je pod zátěží.</p>
---	--	--	--

## CO SI O TOM MYSLÍTE? – BAVÍME SE O 80-TI SUBJEKTECH (PSZ, PŘÍMO ŘÍZENÉ SLOŽKY A REGIONÁLNÍ NEM)

PSZ a organizace řízené MZ ČR potřebují 4,3 Mld. Kč do roku 2023 na KB.	Polovina subjektů nemá zaveden systém řízení bezpečnosti informací.	Třetina své IT nemonitoruje. Jednotky subjektů jedou bez VLAN.	Jen jednotky si ročně nechají udělat testy zranitelnosti nebo penetrační test.
Polovina subjektů nemá nemocniční přístroje v oddělené VLAN.	Pouze pětina nemocnic má SIEM	Jen třetina subjektů má SW na šifrování dat na USB.	Třetina subjektů nemá nástroj k centrálnímu řízení koncového bodu.

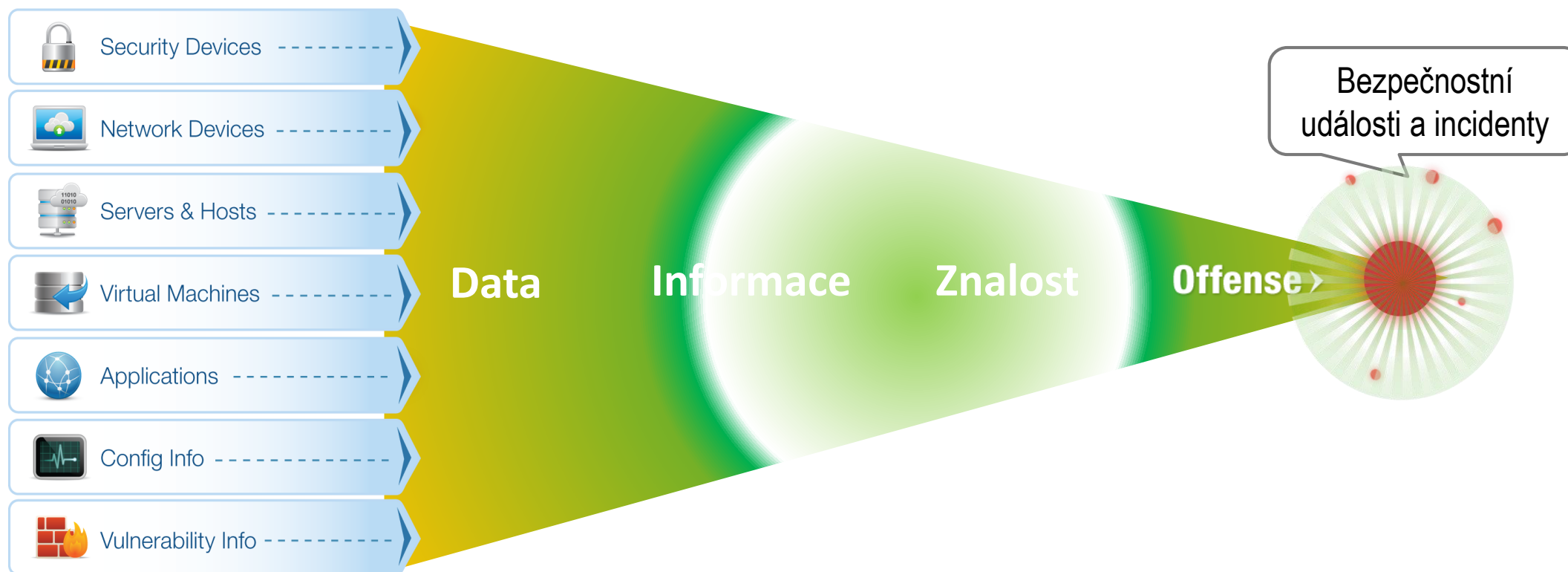
ZAKAZ MALOVANI  
ČERTA NA ZED'



Abychom jen nemalovali čerta na zed'

## CENTRÁLNÍ NÁSTROJ BEZPEČNOSTI – TO JE SIEM. JAK FUNGUJE SIEM?

- Produkt rozhodujícím způsobem posiluje kybernetickou bezpečnost, tím že v reálném čase přijímá, normalizuje, ukládá a koreluje logy, síťové toky a zranitelnosti generované zařízeními a aplikacemi v síti. Buduje jejich archivní úložiště a reputační databáze.



Extrémní množství dat



Pokročilá technologie



Vysoká úroveň viditelnosti a přesnosti detekce

**AUTOCONT**



**Jak tedy zavést SIEM a nemít jen další „zbytečnou“ technologii?**

## JAK TEDY ZAVÉST SIEM V NEMOCNICÍCH A NEDODAT JIM JEN DALŠÍ „ZBYTEČNOU“ TECHNOLOGII?

Mít rámcový rozpočet a personální zdroje.	Disponovat aktuálním a podrobným schématem sítě.	Zajistit kvalitní logování aplikací. ZoKB požadavky na logy předepisuje.	Pochopit, že ke kvalitnímu SIEM se propracujete jedině projektově.
Neroubovat SIEM na Log Managment a nebo na Monitoring.	Flow sondy nebo skenery zranitelností jsou vítány.	SIEM musí projít testy. Výkonové a funkční (use cases).	Servis a SOC to jsou spojené nádoby.





**Jsou teda nemocnice v něčem jiné?**

## **NEMOCNICE POCHOPITELNĚ ZASE TAK ODLIŠNÉ NEJSOU, ALE NĚCO PŘECE?**

**Jejich centrální systém je (skoro) vždy aplikace psaná na míru tuzemskou firmou.**

**Najdou se zde „historické“ systémy.**

**Jsou skutečně vystaveny kyberútokům a mediálně exponované.**

**SIEM je pro ně velký skok v kybernetické bezpečnosti vpřed.**

**Služby SOC a servisu se prolínají. Mají zkušenosti s fungováním 7x24.**



**Jakou technologii SIEM nasazujeme?**

**Omezte  
firemní  
bezpečnostní  
hrozby**

**IBM Security  
QRadar SIEM**

**IBM**

**AUTOCONT**

[Dozvědět se více >](#)

## AUTOCONT A QRADAR – ŘEŠENÍ NEJEN PRO NEMOCNICE

K dispozici je dedikovaný realizační a dohledový tým na QRadar SIEM. Obsazené všechny role:

- Specialisté pro návrh a předprodejní podporu
- Projektový vedoucí
- Specialisté pro nasazení
- Vývojáři aplikací
- Specialisté SOC ve vlastním dohledovém centru



**2021**  
kompetence IBM

**IBM PartnerWorld**  
**Expert: Security Operations and Response**

Uznání splnění požadavků, jež jsou nezbytné k prokázání odbornosti v oblasti poskytování hodnoty zákazníkům

*AUTOCONT a.s.*

*J. G. Teltsch Jr.*

John G. Teltsch Jr.  
Generální manažer  
Globální obchodní partneři

**IBM**  
Gold Business Partner

# SESTAVENÍ HLÁŠENÍ KYBERNETICKÉHO INCIDENTU PŘÍMO V QRADAR

IBM QRadar Security Intelligence

admin Help Messages 0 IBM

Dashboard Offenses Log Activity Network Ac... Assets Reports Risks Vulnerabilit... Admin User Analy... App Analyti... Operations NBU report System Time: 9:19 AM

## Formulář hlášení kybernetického bezpečnostního incidentu

Míra ochrany informace \*\*: Neomezeno (veřejné)

Kontaktní údaje

Orgán a osoba uvedená v § 3 písm. c) a e) zákona \*\*: Orgán a osoba

Identifikátor \*\*\*\*: Identifikátor orgánu nebo osoby

E-mail \*\*: nbu\_report@autocont.cz

Telefon \*\*: Telefon

Pokračování \*\*: Iniciační oznámení CERT/CSIRT týmu ID \*\*: ID incidentu

Detaily kybernetického bezpečnostního incidentu / kybernetické bezpečnostní události

Jedná se o hlášení \*\*: INCIDENTU

Datum a čas zjištění \*\*: YYYY MM DD hh mm Časová zóna \*\*: +-hh:mm

Datum a čas výskytu incidentu: YYYY MM DD hh mm Časová zóna: +-hh:mm

Kategorie incidentu \*: Kategorie I - méně závažný kybernetický bezpečnostní incident

# Zdravím účastníky Cacio semináře

LEOŠ STRÁNSKÝ

tel.: +420 603 558 487

e-mail: [Leos.Stransky@autocont.cz](mailto:Leos.Stransky@autocont.cz)

