Audit stavu kybernetické bezpečnosti v organizacích

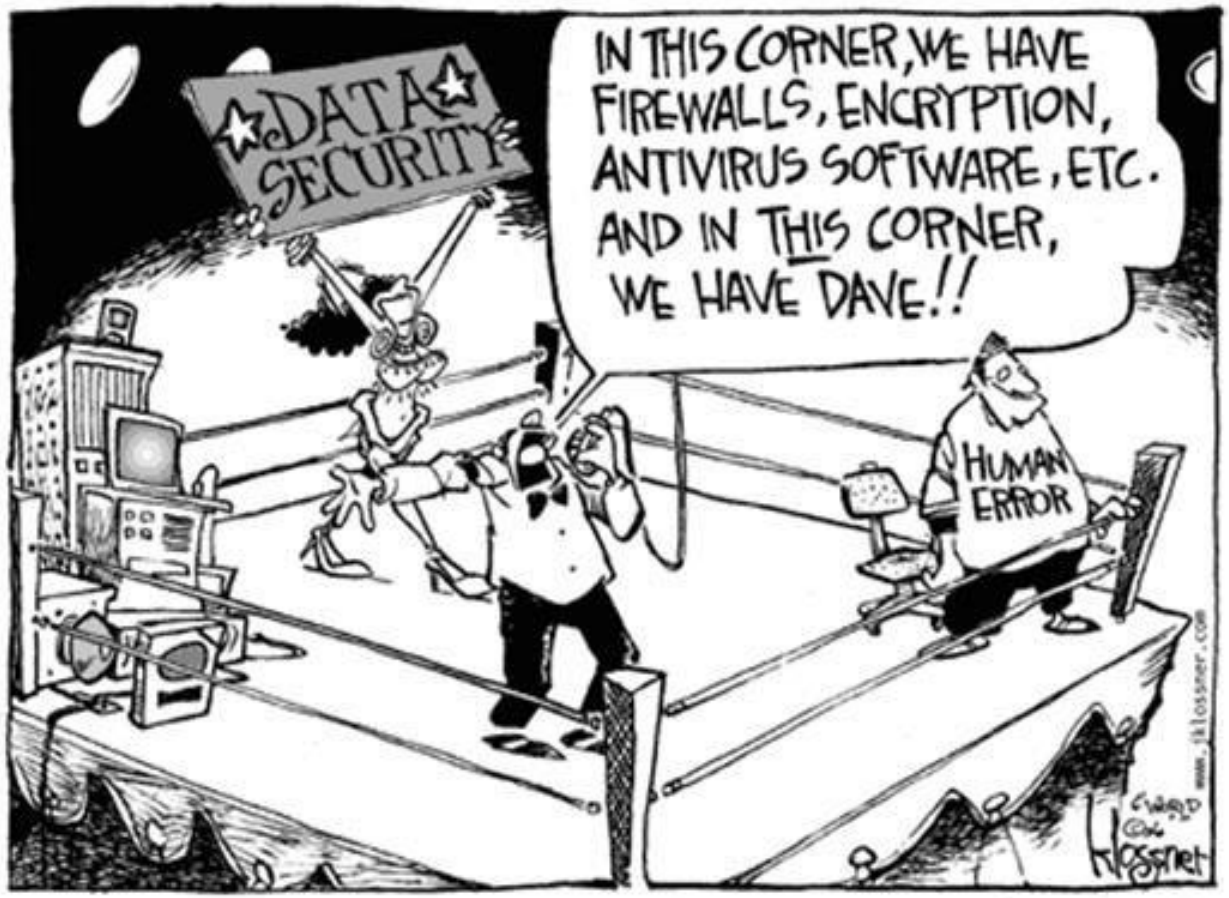
+420 724 573 462
kozak@axenta.cz
Jan Kozák, Presale Technical Specialist

AXENTA

AGENDA

- ÚVOD
- PROČ AUDIT STAVU KYBERNETICKÉ BEZPEČNOSTI?
- CO OD AUDITU NE/OČEKÁVAT?
- JAK AUDIT PROBÍHÁ?
- UKÁZKA TYPIZOVANÉHO AUDIT
- ZÁVĚR

Lepší **špetka**
prevence než **pytel**
nápravných
opatření!



Kdo jsme / víme jak na to

© 2009 [2002]

AXENTA

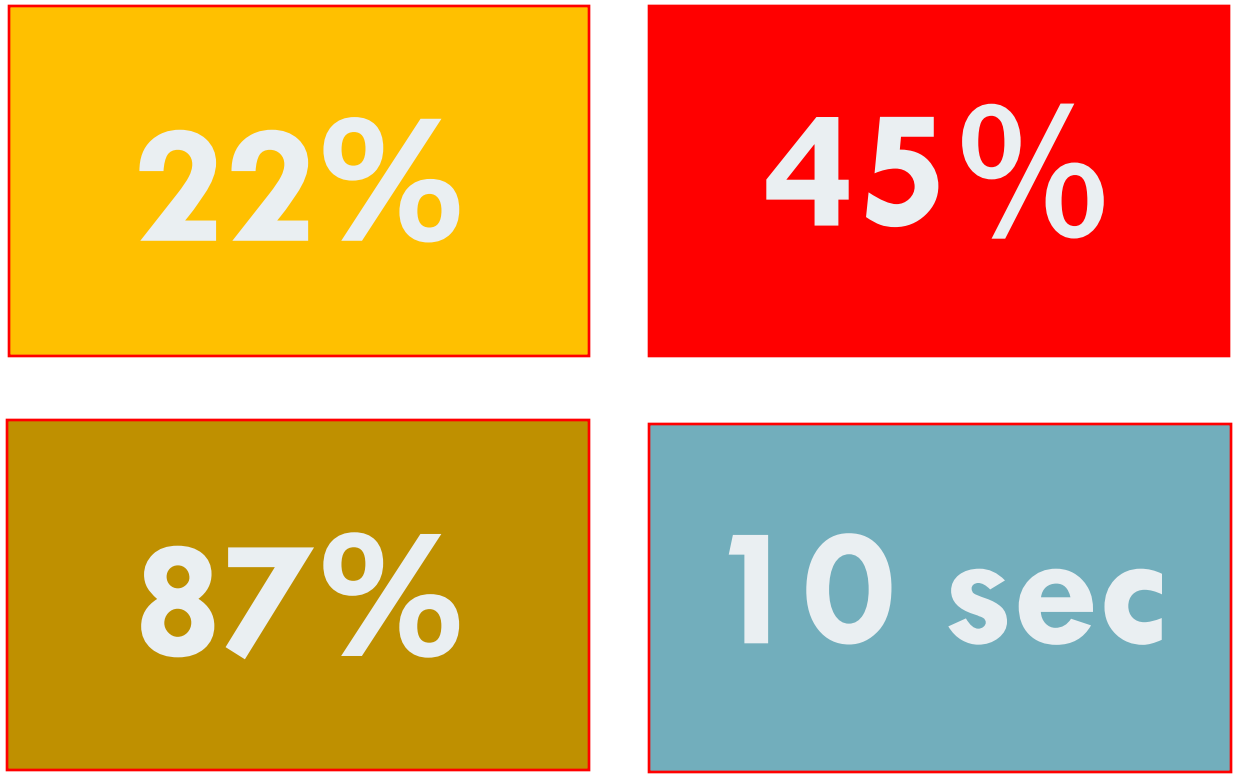
Reference

Finance

Utility

Public + ostatní

Nárůst kybernetických útoků v době COVIDU



* Check Point Security Report 2021

Vybrané kyber. útoky v ČR 2021

Nezvládnuté

- **7.1.2021**
  Nemocnice Horažďovice
- **16.3.2021**
  Poliklinika IPP
- **2.4.2021**
  Asbis CZ
- **7.4.2020**
  Olomoucký magistrát
- **15.4.2021**
  eSports.cz
- **17.5.2021**
  Národní knihovna

Zvládnuté

- **4.3.2021**
  MPSV a pražský magistrát
- **19.3.2021**
  Správa železnic a České dráhy
- **7.4.2021**
  Universita Palackého v Olomouci

Audit stavu kybernetické bezpečnosti

AXENTA

Důvody proč absolvovat audit?

- Odstranění provozní slepoty
- Potvrzení si toho, co už tak nějak tuším
- Pohled někoho jiného a nezávislého na stav
- Návod kde začít, kolik mne to bude stát času a peněz

Co od auditu ne/očekávat?

- **Objektivní** posouzení aktuálního stavu
  - procesy
  - lidé zdroje
  - technika
- **Doporučení** na co se zaměřit (nápravná opatření)
- **Doporučení** s čím začít (prioritizace, Quick Win, 80/20)
- Časovou a finanční **náročnost**

NE

Audit to vyřeší

Jak takový audit probíhá?

Naslouchám

Ptáme se

Ověřujeme

Radíme se

Hodnotíme

Doporučujeme

Vysvětlujeme

Zajímáme se

Ukázka typizovaného auditu

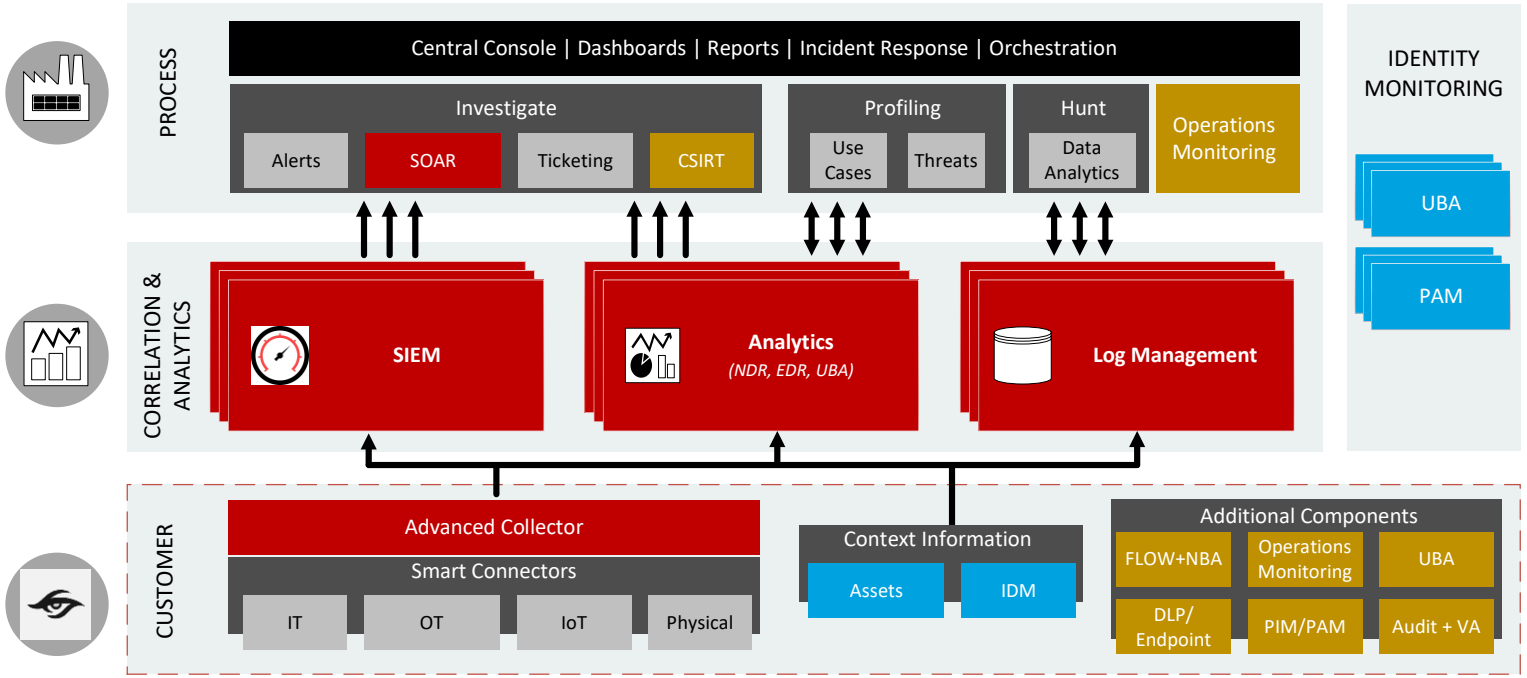
Kdo chvíli stál, stojí opodál

Intelligence-driven

Full-cyberchain

Time & cost-effective

Cyber SOC



Software

Event Management, SIEM, UBA, NDR, EDR, VA, SOAR, Provozní monitoring, Ticketing, Dashboardy

Analytika

Hunting Unknown Unknowns
Reporting/KPI
Threats Exchange/MISP
Threats Intelligence
Vulnerability Management
Runbooks / The Hive

Lidé

Procesy

Incident Response, konzultace, tvorba obsahu, vzdělávání
CSIRT, Forensics, Purple team

AXENTA

Děkuji

SIEM

Investigate

Security

User Behavior Anomaly

IT operations

Mobile Monitoring

Continuous compliance

Security Analytics

Storage

Log Management

Big Data

Workbench

managed cloud

in-house/legacy custom apps

Apps

Applications

SaaS

Systems Monitoring

Insider threats

Virtual

350+ CEF partners

Contextual Security Intelligence

Cloud security

AXENTA