CASE STUDY

-

Zajištění kybernetické bezpečnosti v ne/výrobní společnosti

Jan Kozák, Presale Technical Specialist

kozak@axenta.cz

AXENTA

Kdo jsme / víme jak na to

© 2009 [2002]

AXENTA

Co děláme?

Služby a procesy
v rámci IB a KB

Služby
bezpečnostního dohledového centra
(SOC)

Technologie pro
monitoring
kybernetické bezpečnosti

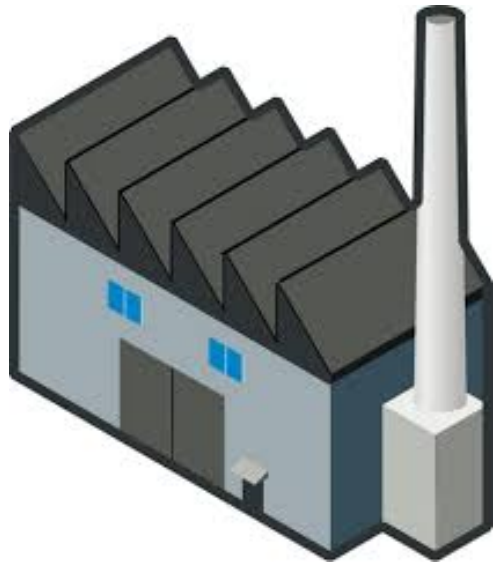
Zákazník *****

Společnost *** je známým průmyslovým podnikem, který se zabývá zpracováním kovových komponent v ucelené systémy ochrany.

Aktuálně uzavřela významný kontrakt na dodávku specializovaných dílů do bojových prostředků a její zákazník požadoval zvýšení ochrany a schopností detekce kybernetických útoků.

V oblasti zabezpečení kybernetické bezpečnosti neměla tato strojírenská společnost dostatečné zkušenosti a proto na trhu poptala komplexní zajištění.

V rámci výběrového řízení si jako partnera vybrala naši společnost.



Technologická Spolupráce

Sdružení českých a slovenských firem a expertů zabývajících se **kyber. bezpečností**

NSM NETWORK SECURITY MONITORING CLUSTER

Založeno **2010**

20 členů

opentext™

eset® Progress. Protected.

MUNI

Systémoví integrátoři

Konzultační specialisté

TESKALABS

Progress Flowmon

safetica

STŘEDNÍ ŠKOLA **INFORMATIKY, POŠTOVNICTVÍ** A **FINANČNICTVÍ** BRNO

CKB cluster kybernetickej bezpečnosti

Založeno **2018**

15 členů

AXENTA

Reference

Finance

Utility

Public + ostatní

AXENTA

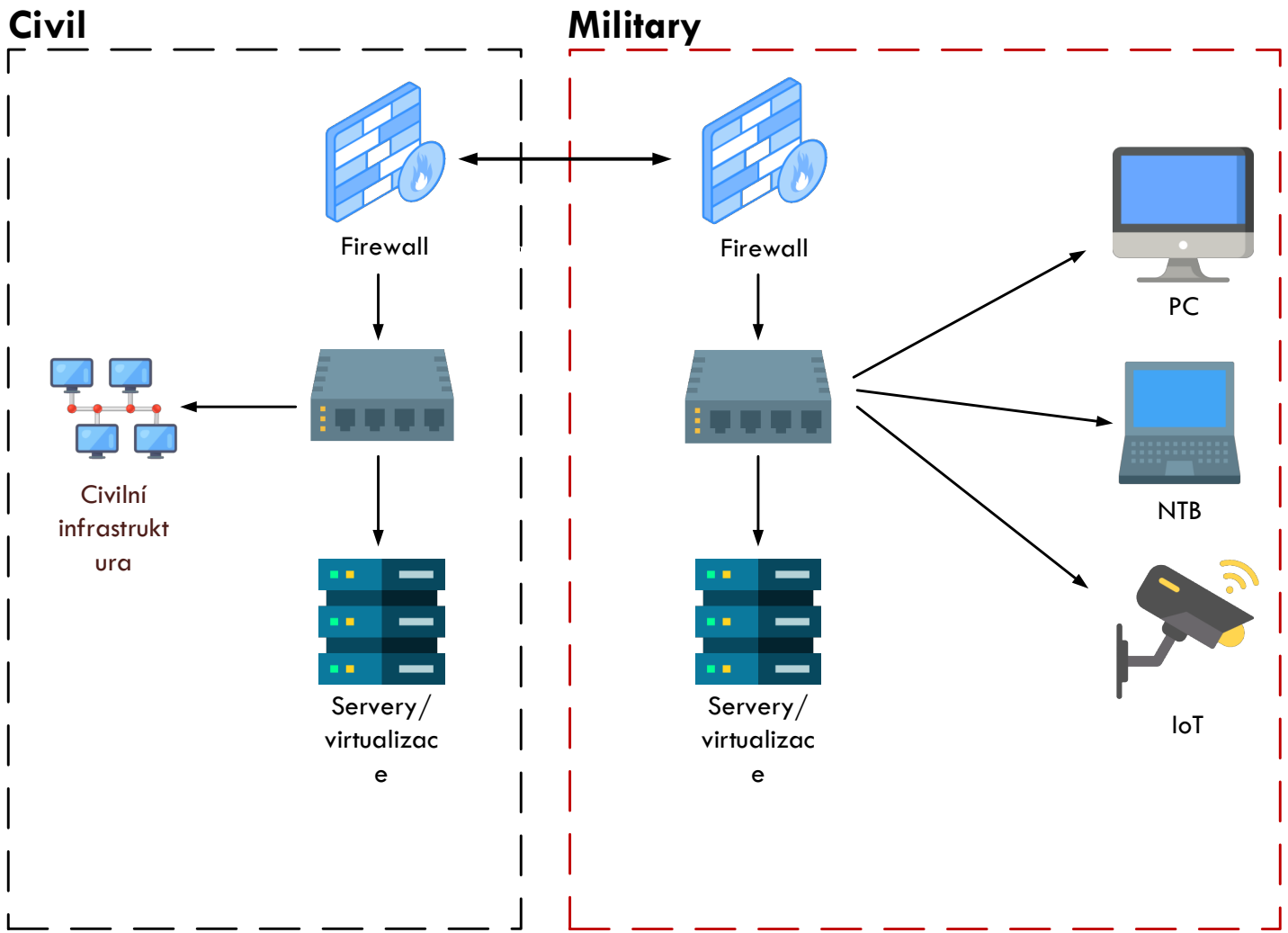
Lepší **špetka**
prevence než **pytel**
nápravných
opatření!

AXENTA


Case Study

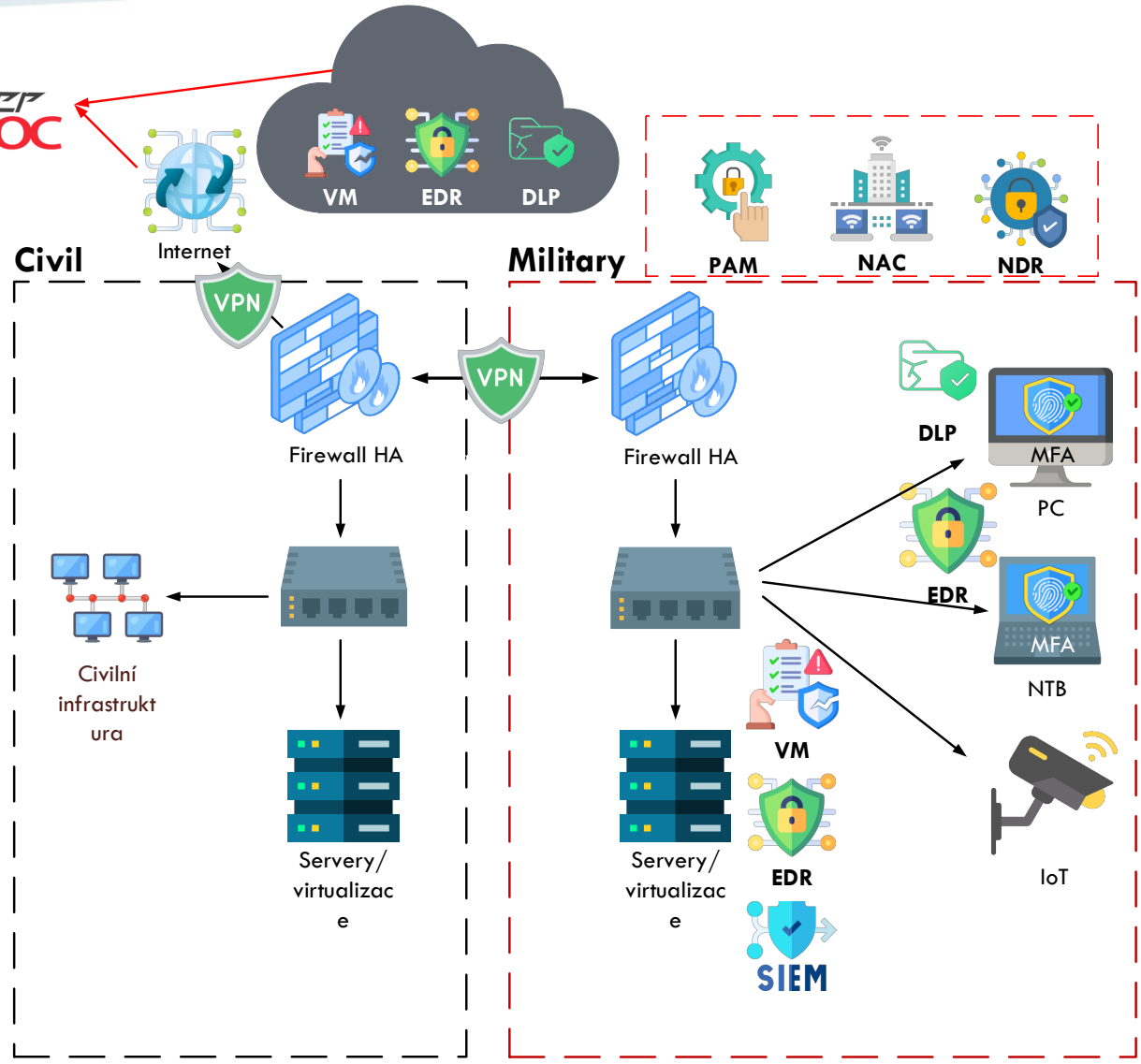
Původní stav

- Existuje pouze jedna síť
- Není dokončena segmentace
- Nejsou řízené přístupy zařízení
- Není FW v HA
- Nejsou instalovány technologie pro monitoring KB
- Nejsou popsány procesy a vytvořeny bezpečnostní směrnice



Cílový stav

- Civilní a Military část oddělena FW v HA
- Provedena segmentace a řízena komunikace
- Nasazen Network Access Control
- Přístupy k systému zabezpečeny MFA + VPN
- Privilegované účty kontrolovány PAM
- Detekce v síti monitorována NDR
- Koncové stanice a servery zabezpečeny EDR/XDR
- Logy zaznamenávány a vyhodnocovány LM+SIEM
- Detekce zranitelnosti pomocí VM
- Dohled prostřednictvím SOC
- Vytvořeny směrnice a procesy

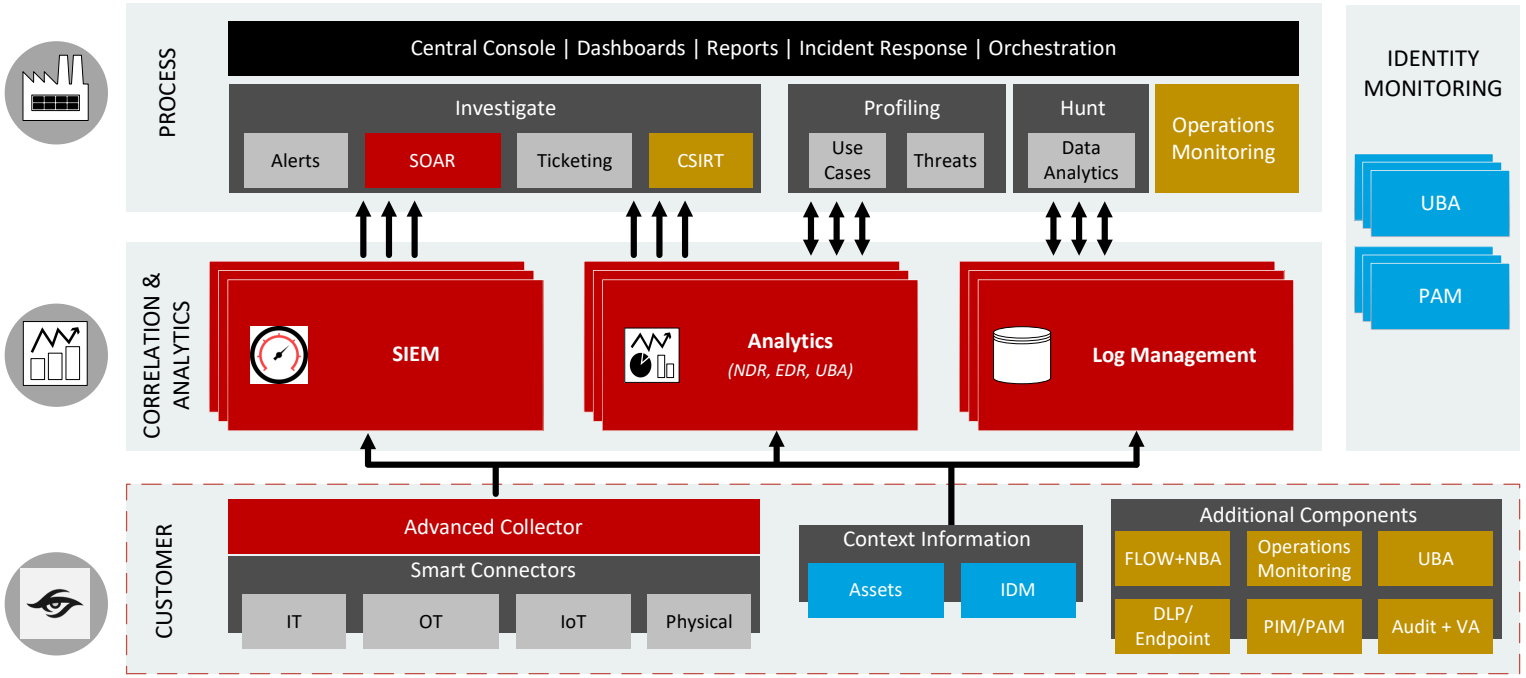


Intelligence-driven

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

Děkujeme

SIEM

Investigate

Security

User Behavior Anomaly

Continuous compliance

IT operations

Mobile Monitoring

Security Analytics

Storage

Log Management

Big Data

Workbench

managed cloud

in-house/legacy custom apps

Apps

Applications

SaaS

Systems Monitoring

Insider threats

Virtual

Cloud security

350+ CEF partners

Contextual Security Intelligence

AXENTA