VYPOŘÁDÁNÍ IDENTIFIKOVANÝCH RIZIK V OT PROSTŘEDÍCH

CORPUS SOLUTIONS
CYBERSECURITY EXPERTS

sales@corpus.cz
+420 241 020 333
www.corpus.cz

Corpus Solutions a.s.
Štětkova 1638/18
140 00 Praha 4

PŘEDSTAVENÍ

Pavel Klimeš

- Ředitel rozvoje bezpečnostních produktů v Corpus Solutions a.s.
- Nastavuje strategie efektivní kybernetické obrany u zákazníků
- Praktické zkušenosti s detekcí a zvládáním kybernetických útoků
- Autor tréninkového konceptu Cyber Defense Exercise
- 24 let praxe v oboru kybernetická bezpečnost

pavel.klimes@corpus.cz

Agenda

- Security Assessment – příběhy od skutečných zákazníků
- Moderní přístupy ke zvýšení bezpečnosti
- Zavedení bezpečnostního monitoringu OT prostředí, aktivace služeb SOC

Security Assessment

Zákazník č. 1 - Energetika

PRŮBĚH PoC – PRŮBĚŽNÉ VYHODNOCENÍ

COUNTERS

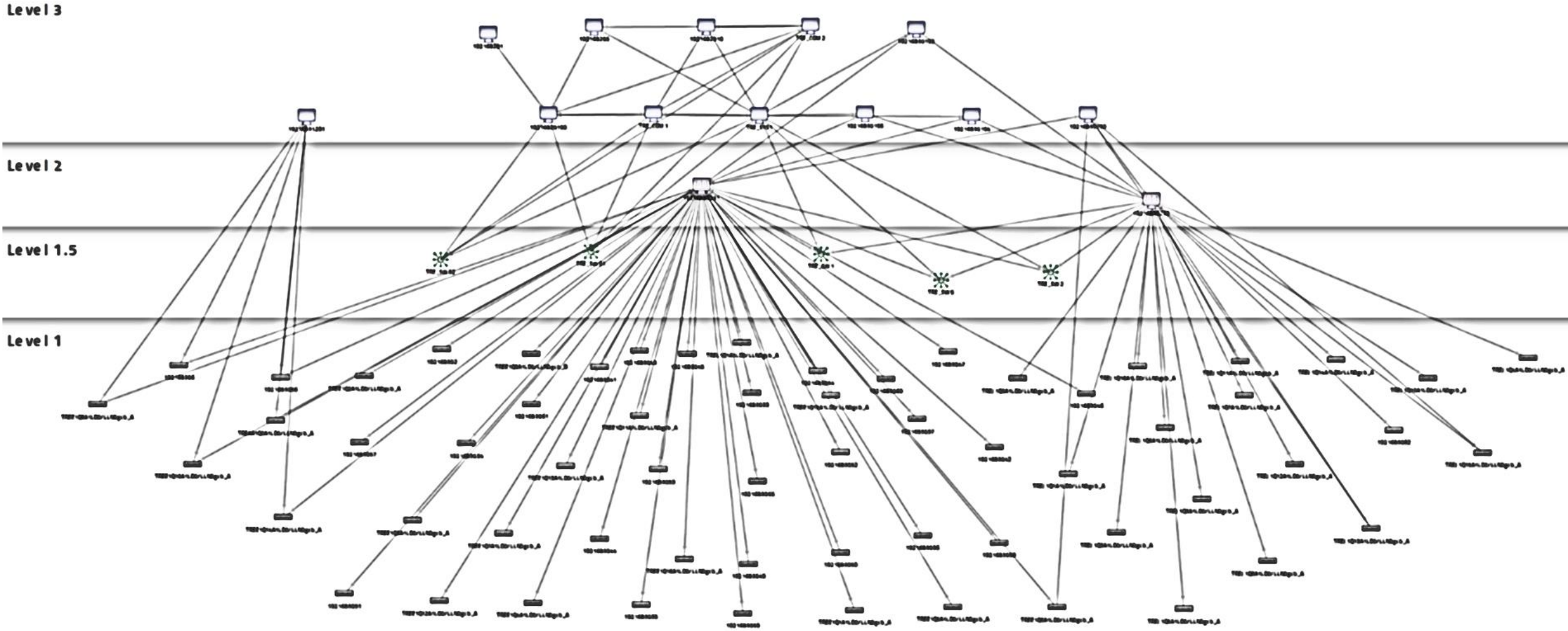
11	64	45	0	15
Vendors	OT Assets	IT Assets	IoT Assets	Protocols

KEY FINDINGS

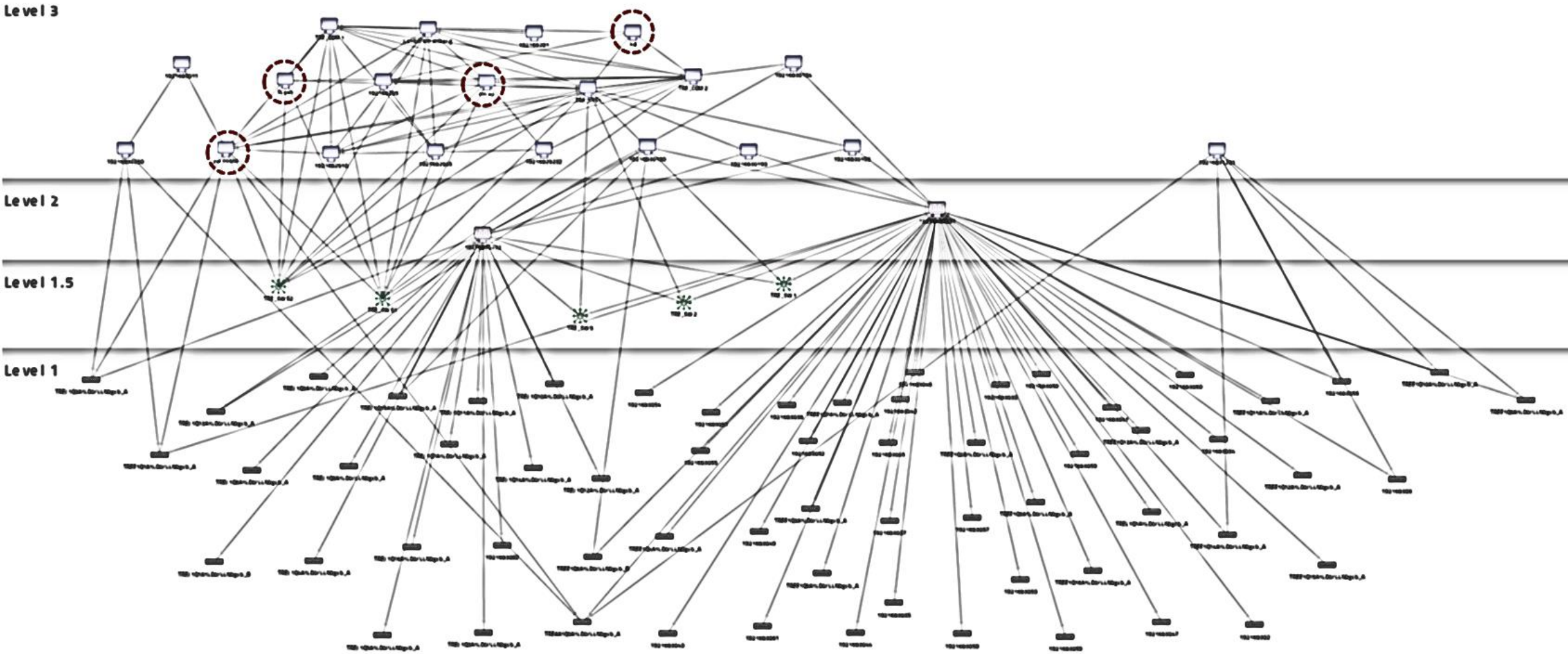
- 4 assets have 3 unpatched vulnerabilities - Full Match
- Top 4 Vulnerable Assets
- 18 assets are using 2 unsecured protocols: SMB, SNMP
- 4 assets have multiple network interfaces
- 6 assets are using default passwords

NETWORK HYGIENE SCORE **70%**

SLEDOVANÁ INFRASTRUKTURA – DLE MODELU PERA



ZÁZNAM ÚTOKU V PROSTŘEDÍ DLE PERA



ZÁCHYT PENETRAČNÍHO TESTU

IDENTIFIKACE PRŮBĚHU PEN-TESTU

- Každé připojení stanice útočníka bylo alertováno
- Techniky útočníka nástroj rozpoznal, pojmenoval a alertoval:
  - Skenování prvků v síti
  - Způsobení kolizí adres v síti
  - Používání vzorků malware
  - Neúspěšné pokusy o přihlášení
  - Průnik do úrovně Level 1 (dle PERA)
- Pro každé zařízení útočníka byl uložen záznam metadat o jeho chování

NAME	IP	MAC
nmap	[redacted] [redacted] fe80::2ad2:44ff:fe8c:f4d6	28:D2:44:8C:F4:D6
pwnbook	[redacted] [redacted] [redacted] fe80::6e9a:cd3d:b19c:4171	3C:97:0E:B9:B0:58
RLyeh	[redacted] fe80::1c59:b8c5:69a5:5f0a	38:C9:86:30:A1:82
kali	[redacted] fe80::a00:27ff:fe3c:6379	08:00:27:3C:63:79

PRŮBĚH PoC – PRŮBĚŽNÉ VYHODNOCENÍ

COUNTERS

11	64	45	0	15
Vendors	OT Assets	IT Assets	IoT Assets	Protocols

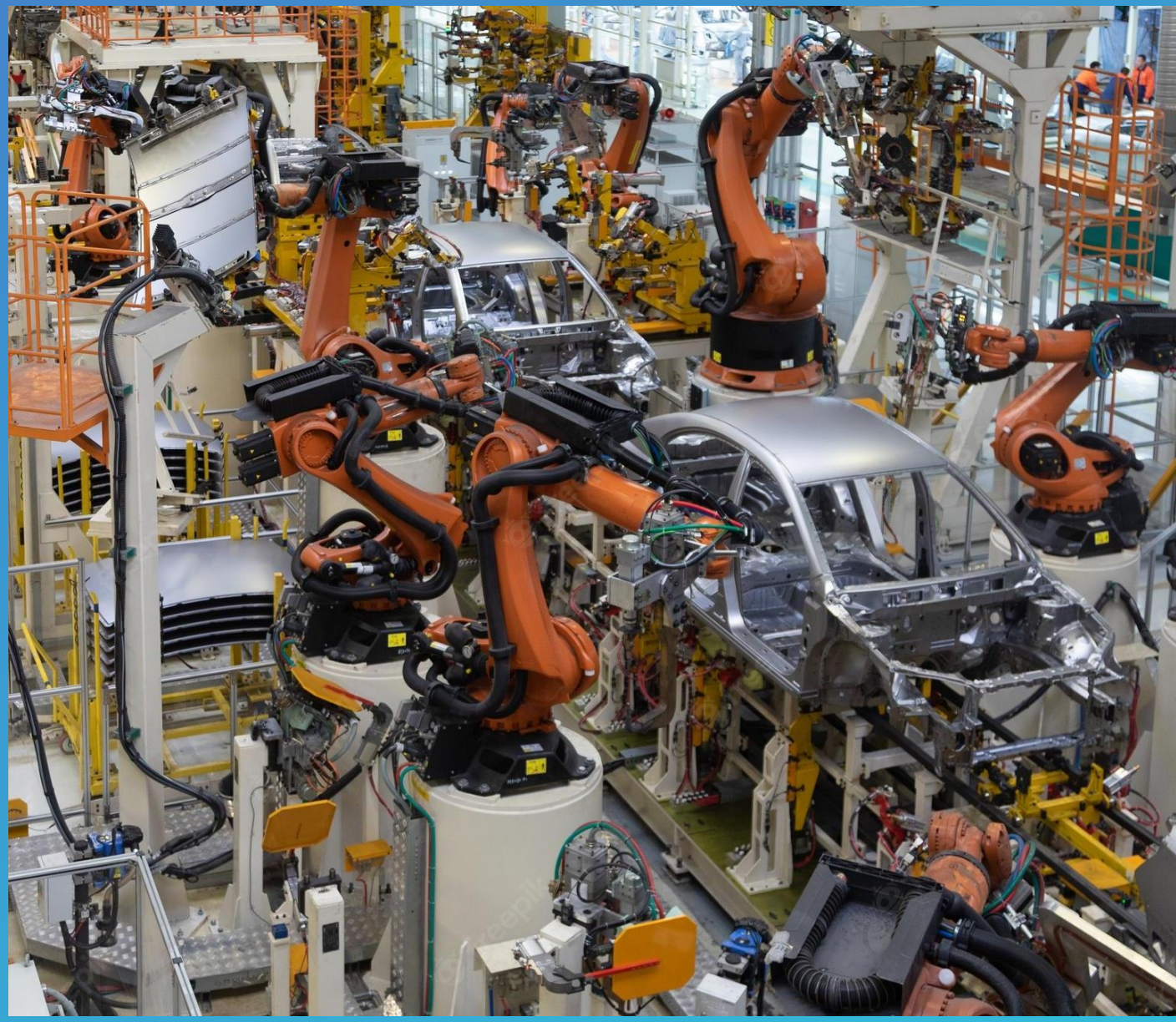
KEY FINDINGS

- ! 19 security alerts have been detected
- ! 43 process integrity alerts have been detected
- 1 asset was communicating with 1 external IP (1 of them is ghost)
- 28 assets are using 8 unsecured protocols: FTP, SMB, SMTP, SNMP, SSL,...
- 6 assets have multiple network interfaces
- 7 assets managed 9 assets remotely using protocols: RDP, SSH, TELNET, VNC
- 2 OT-assets performed data-acquisition write operations on 62 PLCs/Controllers/RTUs/IEDs
- 7 assets are using default passwords
- 2 assets using IT protocols: CAPWAP-CONTROL, LDAPS,... , with 3 PLCs/Controllers/RTUs/IEDs

NETWORK HYGIENE SCORE **10%**

Security Assessment

Zákazník č. 2 - Automotiv



PRŮBĚH PoC – PRŮBĚŽNÉ VYHODNOCENÍ

COUNTERS

13	232	429	0	28
Vendors	OT Assets	IT Assets	IoT Assets	Protocols

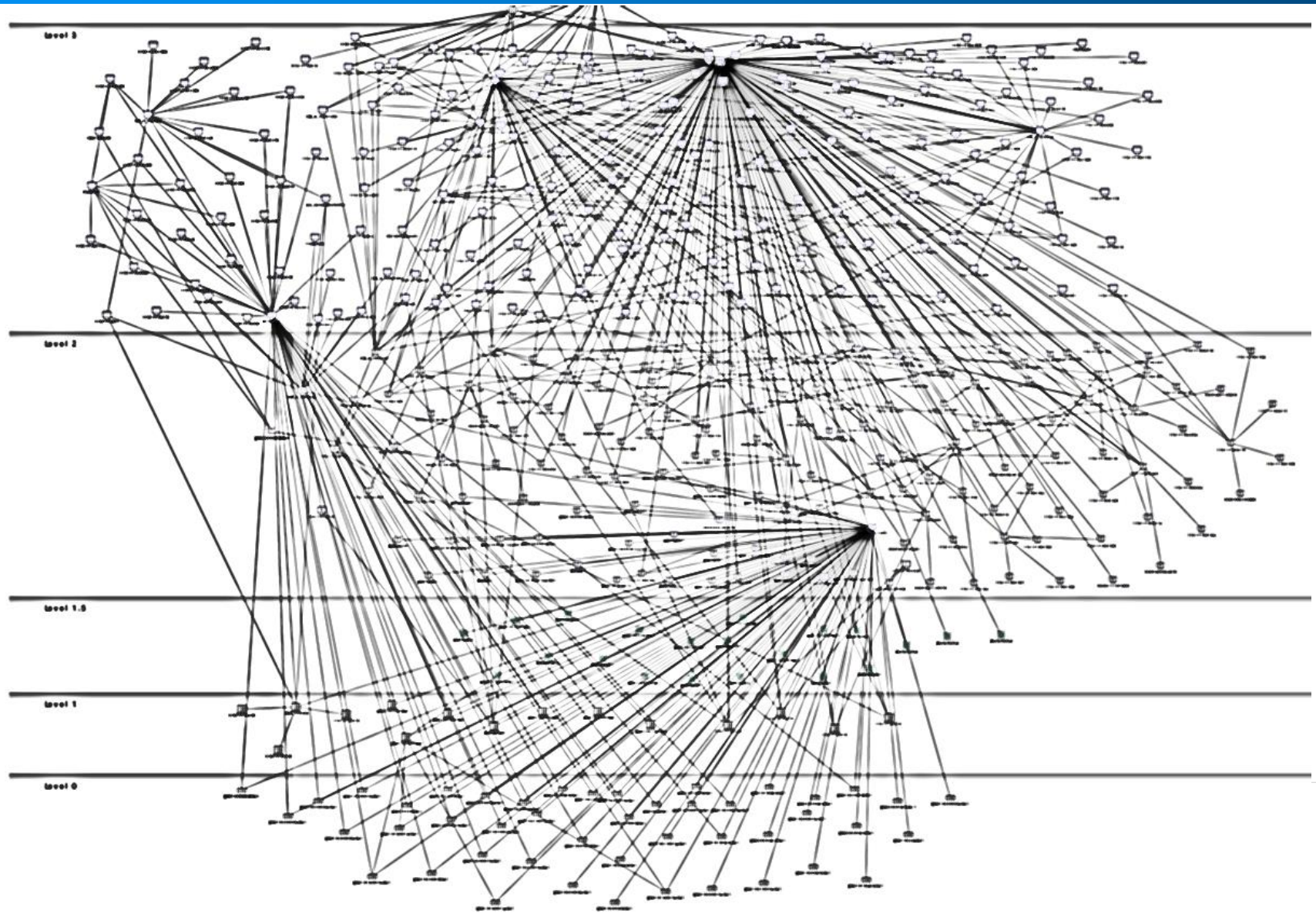
KEY FINDINGS

- ! 11 security alerts have been detected
- ! 587 process integrity alerts have been detected
- 2 assets have 11 unpatched vulnerabilities - Full Match
- Top 2 Vulnerable Assets
- 470 assets were communicating with 2 external IPs
- 47 assets are using 5 unsecured protocols: FTP, SMB, SNMP, SSL, VNC
- 25 assets have 26 unpatched vulnerabilities - Vendor and Model Match
- 1 asset has multiple network interfaces
- 5 assets managed 6 assets remotely using protocols: RDP, VNC
- 8 assets are using SMBv1 Protocol only for negotiate
- 10 assets are using default passwords
- 2 assets using IT protocol: SSL , with 5 PLCs/Controllers/RTUs/IEDs

NETWORK HYGIENE SCORE **22%**

The calculation represented in the Hygiene Score indicates the cumulative risk level that the alerts, insights, and assets pose to the system. A low value means that your system is more vulnerable to attacks.

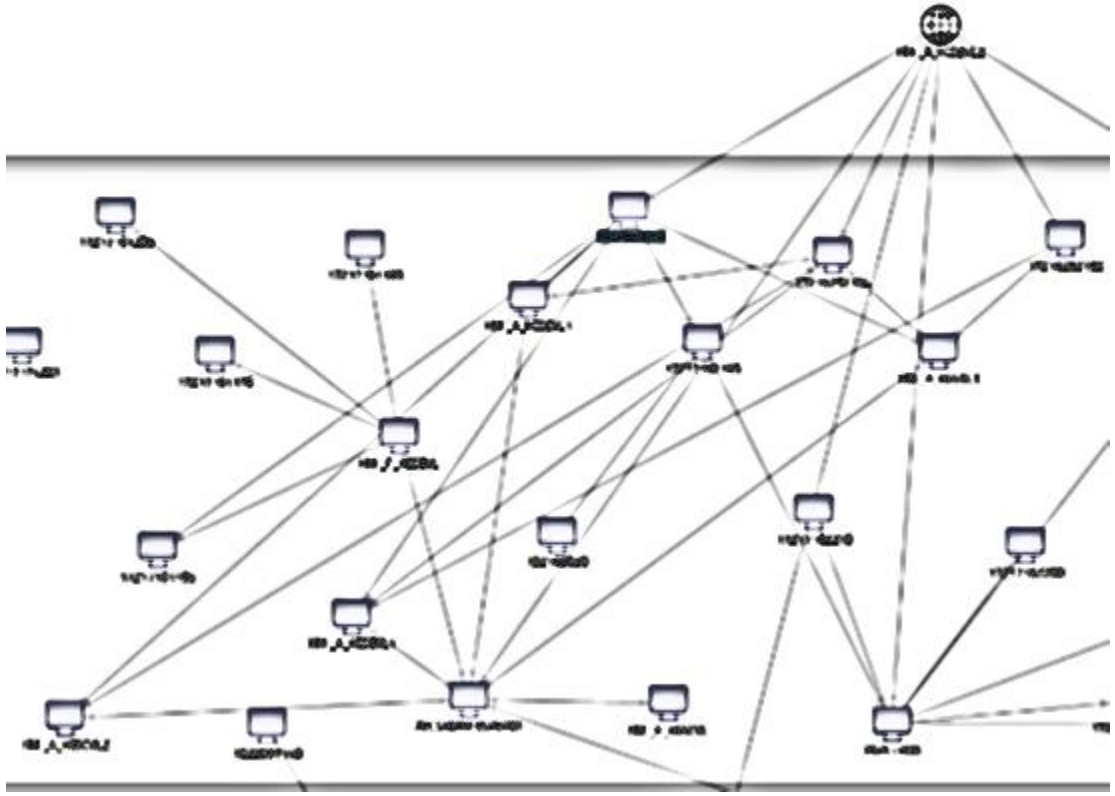
PRŮBĚH PoC – PERA MODEL



Průběh PoC – Zajímavosti (RASPBERRY Pi)

Nález zařízení „RASPBERRYPI“

- Zařízení bylo v síti připojeno jen dočasně
- Alertováno jako cizí zařízení
- Alertováno jako „HIGHLY CONNECTED ASSET“
- Zaznamenány neúspěšné pokusy o přihlášení k více OT zařízením



Průběh PoC – Zajímavosti (EWON Router)

Nález zařízení „EWON Router“

- Zařízení bylo v síti připojeno jen dočasně pro účely pokrytí vzdálených přístupů servisních partnerů
- Alertováno jako cizí zařízení
- Alertováno jako „HIGHLY CONNECTED ASSET“
- Zařízení nebylo dokumentováno
- Zařízení přetrvává v prostředí i rok poté, co již není nezbytné.

Kybernetická bezpečnost v OT

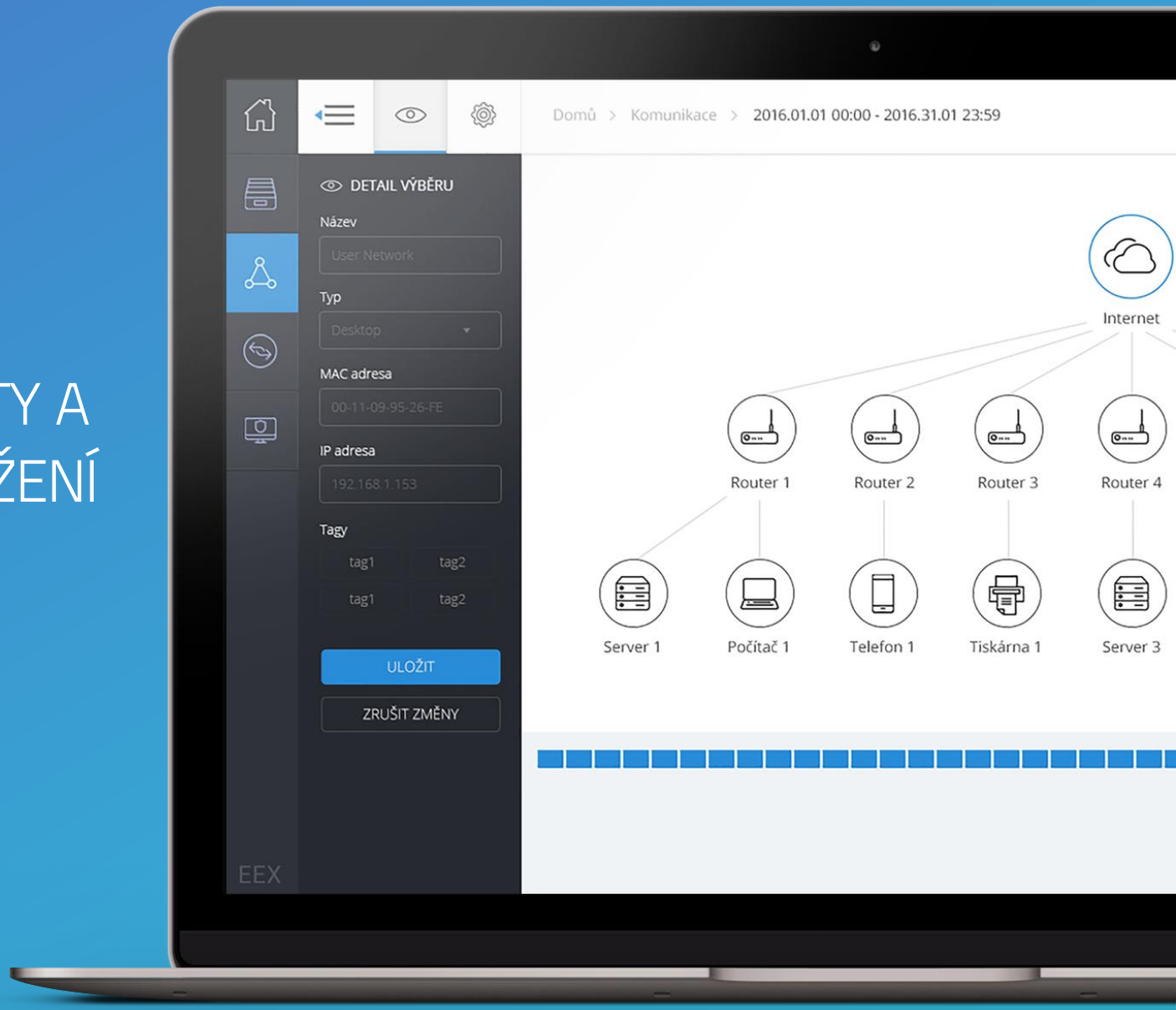
Moderní přístupy ke zvýšení bezpečnosti

Bezpečnostní opatření v OT

Id	Opatření
O1	Ochrana integrity sítě
O2	Vypořádání zranitelností
O3	Centrální správa přístupových údajů
O4	Bezpečný přístup technické podpory
O5	Řízení komunikací mezi OT sítěmi
O6	Konfigurační BASELINE pro IT systémy ve výrobě
O7	Bezpečnostní požadavky na dodavatele
O8	Plány zálohování a obnovy (DR)
O9	Reakční scénáře

Opatření pro podporu visibility a detekce kybernetického ohrožení

OPATŘENÍ PRO PODPORU VISIBILITY A DETEKCE KYBERNETICKÉHO OHROŽENÍ



OT BEZPEČNOSTNÍ NÁSTROJE – ANOMALY DETECTION

PROVOZ POD DOHLEDEM UMĚLÉ INTELIGENCE

Check Point Asset and Anomaly Detection chrání bezpečnost lidí, majetku a kritických procesů před kybernetickými útoky.

Nástroj poskytuje:

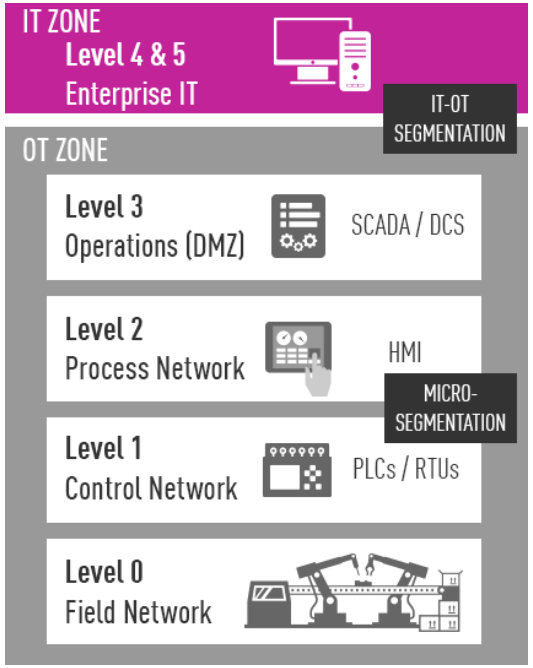
- detailní vhled do sítí průmyslových řídicích systémů
- monitoring v reálném čase, pasivní vulnerability management
- kontrolu nad vzdáleným přístupem třetích stran

V chráněné OT infrastruktuře jsou zcela pasivní a tudíž bezpečné pro zachování dostupnosti a stability výrobních procesů.

OT BEZPEČNOSTNÍ NÁSTROJE – ASSET AND ANOMALY DETECTION

KLÍČOVÉ VLASTNOSTI POUŽÍVANÝCH NÁSTROJŮ

- Využívají moderní algoritmy – ML/AI a neuronové sítě
- Vizualizují infrastrukturu dle modelu PERA a dokumentují aktiva
- Detekují zranitelnosti a projevy známých kybernetických hrozeb
- Upozorňují na netypické chování – detekce anomálií
- Tvoří baseline pravidla, vzory správného a nebezpečného chování
  - Mód učení - Odposlech komunikace, interakcí, vytváření pravidel
  - Mód provozní - Aplikování naučené báze dat a alerting

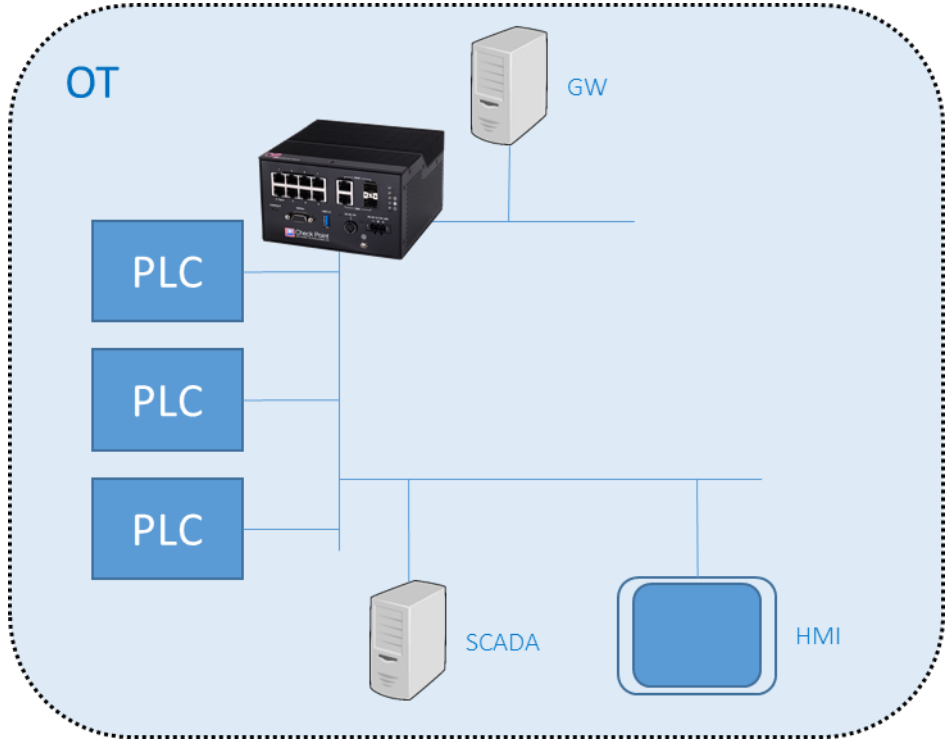


ICS Vendors

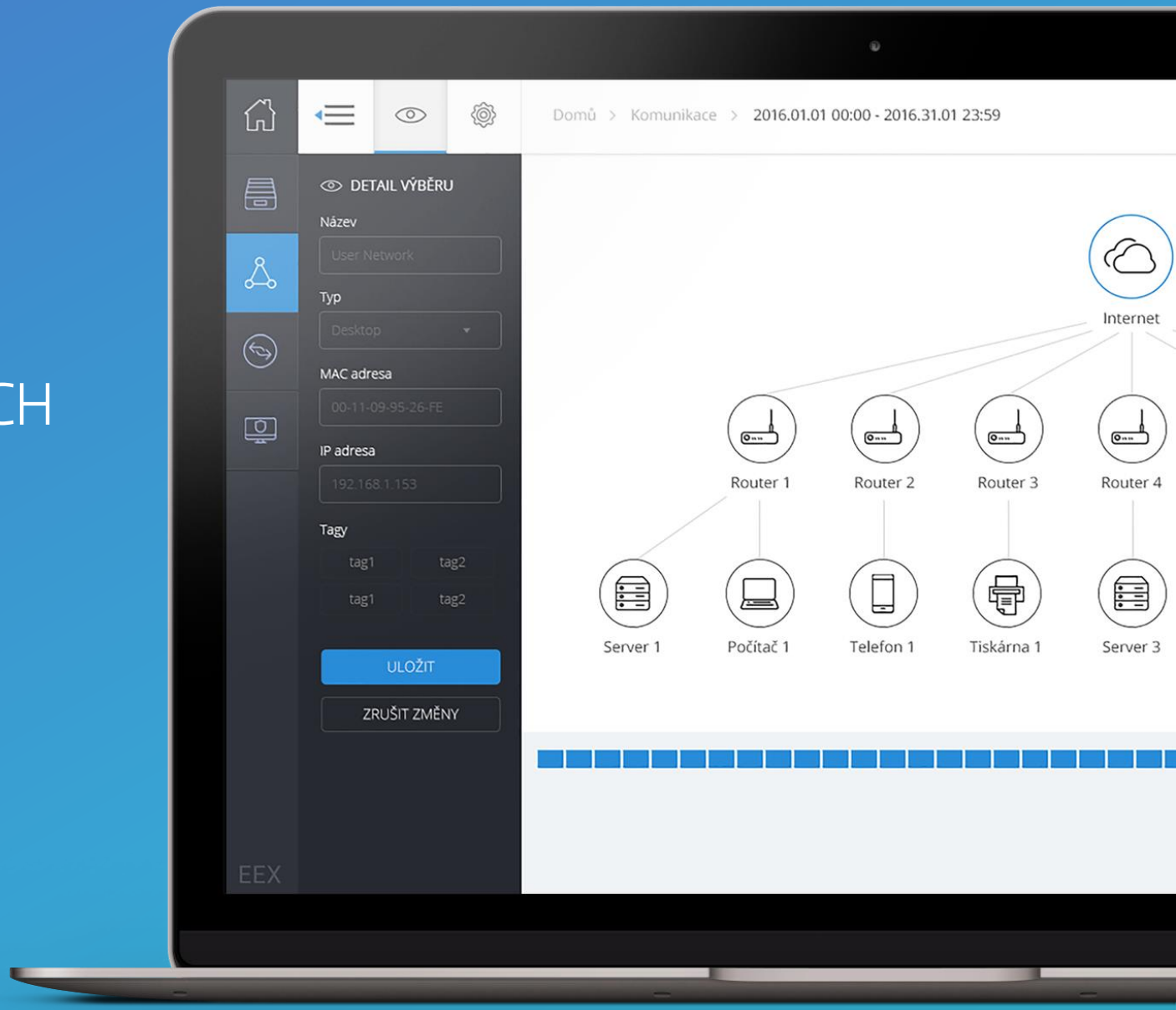
ABB · Honeywell · GE · Schneider Electric · OMRON · EMERSON · Rockwell Automation · MITSUBISHI · YOKOGAWA · SIEMENS

BEZPEČNOSTNÍ OPATŘENÍ V OT

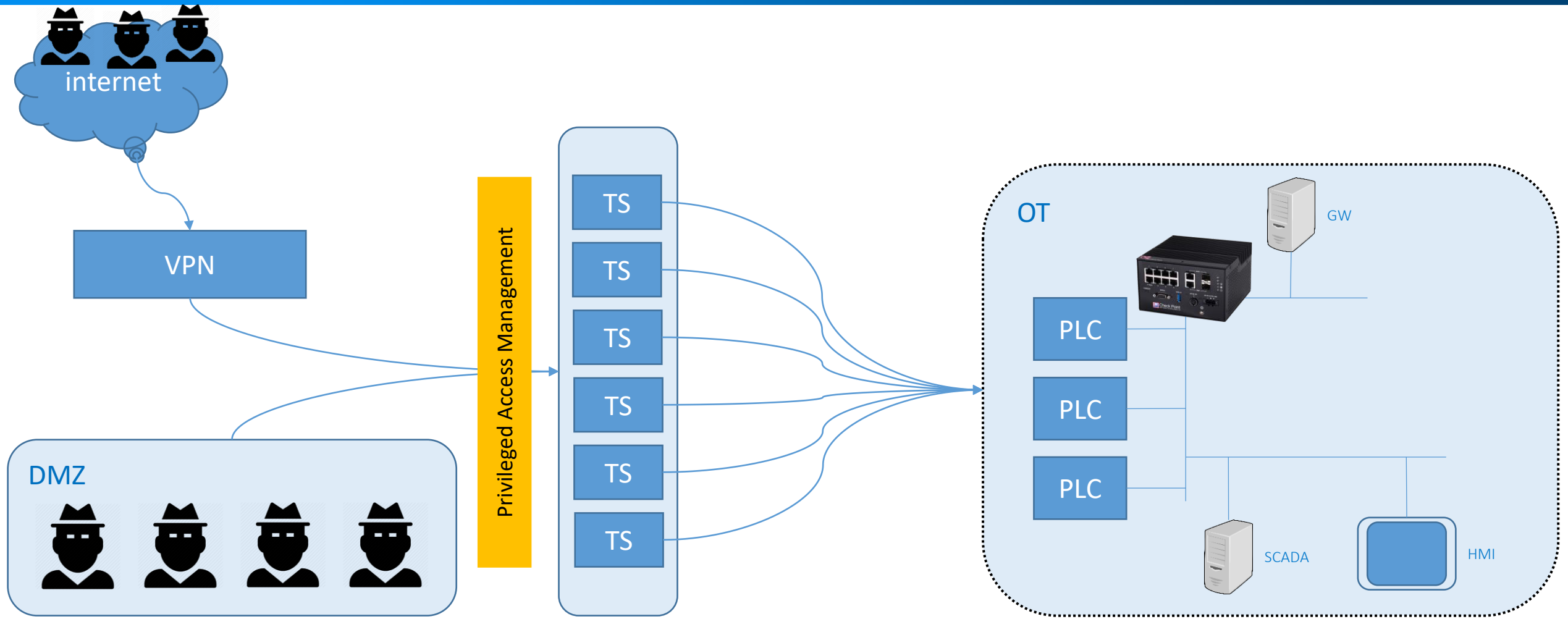
Id	Opatření	Přínos opatření
O1	Ochrana integrity sítě	Opatření uplatněno zavedením nástrojů typu AAD.
O2	Vypořádání zranitelností	
O3	Centrální správa přístupových údajů	Opatření pokryto částečně zavedením AAD – pouze schopnost zaznamenání porušení bezpečnostních zásad nebo standardů.
O4	Bezpečný přístup technické podpory	
O5	Řízení komunikací mezi OT sítěmi	
O6	Konfigurační BASELINE pro IT systémy ve výrobě	
O7	Bezpečnostní požadavky na dodavatele	
O8	Plány zálohování a obnovy (DR)	
O9	Reakční scénáře	



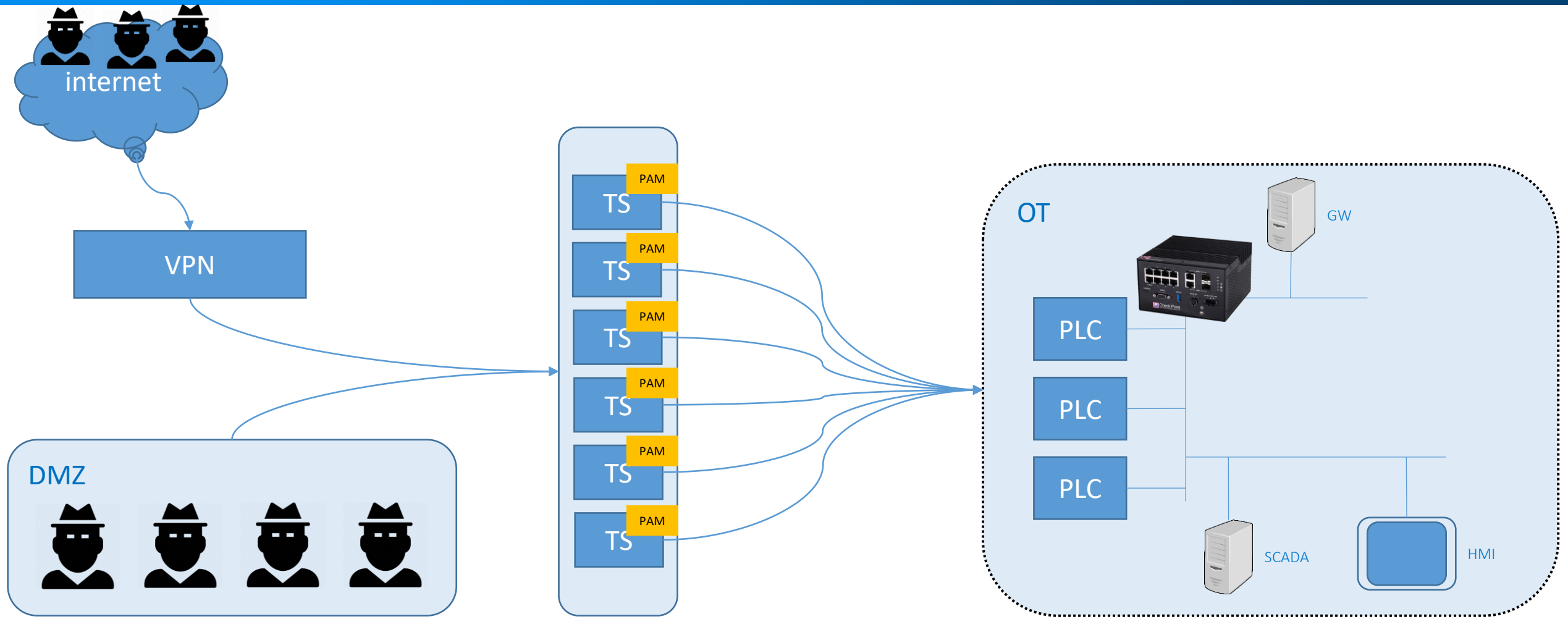
OPATŘENÍ PRO ŘÍZENÍ VZDÁLENÝCH PŘÍSTUPŮ A PASSWORD MGMT.



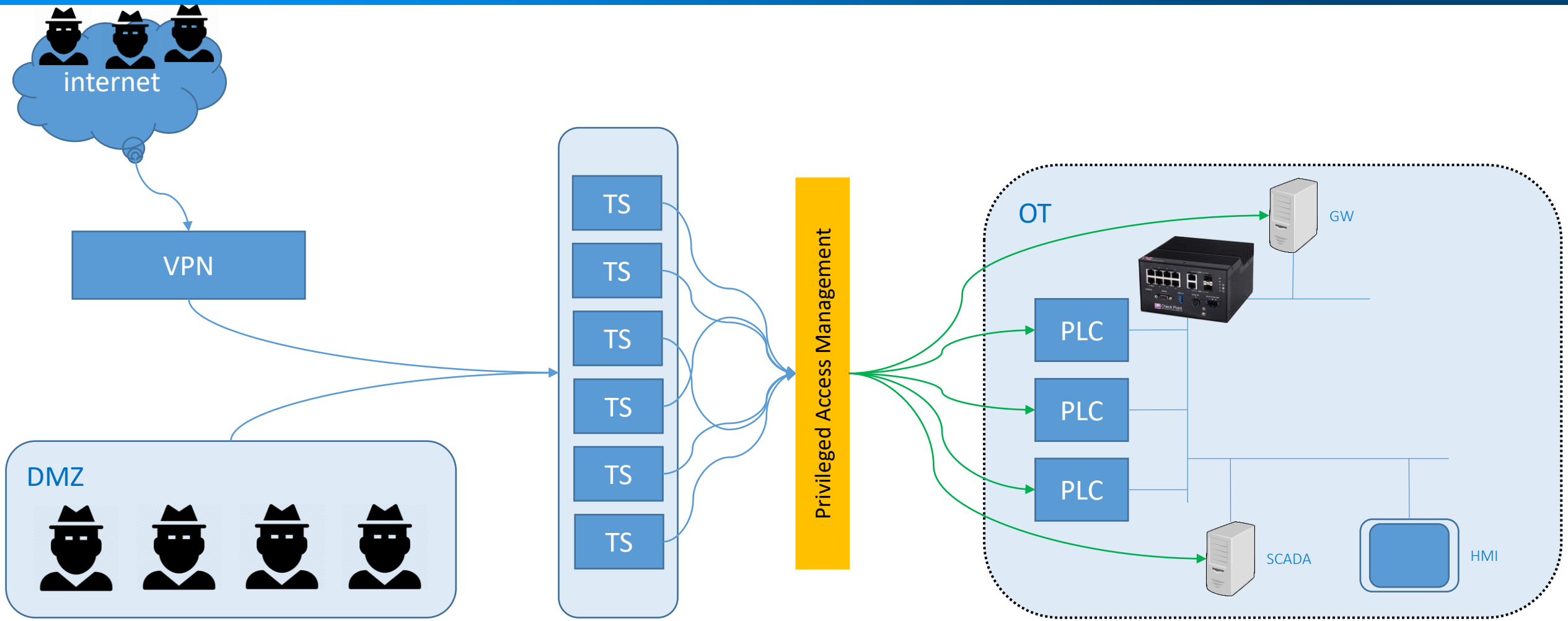
PIM Jump Server (FRONT) + AAD Integrity protection



JUMP + PSM + AAD INTEGRITY PROTECTION



PIM Jump Server (BACK) + AAD Integrity protection



Bezpečnostní opatření v OT

Id	Opatření	Přínos opatření
O1	Ochrana integrity sítě	Opatření uplatněno zavedením nástrojů typu AAD, PIM a soustavou JUMP SERVERŮ.
O2	Vypořádání zranitelností	
O3	Centrální správa přístupových údajů	Opatření pokryta plně a částečně zavedením nástrojů AAD a zavedením systému řízení privilegovaných přístupů. Je tedy minimalizováno riziko zavlečení nákazy.
O4	Bezpečný přístup technické podpory	
O5	Řízení komunikací mezi OT sítěmi	
O6	Konfigurační BASELINE pro IT systémy ve výrobě	
O7	Bezpečnostní požadavky na dodavatele	
O8	Plány zálohování a obnovy (DR)	
O9	Reakční scénáře	

Jump server

Privileged Access Management

OT Security Monitoring

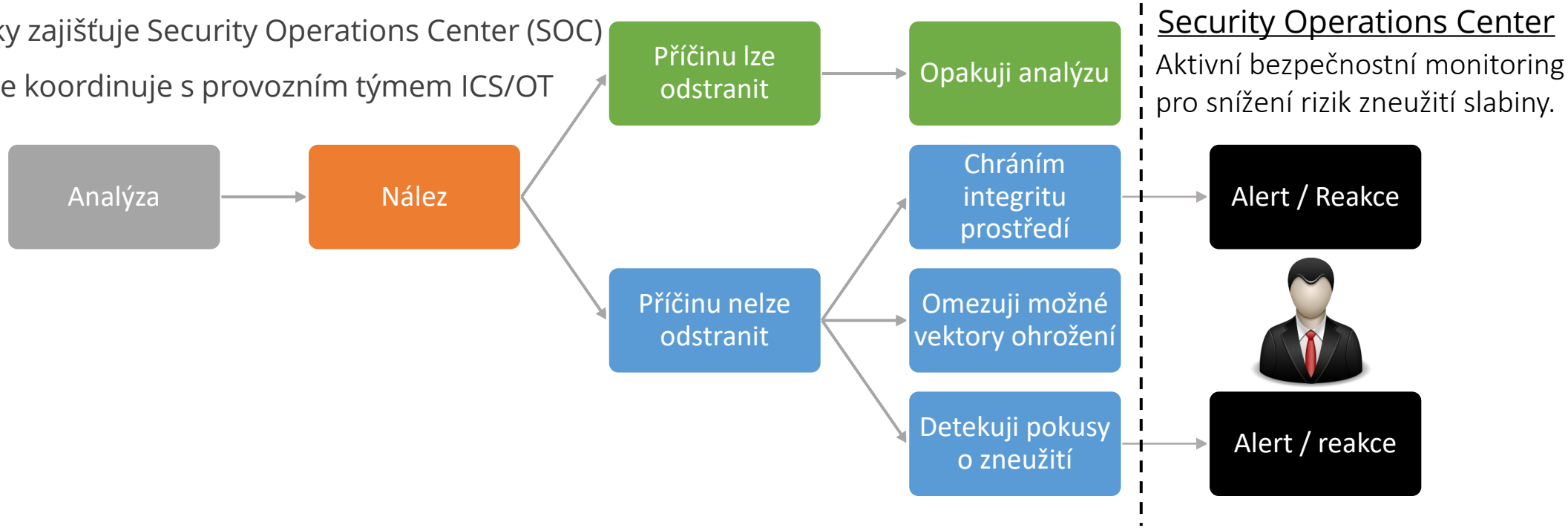
PROAKTIVNÍ BEZPEČNOSTNÍ DOHLED A REAKCE NA INCIDENTY

PROAKTIVNÍ BEZPEČNOSTNÍ DOHLED A REAKCE

ZPŮSOB VYPOŘÁDÁNÍ IDENTIFIKOVANÝCH NÁLEZŮ

- U některých nálezů **nelze** příčinu odstranit v požadovaném čase a rozpočtu

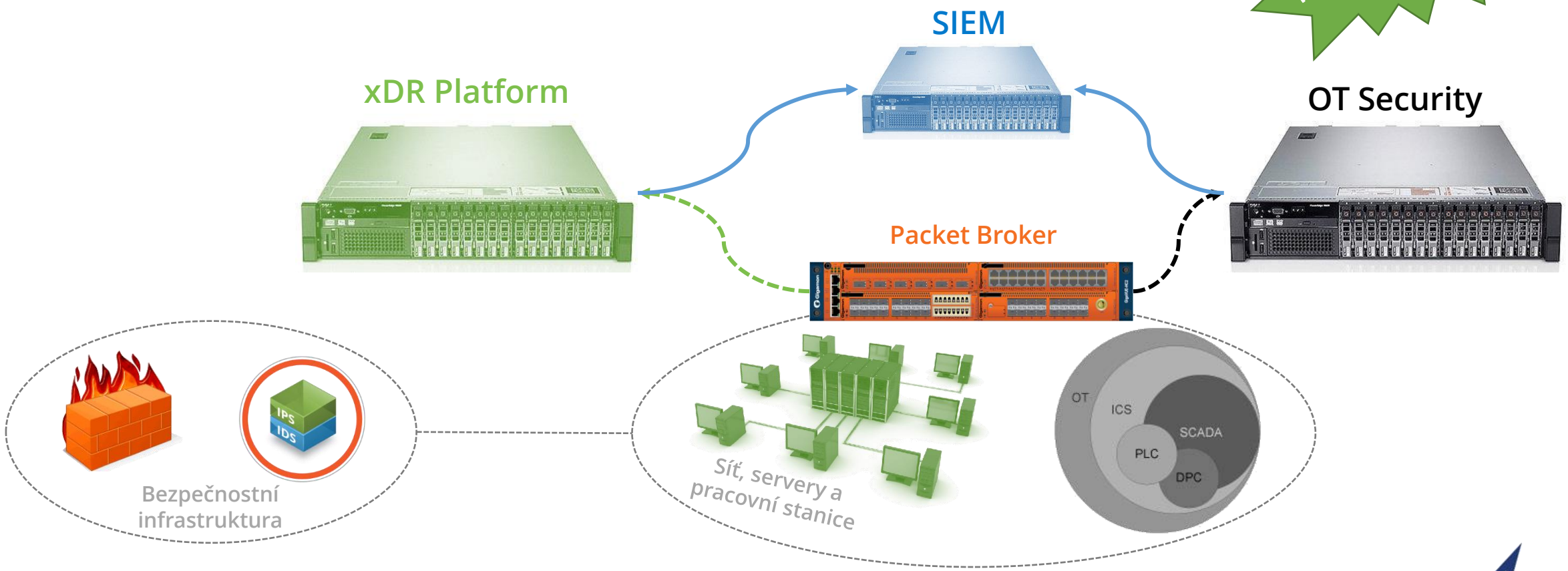
- Proto je zvolen způsob aktivního dohledu
  - Typicky zajišťuje Security Operations Center (SOC)
  - Reakce koordinuje s provozním týmem ICS/OT



SOC DRIVEN – KYBERNETICKÁ BEZPEČNOST

Moderní nástroje pro efektivní zastřežení prostředí OT/IoT

Rychlá implementace: 3 – 20 týdnů

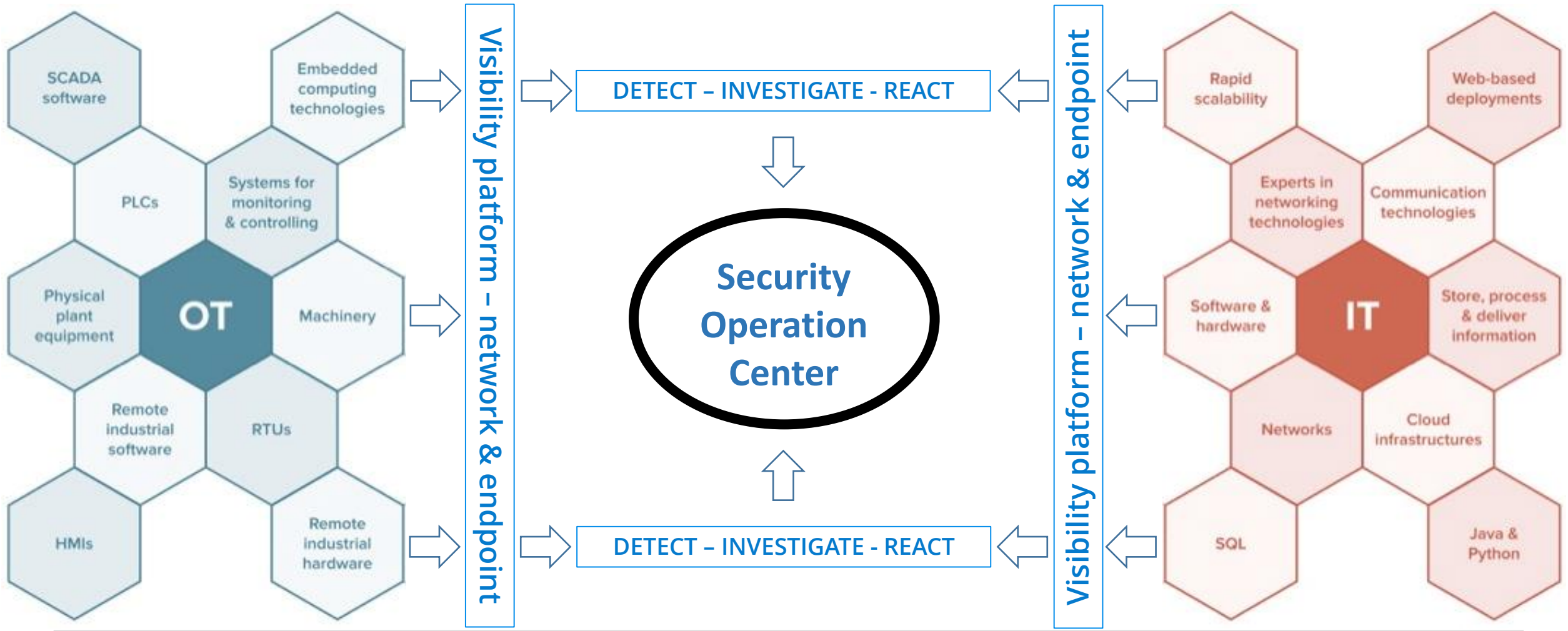


LOCKHEED MARTIN

Průzkum | Zbrojení | Doručení | Exploitace | Instalace | C&C | Cíl

Security Operations Center

Koncepce fungování hybridního SOC



Bezpečnostní opatření v OT

Id	Opatření	Přínos opatření
O1	Ochrana integrity sítě	Opatření uplatněno zavedením nástrojů typu AAD, PIM a soustavou JUMP SERVERŮ.
O2	Vypořádání zranitelností	
O3	Centrální správa přístupových údajů	Opatření pokryto částečně zavedením nástrojů AAD a zavedením systému řízení privilegovaných přístupů. Je tedy minimalizováno riziko zavlečení nákazy.
O4	Bezpečný přístup technické podpory	
O5	Řízení komunikací mezi OT sítěmi	
O6	Konfigurační BASELINE pro IT systémy ve výrobě	
O7	Bezpečnostní požadavky na dodavatele	
O8	Plány zálohování a obnovy (DR)	
O9	Reakční scénáře	

Jump server

Privileged Access Management

OT Security Monitoring

Security Operations Center