

Ochrana proti kybernetickým útokům, bezpečnost IoT a OT systémů

21.1.2026





Kdo jsem?

Kdo jsem?

Jakub Alimov, CEH, CHFI



architekt kybernetické bezpečnosti,

RANSOMWARE hunter,

konzultant informační bezpečnosti,

více jak 16+ let prokazatelných zkušeností s kybernetickou
bezpečností

<https://www.linkedin.com/in/jakub-alimov-332b1020/>



Kdo je Alinet?



**Jsme IT Security firma se
specializací na
kybernetické útoky.**

DIGITAL FORENSICS AND INCIDENT RESPONSE





**Jsme IT Security firma se
specializací na
kybernetické útoky.**

DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ RANSOMWARE útoky
- ✓ Forezní vyšetřování kybernetických incidentů
- ✓ Krizové řízení
- ✓ AUDIT připravenosti na RANSOMWARE útok



**Jsme IT Security firma se
specializací na
kybernetické útoky.**

DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ RANSOMWARE útoky
- ✓ Forenzní vyšetřování kybernetických incidentů
- ✓ Krizové řízení
- ✓ AUDIT připravenosti na RANSOMWARE útok

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI



**Jsme IT Security firma se
specializací na
kybernetické útoky.**

DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ RANSOMWARE útoky
- ✓ Forenzní vyšetřování kybernetických incidentů
- ✓ Krizové řízení
- ✓ AUDIT připravenosti na RANSOMWARE útok

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI

- ✓ NASTARTOVÁNÍ kybernetické bezpečnosti
- ✓ ARCHITEKT kybernetické bezpečnosti dle ZoKB
- ✓ Přehledové testy zranitelností
- ✓ ISO IEC 27001, ISO IEC 62443, NIST CSF, NIS2
- ✓ Zabezpečení kritické infrastruktury



**Jsme IT Security firma se
specializací na
kybernetické útoky.**

DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ RANSOMWARE útoky
- ✓ Forenzní vyšetřování kybernetických incidentů
- ✓ Krizové řízení
- ✓ AUDIT připravenosti na RANSOMWARE útok

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI

- ✓ NASTARTOVÁNÍ kybernetické bezpečnosti
- ✓ ARCHITEKT kybernetické bezpečnosti dle ZoKB
- ✓ Přehledové testy zranitelností
- ✓ ISO IEC 27001, ISO IEC 62443, NIST CSF, NIS2
- ✓ Zabezpečení kritické infrastruktury

SLUŽBA DETEKCE KYBERNETICKÝCH UDÁLOSTÍ



**Jsme IT Security firma se
specializací na
kybernetické útoky.**

DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ RANSOMWARE útoky
- ✓ Forenzní vyšetřování kybernetických incidentů
- ✓ Krizové řízení
- ✓ AUDIT připravenosti na RANSOMWARE útok

SLUŽBY KYBERNETICKÉ BEZPEČNOSTI

- ✓ NASTARTOVÁNÍ kybernetické bezpečnosti
- ✓ ARCHITEKT kybernetické bezpečnosti dle ZoKB
- ✓ Přehledové testy zranitelností
- ✓ ISO IEC 27001, ISO IEC 62443, NIST CSF, NIS2
- ✓ Zabezpečení kritické infrastruktury

SLUŽBA DETEKCE KYBERNETICKÝCH UDÁLOSTÍ

- ✓ Proaktivní monitoring kybernetické bezpečnosti
- ✓ Dohled kritických assetů ve společnosti
- ✓ Visibilita co se děje

✓ Ochrana perimetru



Kybernetické útoky v roce 2025

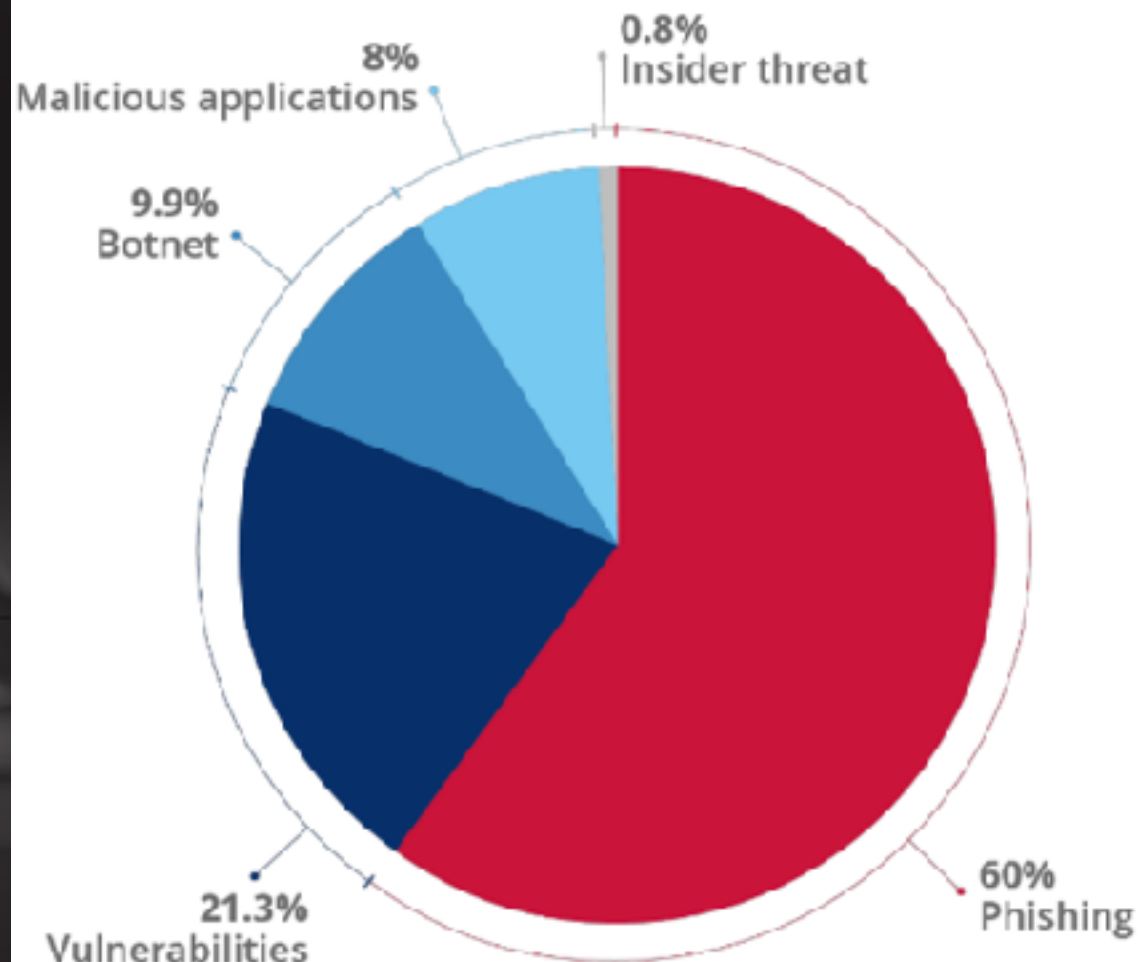
Kybernetické útoky v roce 2025?

Vektor útoku

Zdroj: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

Fig. 1 - Most identified initial infection vector.

Source: ENISA dataset



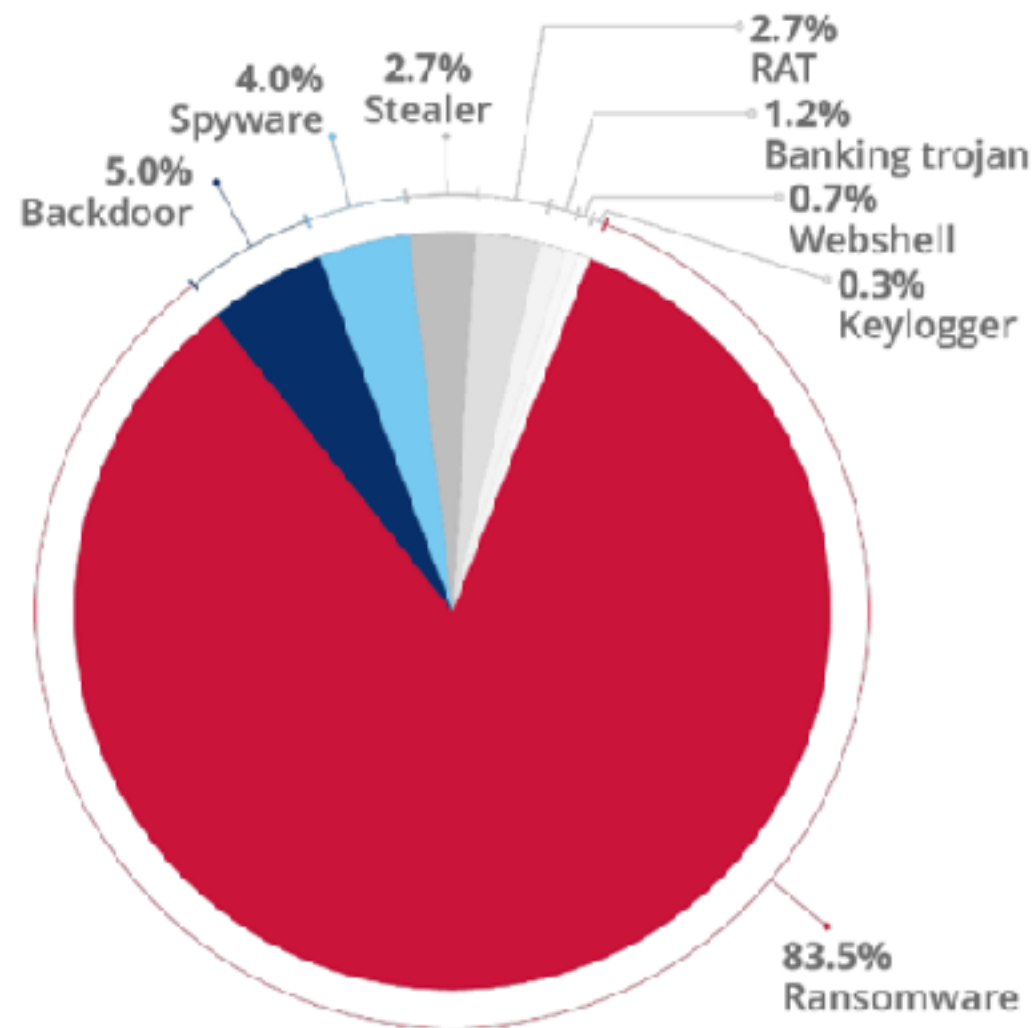
Kybernetické útoky v roce 2025?

Typy útoků

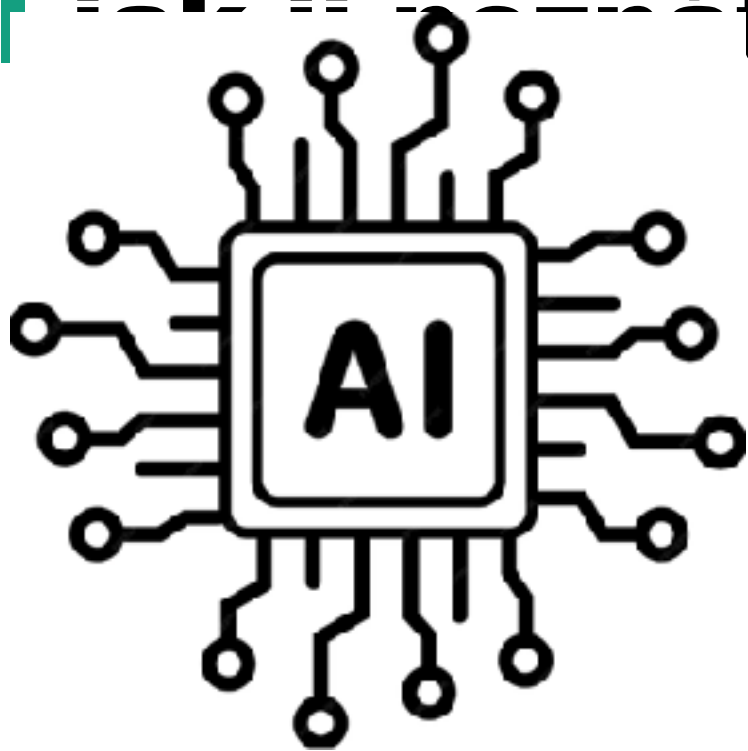
Zdroj: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

Fig. 3 - Distribution of identified malicious codes.

Source: ENISA dataset



AI ... te...



- ✓ Předvídatelný vývoj **AI** v kybernetických útocích
- ✓ **AI** jako nástroj k posílení a usnadnění aktivit útočníka
- ✓ více než 80% phishingových aktivit bylo generováno **AI**
- ✓ Zneužití komerčních LLM pro hacking = **WormGPT, EscapeGPT a FraudGPT,**
- ✓ **AI** automatizace aktivit sociálního inženýrství a vývoj škodlivého kódu
- ✓ **Přeškolené/odkloněné AI** používají na vlastní infrastrukturu pro nesnadné odhalení

Časová osa **RANSOMWARE** útoku ...



... ovládnutí sítě trvalo pouhých 88 minut !

Časová osa **RANSOMWARE** útoku



DNEŠ díky AI ještě rychleji !!

ovládnutí sítě trvalo pouhých **88 minut !**



Útočníci jsou rychlejší než kdykoliv dříve.



Útočníci jsou rychlejší než kdykoliv dříve.

Obrana musí být stejně adaptivní!



Obrana před kybernetickými útoky

Legislativa

Zákon č. 264/2025 Sb.

Zákon o kybernetické bezpečnosti

NIS2

§14

Zdroj: <https://www.e-sbirka.cz/sb/2025/264/0000-00-00?zalozka=text>

§ 14

Seznam bezpečnostních opatření

- (1) Pro poskytovatele regulované služby v režimu vyšších povinností jsou
- a) organizačními opatřeními
 - 1. systém řízení bezpečnosti informací,
 - 2. požadavky na vrcholné vedení,
 - 3. stanovení bezpečnostních rolí,
 - 4. řízení bezpečnostní politiky a bezpečnostní dokumentace,
 - 5. řízení aktiv,
 - 6. řízení rizik,
 - 7. řízení dodavatelů,
 - 8. bezpečnost lidských zdrojů,
 - 9. řízení změn,
 - 10. akvizice, vývoj a údržba,
 - 11. řízení přístupu,
 - 12. zvládání kybernetických bezpečnostních událostí a incidentů,
 - 13. řízení kontinuity činností a
 - 14. provádění auditu kybernetické bezpečnosti,
 - b) technickými opatřeními
 - 1. fyzická bezpečnost,
 - 2. bezpečnost komunikačních sítí,
 - 3. správa a ověřování identit,
 - 4. řízení přístupových práv a oprávnění,
 - 5. detekce kybernetických bezpečnostních událostí,
 - 6. zaznamenávání událostí,
 - 7. vyhodnocování kybernetických bezpečnostních událostí,
 - 8. aplikační bezpečnost,
 - 9. kryptografické algoritmy,
 - 10. zajišťování dostupnosti regulované služby a
 - 11. zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv.

Technická opatření (§ 14 odst. 1 pís. b)

- 1) **Fyzická bezpečnost** – zabezpečení zařízení a infrastruktury proti neoprávněnému přístupu a manipulaci.
- 2) **Bezpečnost komunikačních sítí** – opatření pro ochranu sítí před narušením, odposlechem a útoky.
- 3) **Správa a ověřování identit** – systémy pro autentizaci a autorizaci uživatelů/služeb.
- 4) **Řízení přístupových práv a oprávnění** – kontrola, kdo a jak může přistupovat k systémům a datům.
- 5) **Detekce kybernetických bezpečnostních událostí** – monitorování anomálií v síťovém či aplikačním provozu.
- 6) **Zaznamenávání událostí** – auditní logy a jejich bezpečné uchovávání pro vyšetřování a analýzu.
- 7) **Vyhodnocování kybernetických bezpečnostních událostí** – analýza zachycených událostí s cílem odhalit útoky a jejich dopady.
- 8) **Aplikační bezpečnost** – ochrana systémů a software před zranitelnostmi a útoky (např. testování, zabezpečený vývoj).
- 9) **Kryptografické algoritmy** – použití silných kryptografických mechanismů pro ochranu dat, identit a komunikace.
- 10) **Zajišťování dostupnosti regulované služby** – opatření pro odolnost a nepřetržité poskytování služeb (např. redundance, DDoS ochrana).
- 11) **Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv** – ochrana OT/ICS systémů, průmyslových řídicích systémů a podobných technických prostředí.

Technická opatření (§ 14 odst. 1 pís. b)

- 1) **Fyzická bezpečnost** – zabezpečení zařízení a infrastruktury proti neoprávněnému přístupu a manipulaci.
- 2) **Bezpečnost komunikačních sítí** – opatření pro ochranu sítí před narušením, odposlechem a útoky.
- 3) **Správa a ověřování identit** – systémy pro autentizaci a autorizaci uživatelů/služeb. **PAM**
- 4) **Řízení přístupových práv a oprávnění** – kontrola, kdo a jak může přistupovat k systémům a datům. **PAM**
- 5) **Detekce kybernetických bezpečnostních událostí** – monitorování anomálií v síťovém či aplikačním provozu. **SOC**
- 6) **Zaznamenávání událostí** – auditní logy a jejich bezpečné uchovávání pro vyšetřování a analýzu. **SOC**
- 7) **Vyhodnocování kybernetických bezpečnostních událostí** – analýza zachycených událostí s cílem odhalit útoky a jejich dopady. **SOC**
- 8) **Aplikační bezpečnost** – ochrana systémů a software před zranitelnostmi a útoky (např. testování, zabezpečený vývoj).
- 9) **Kryptografické algoritmy** – použití silných kryptografických mechanismů pro ochranu dat, identit a komunikace.
- 10) **Zajišťování dostupnosti regulované služby** – opatření pro odolnost a nepřetržité poskytování služeb (např. redundance, DDoS ochrana).
- 11) **Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv** – ochrana OT/ICS systémů, průmyslových řídicích systémů a podobných technických prostředí.

Technická opatření (§ 14 odst. 1 pís. b)

- 1) **Fyzická bezpečnost** – zabezpečení zařízení a infrastruktury proti neoprávněnému přístupu a manipulaci.
- 2) **Bezpečnost komunikačních sítí** – opatření pro ochranu sítí před narušením, odposlechem a útoky.
- 3) **Správa a ověřování identit** – systémy pro autentizaci a autorizaci uživatelů/služeb. **PAM**
- 4) **Řízení přístupových práv a oprávnění** – kontrola, kdo a jak může přistupovat k systémům a datům. **PAM**
- 5) **Detekce kybernetických bezpečnostních událostí** – monitorování anomálií v síťovém či aplikačním provozu. **SOC**
- 6) **Zaznamenávání událostí** – auditní logy a jejich bezpečné uchovávání pro vyšetřování a analýzu. **SOC**
- 7) **Vyhodnocování kybernetických bezpečnostních událostí** – analýza zachycených událostí s cílem odhalit útoky a jejich dopady. **SOC**
- 8) **Aplikační bezpečnost** – ochrana systémů a software před zranitelnostmi a útoky (např. testování, zabezpečený vývoj).
- 9) **Kryptografické algoritmy** – použití silných kryptografických mechanismů pro ochranu dat, identit a komunikace.
- 10) **Zajišťování dostupnosti regulované služby** – opatření pro odolnost a nepřetržité poskytování služeb (např. redundance, DDoS ochrana).
- 11) **Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv** – ochrana OT/ICS systémů, průmyslových řídicích systémů a podobných technických prostředí.



Zabezpečení privilegovaných účtů = PAM

Výzvy a cíle zabezpečení privilegovaných účtů

- ✓ **JASNÉ** **centrální řízení privilegovaných účtů**
- ✓ **OPRAVDOVÉ** **využití least privilege access** = minimální oprávnění
- ✓ **MAXIMÁLNÍ** **přehled o VŠECH aktivitách privilegovaných účtů** (video, metadata, logy)
- ✓ **VYNUCUJE** **restrikce pro připojení k systémům** (rotace hesel, délky hesel, peer server administrátor, just in time administrátor, dodavatelé)
- ✓ **JEDNA ZABEZPEČENÁ PLATFORMA** pro správu všech privilegovaných účtů napříč segmentem IT (AD, NETWORK, SQL, linuxy, managementy)
- ✓ **BENEFIT** **soulad s legislativou = NIS2**
- ✓ **BENEFIT NEZNÁME** **žádná hesla a bezpečnost**



Co jsme udělali ...

Co jsme udělali

- ✓ Vzali jsme jednu z TOP PAM na světě
- ✓ ODDĚLILI od infrastruktury !
- ✓ MAXIMÁLNĚ zahardenovali
- ✓ VŠE ENTERPRISTE (HW, HA, OS, support)
- ✓ ZAINTEGROVALI **service desk** a **Log management**
- ✓ Dodali naše Know-how z reálných útoků
- ✓ VŠE zautomatizovali
- ✓ To VŠE do HW appliance PAM

Výsledek je HW APPLIANCE

- ✓ JEDINÉ rozhraní jak se přihlásit privilegovaně do systémů, managementů atd.
- ✓ Úzká Integrace s JUMP servery
- ✓ Jednoduše vyřešeny požadavky dodavatelů a na privilegovaný přístup
- ✓ Napojeno do vlastního SOCu, víme o všem VČAS
- ✓ Analytické nástroje a reporting
- ✓ Dodali naše Know-how z reálných útoků
- ✓ To VŠE do HW appliance PAM
- ✓ NO CLOUD pouze onpremise



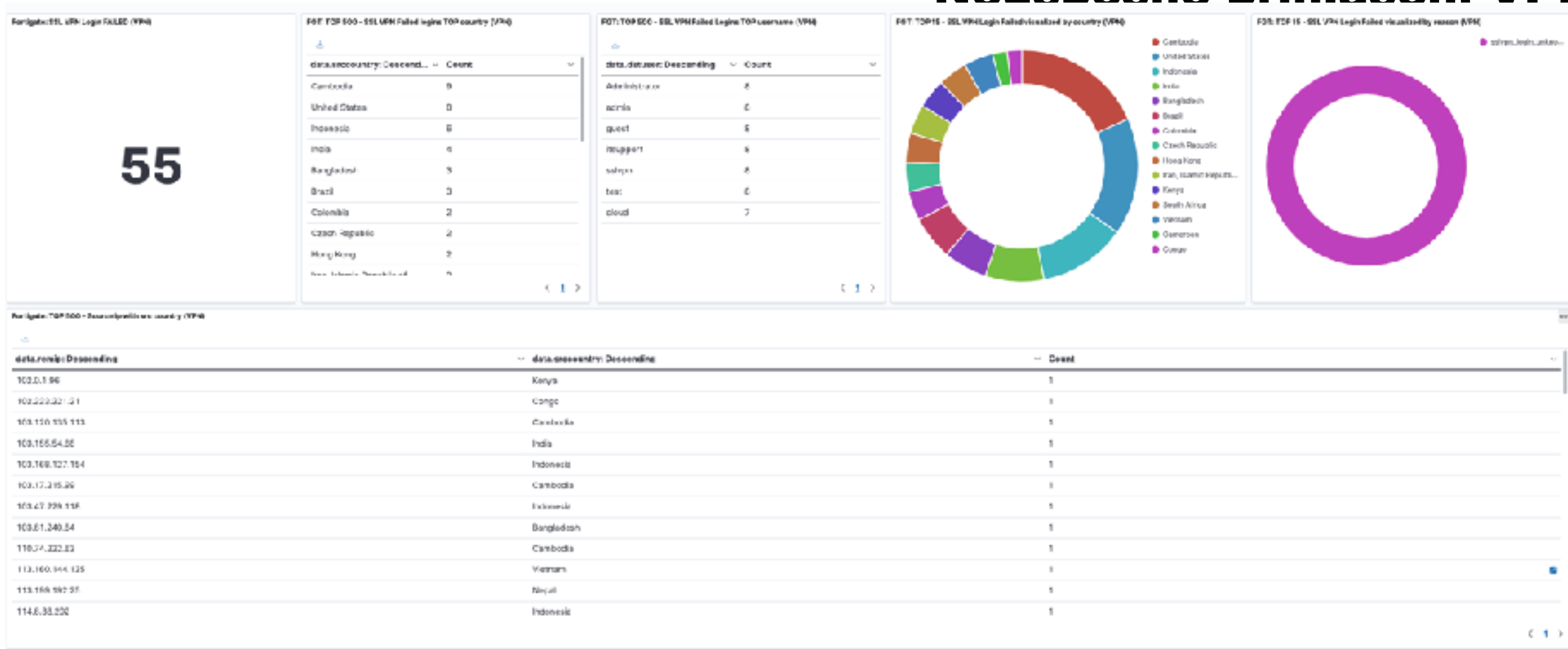
Proaktivní monitoring kybernetické bezpečnosti = SOC

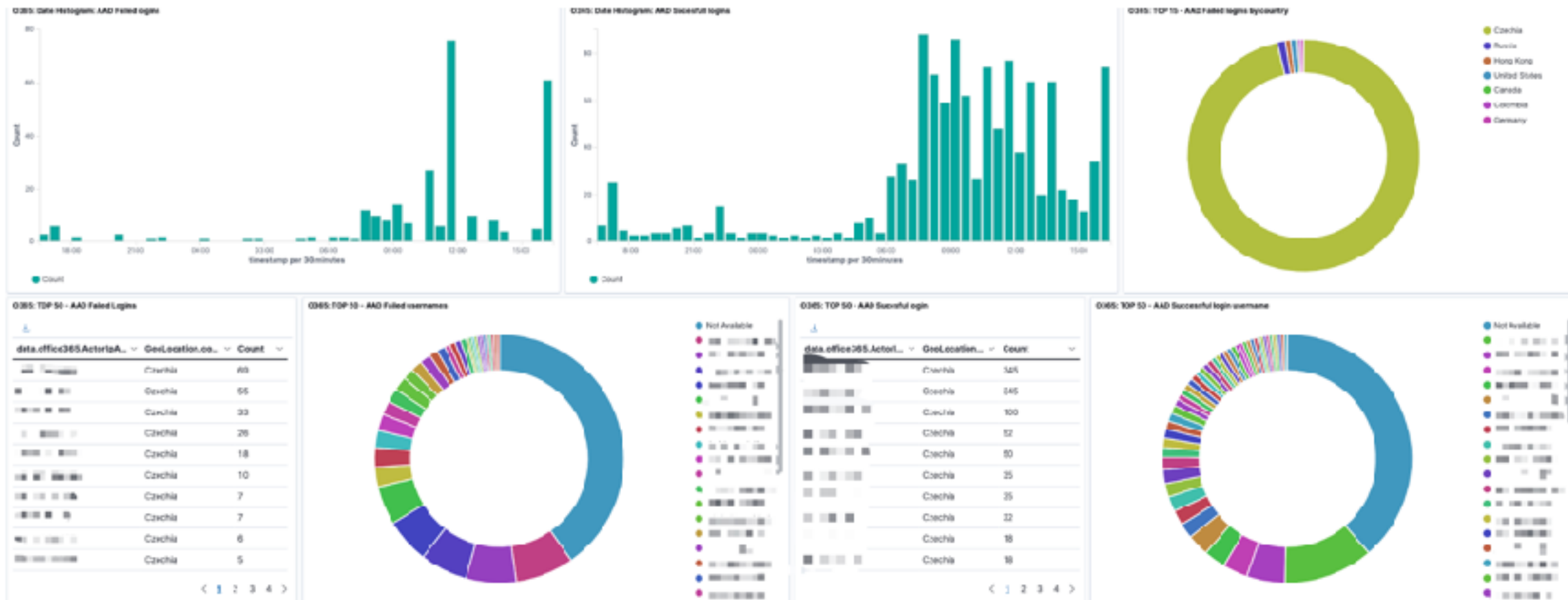
Proaktivní monitoring SOC

- ✓ **24x7 monitoring** kritických systémů
- ✓ **Security monitoring**
 - ✓ **Záloh**
 - ✓ AD,FW ,VPN, EDR, DLP
 - ✓ Cloudy
 - ✓ Privilegovaných účtů
 - ✓ **Honeypoty na síti**
- ✓ Detekování útoků v ranné fázi
- ✓ Rychlá reakce na incidenty

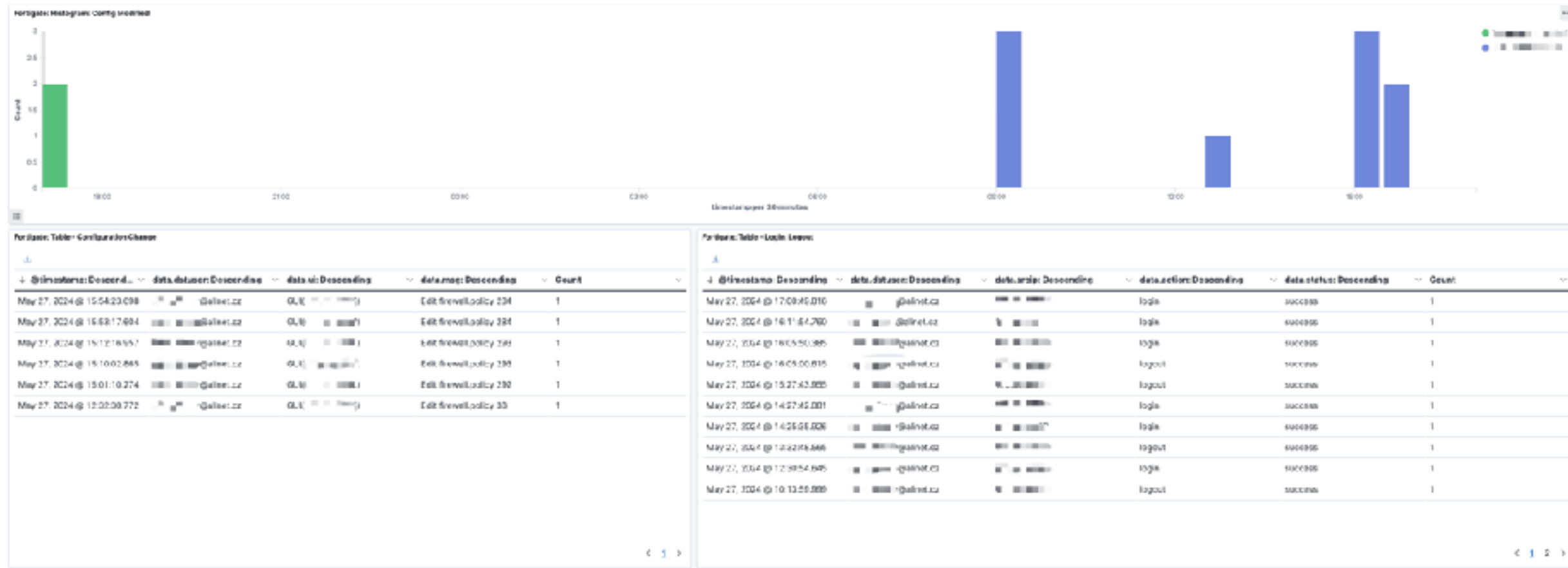
Proaktivní n SOC



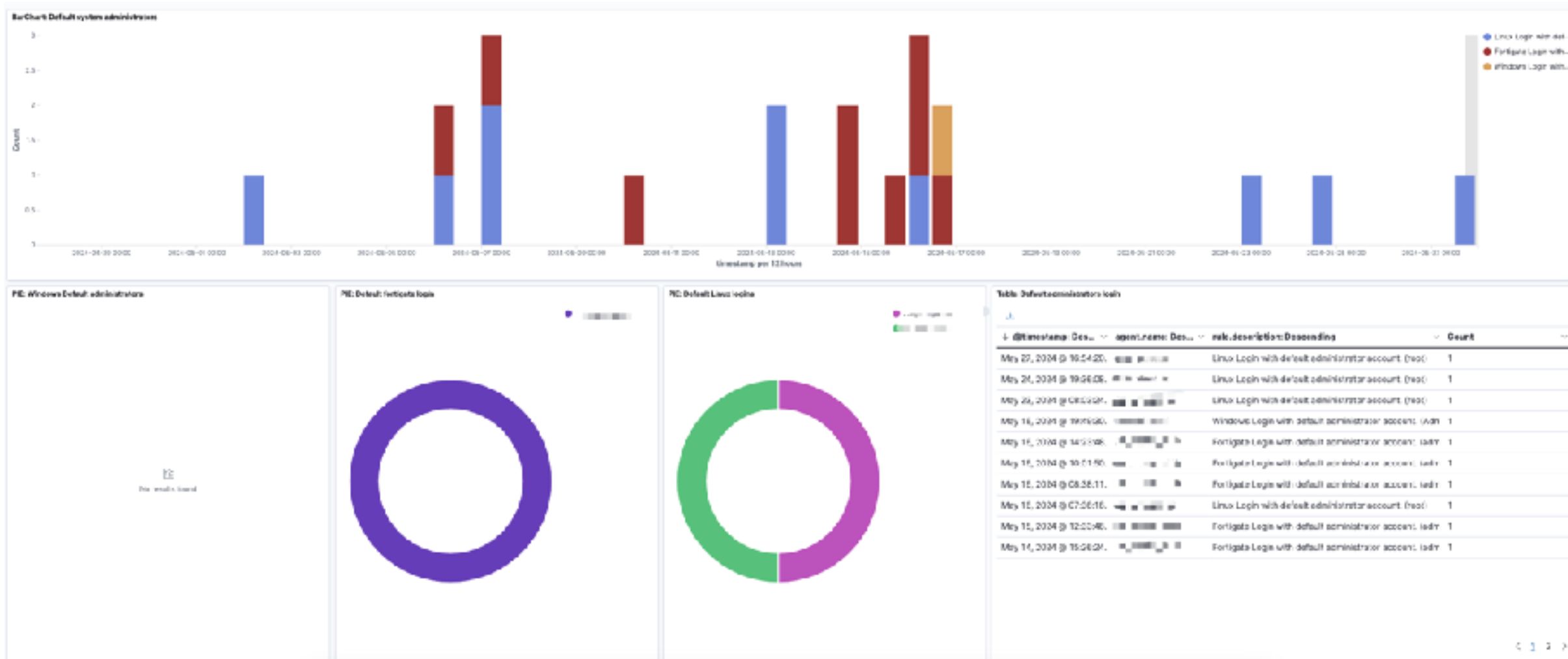


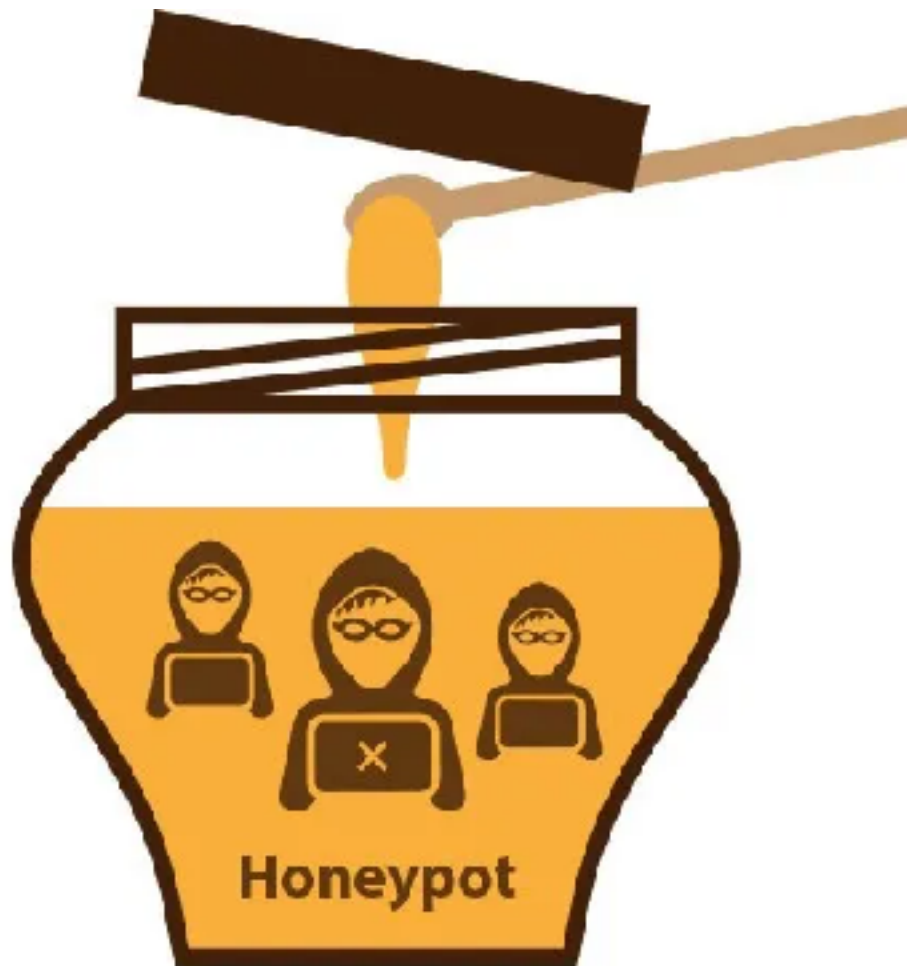


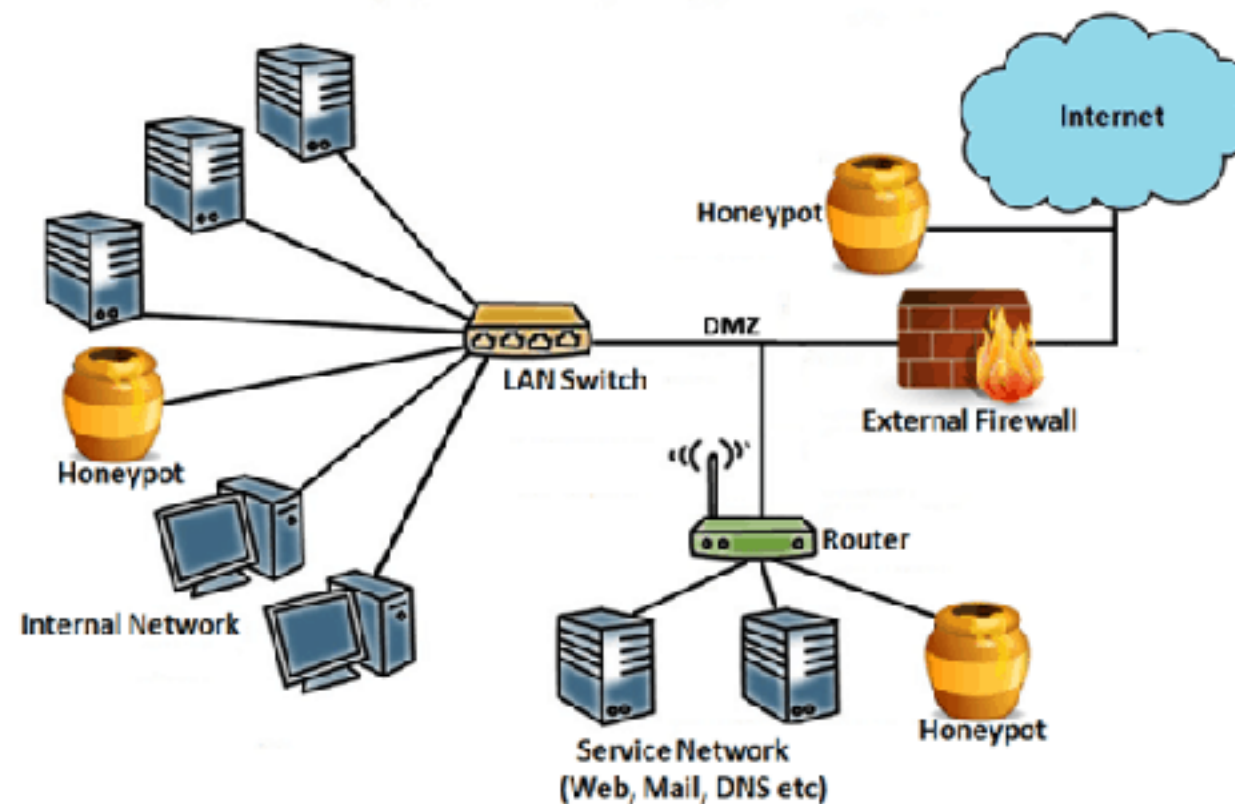
Proaktivní monitoring – Monitoring změn FW



Proaktivní monitoring – Defaultní administrátoři









Jak by to mělo dnes vypadat?



Administrátor
nebo dodavatel



Administrátor
nebo dodavatel



PAM appliance

- ✓ MFA ověření
- ✓ Přiřazená role
- ✓ Minimálního oprávnění
- ✓ ZTNA



Administrátor
nebo dodavatel

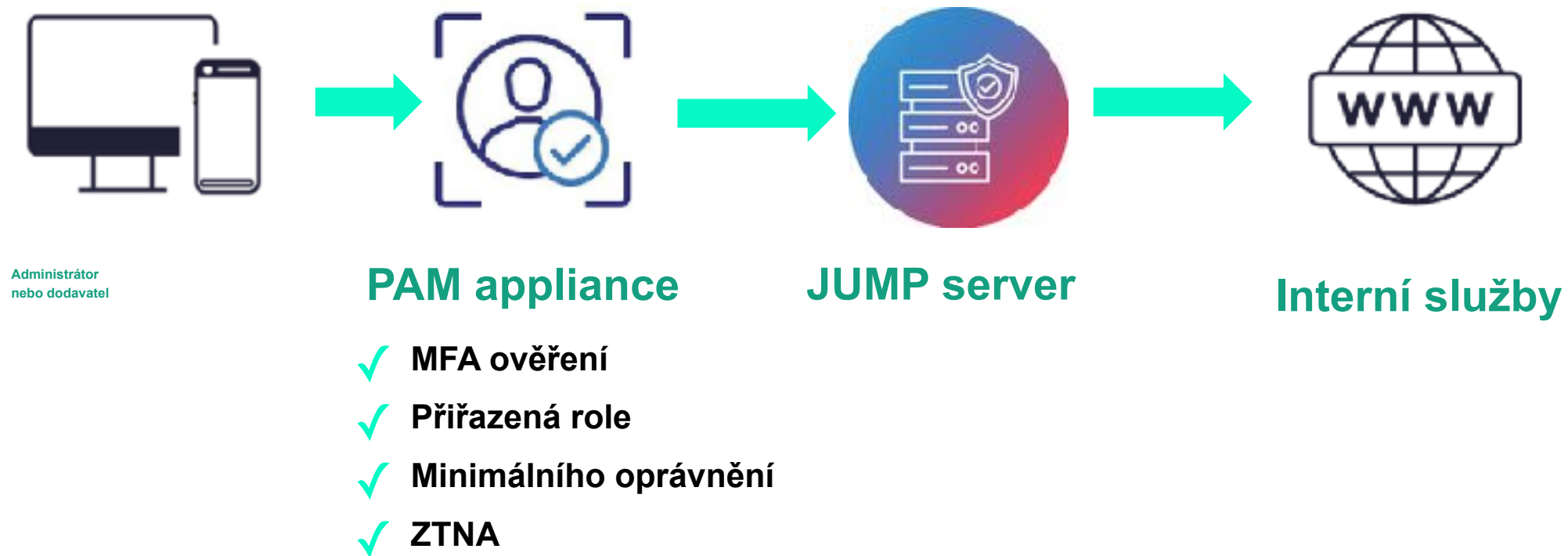


PAM appliance



JUMP server

- ✓ MFA ověření
- ✓ Přiřazená role
- ✓ Minimálního oprávnění
- ✓ ZTNA





SOC



Administrátor
nebo dodavatel



PAM appliance



JUMP server



Interní služby

- ✓ MFA ověření
- ✓ Přiřazená role
- ✓ Minimálního oprávnění
- ✓ ZTNA


ManageEngine
PAM360




Dashboard
 
Resources
 
Groups
 
Connections

Cloud Environments

SSH Keys

Certificates

Users

Admin

Audit

Remote Connections

- All My Connections
- Owned and Managed
- Favorites
- Recently Accessed
- Web App Connections
- HTTPS Gateway Connections
- Secure File Transfer
- Folders
- Resource Groups
 - Applikace
 - Domenove kontrolery
 - MySQL Server
- Default Groups
 - mvaclavik's Default Group

Resources

Name ▾

	APP01 172.30.244.253
	DC01 172.30.244.252
	Linux 172.30.244.254

Accounts

Domain Accounts
Local Accounts

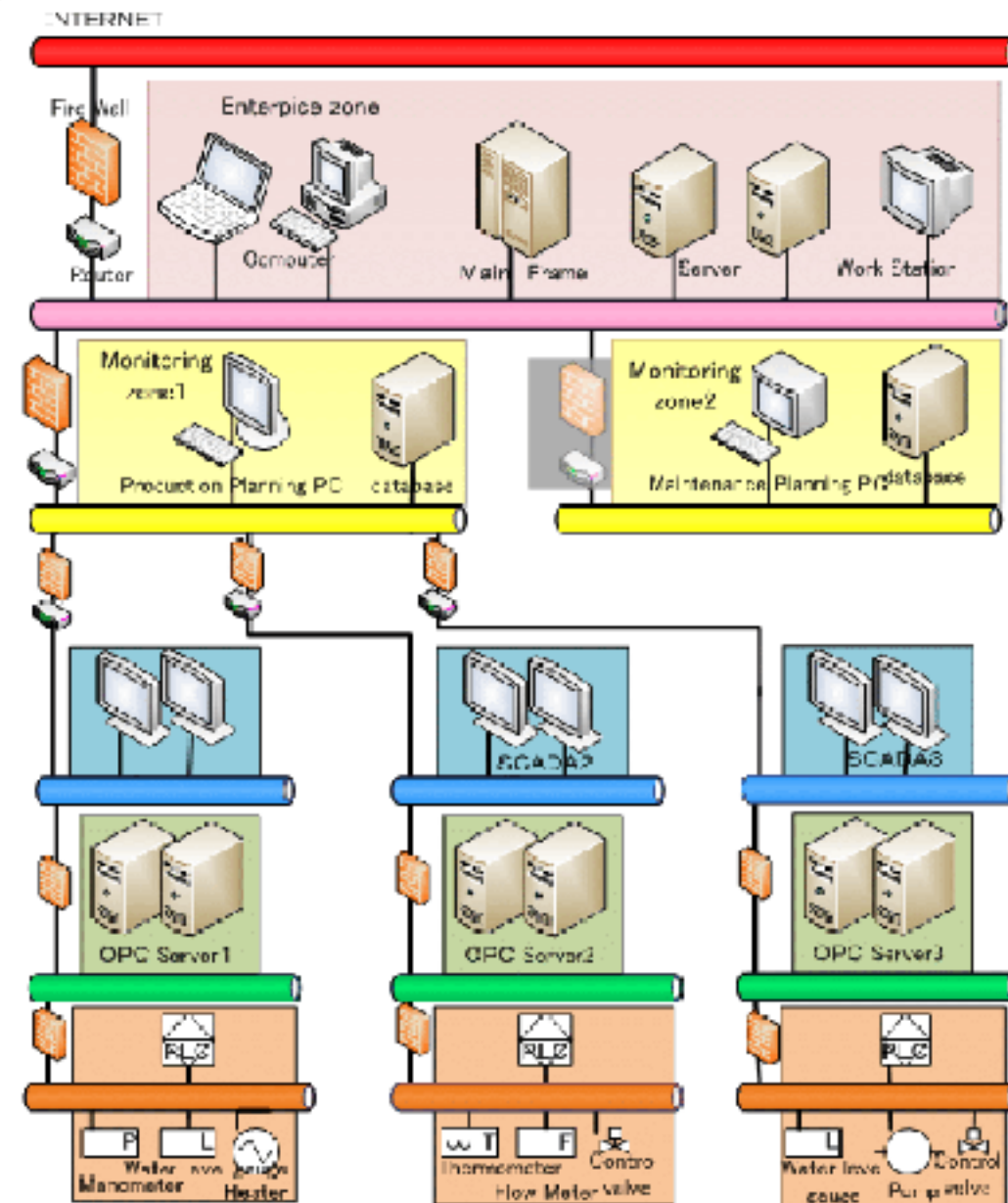
DC01


Administrator


Facing problems in launching remote connection

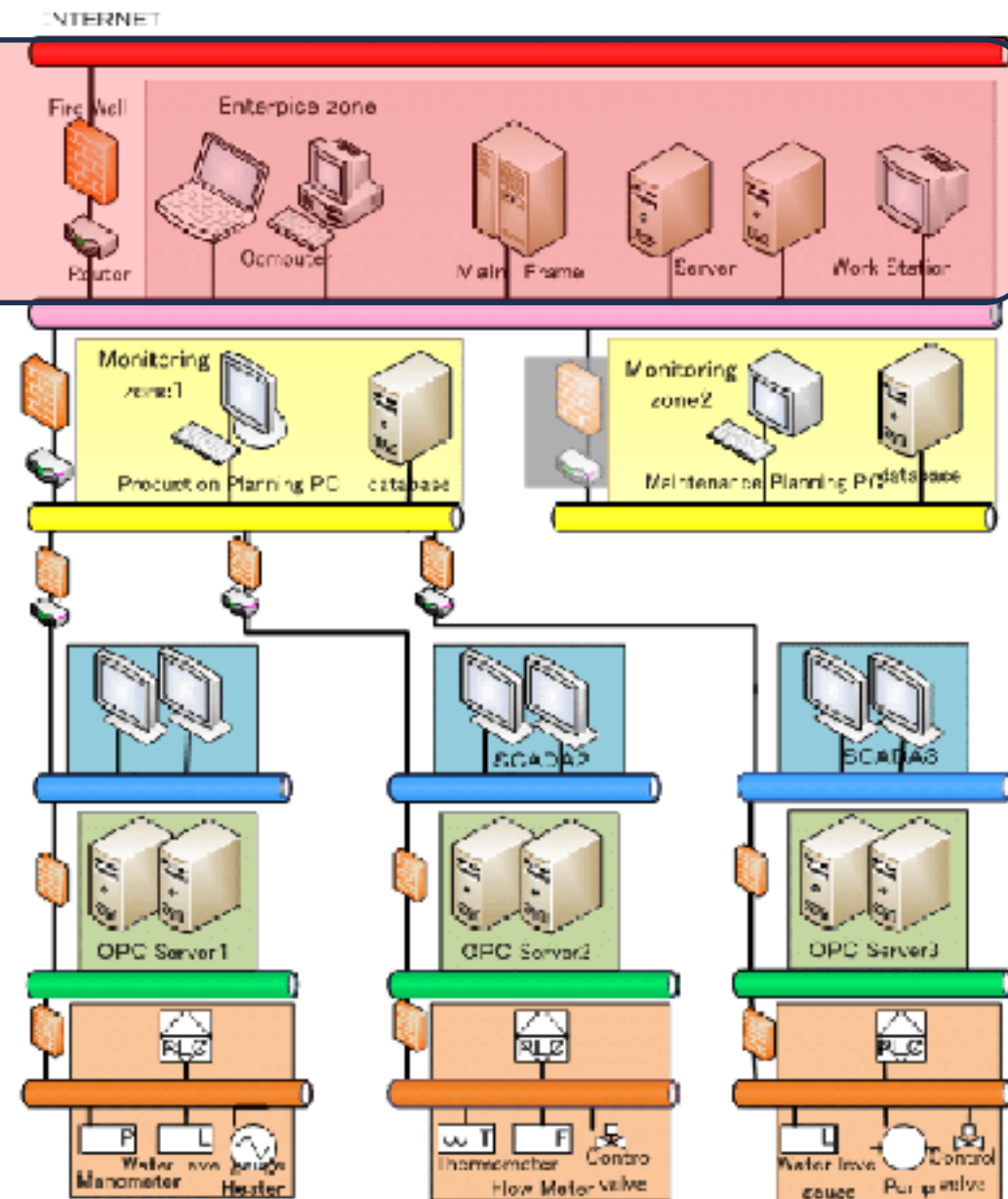


Jak zabezpečit IoT OT systémy?



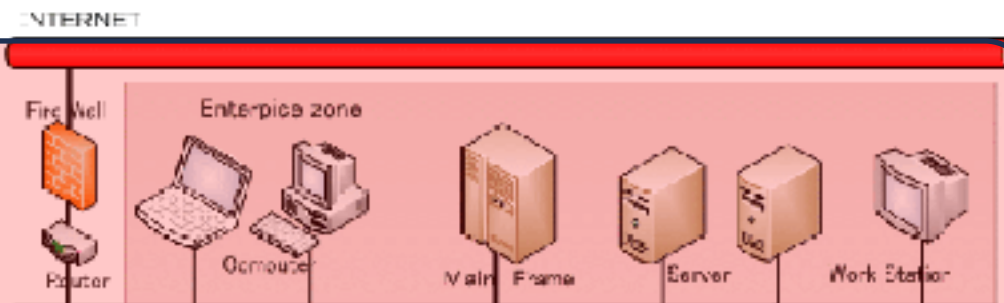
Level 4

■ ENTERPRISE ZONE



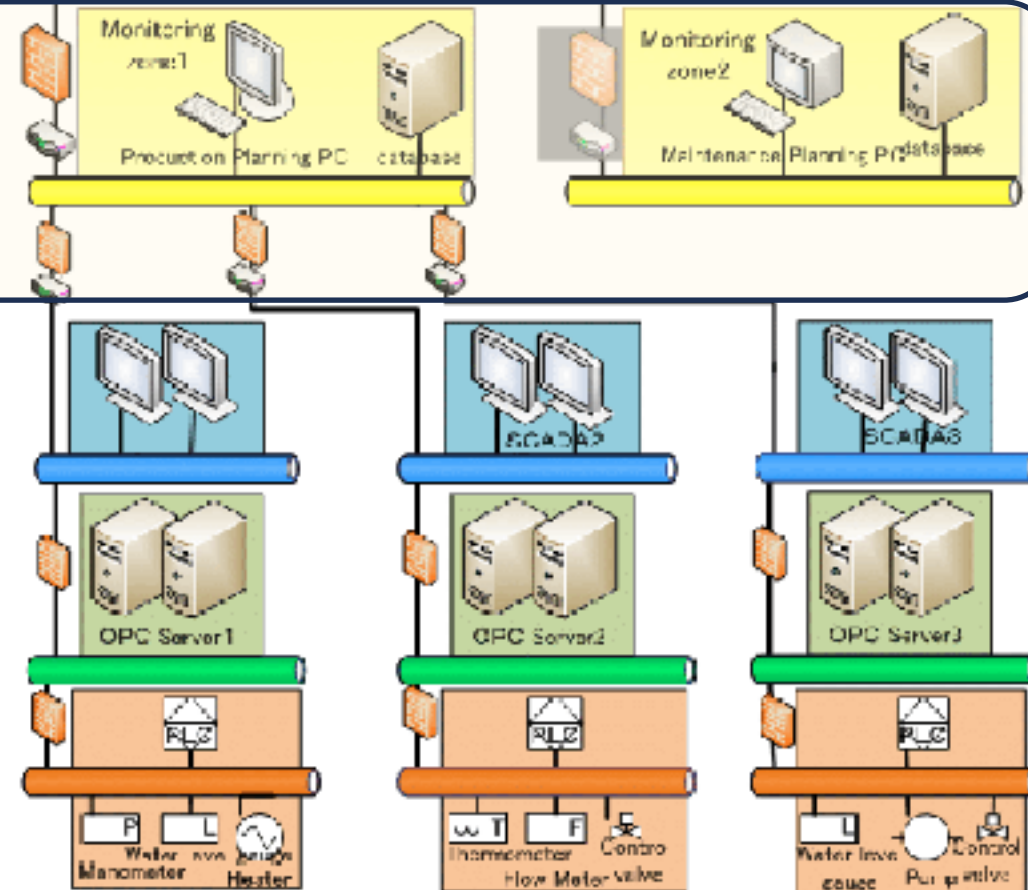
Level 4

■ ENTERPRISE ZONE



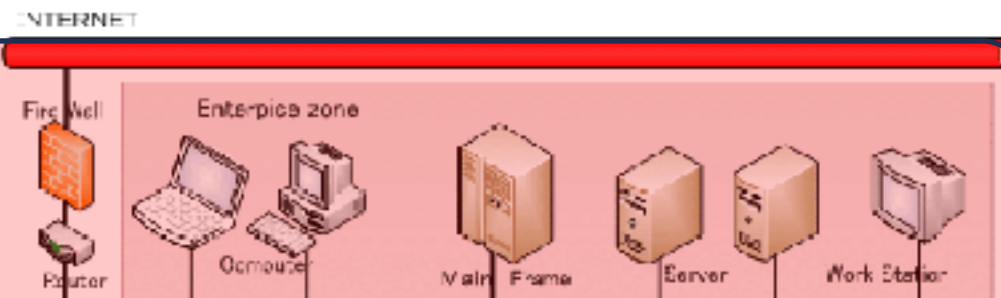
DMZ

■ DMZ ZONE



Level 4

■ ENTERPRISE ZONE



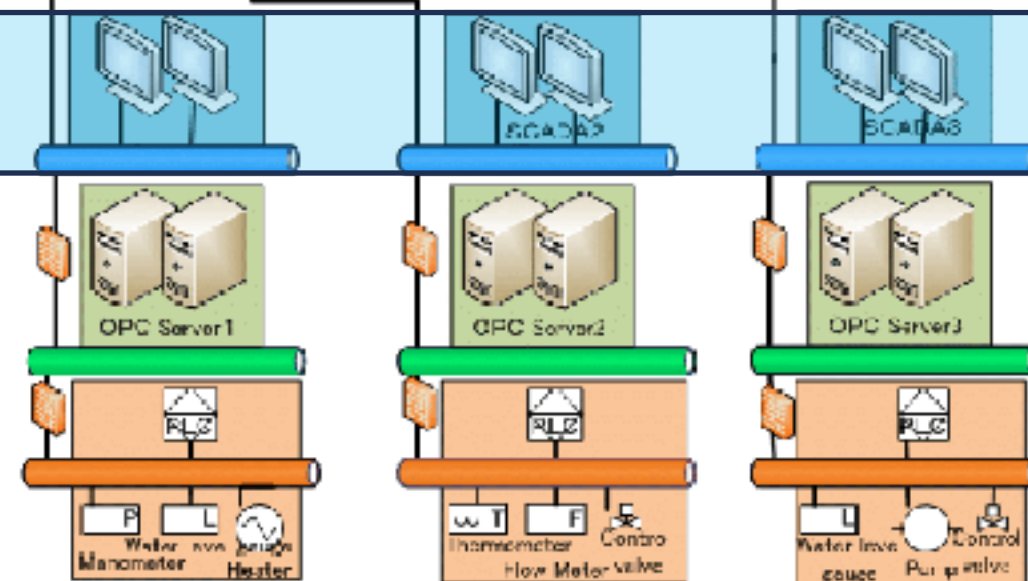
DMZ

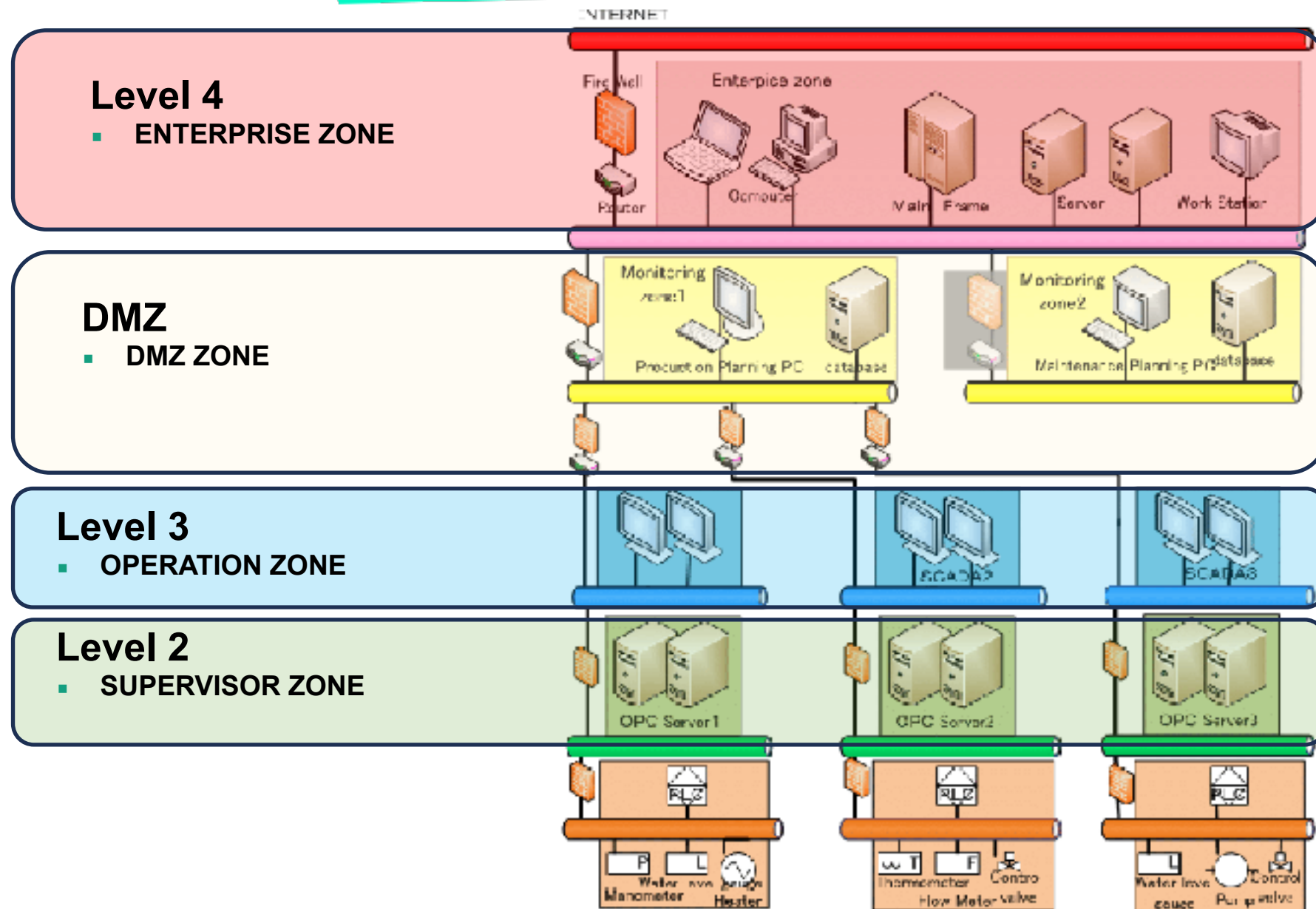
■ DMZ ZONE

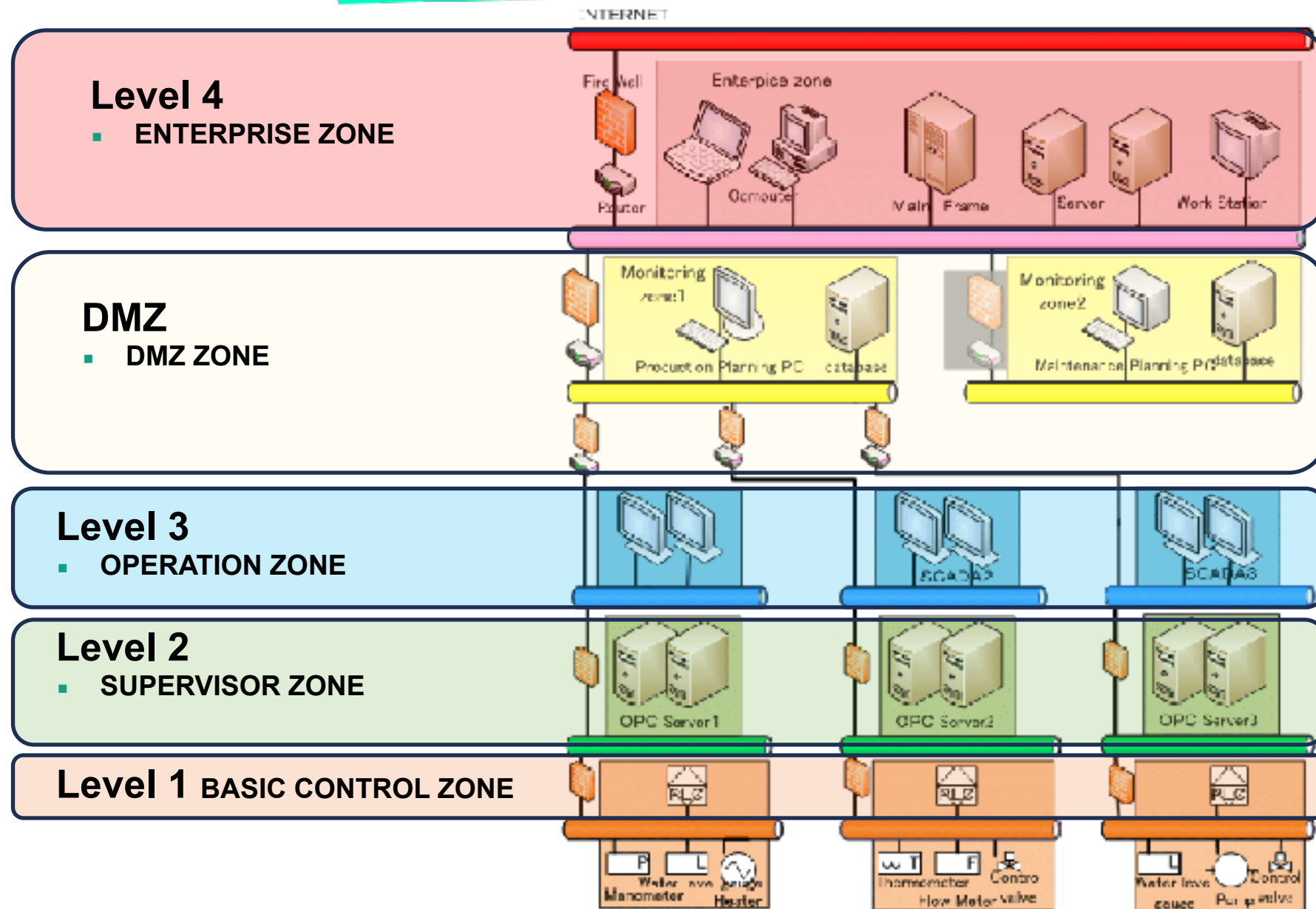


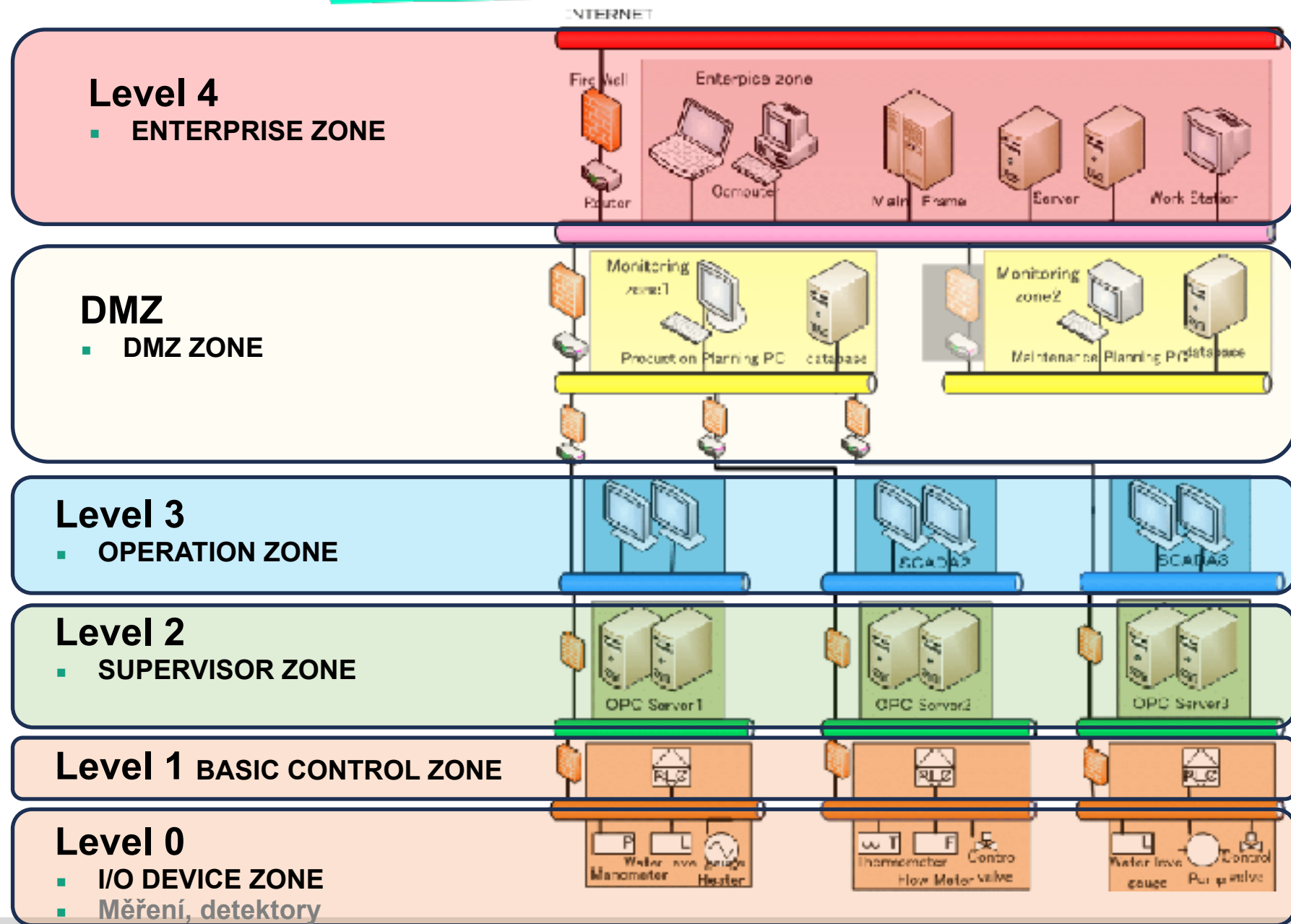
Level 3

■ OPERATION ZONE





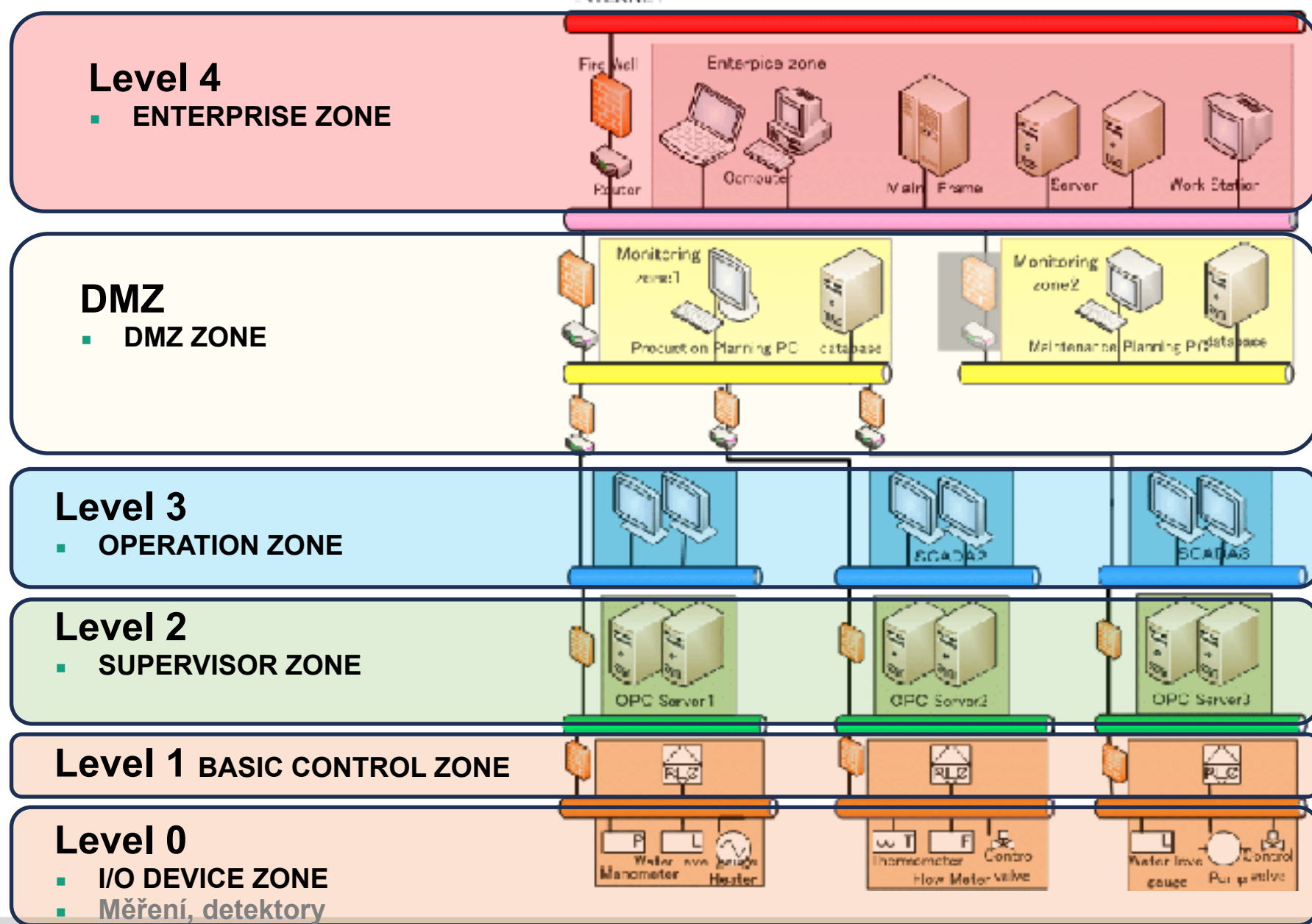




IT ZONE

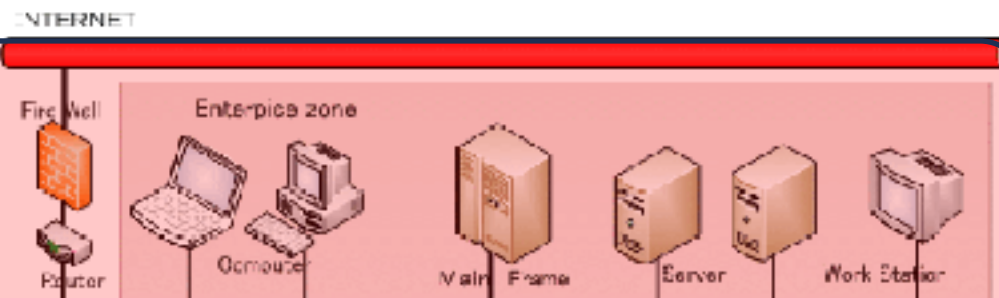
DMZ ZONE

CONTROL ZONE



IT ZONE

Level 4 ■ ENTERPRISE ZONE



DMZ ZONE

DMZ ■ DMZ ZONE



Wide Area
Network

CONTROL ZONE

Level 3 ■ OPERATION ZONE



Level 2 ■ SUPERVISOR ZONE



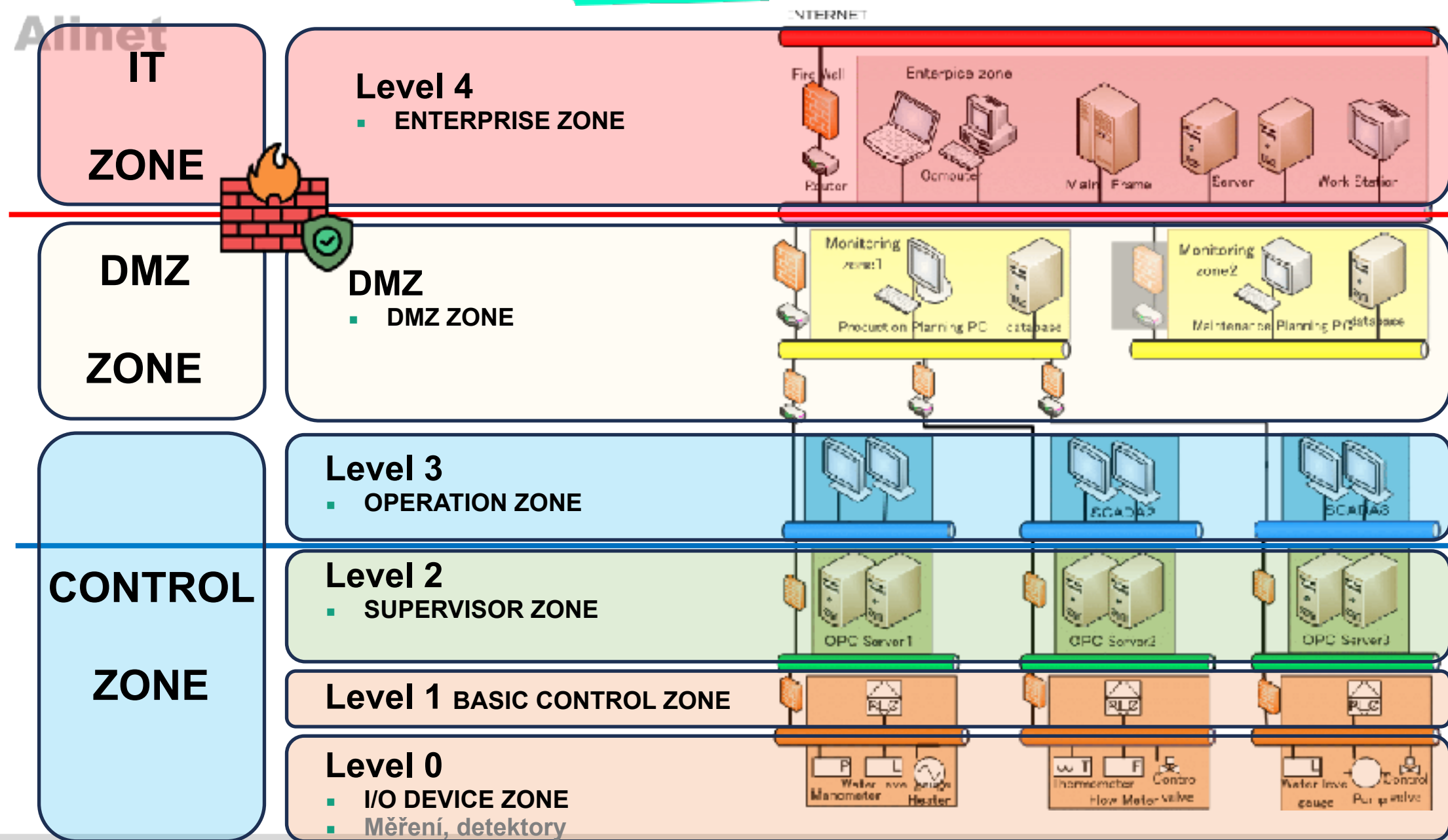
Level 1 BASIC CONTROL ZONE



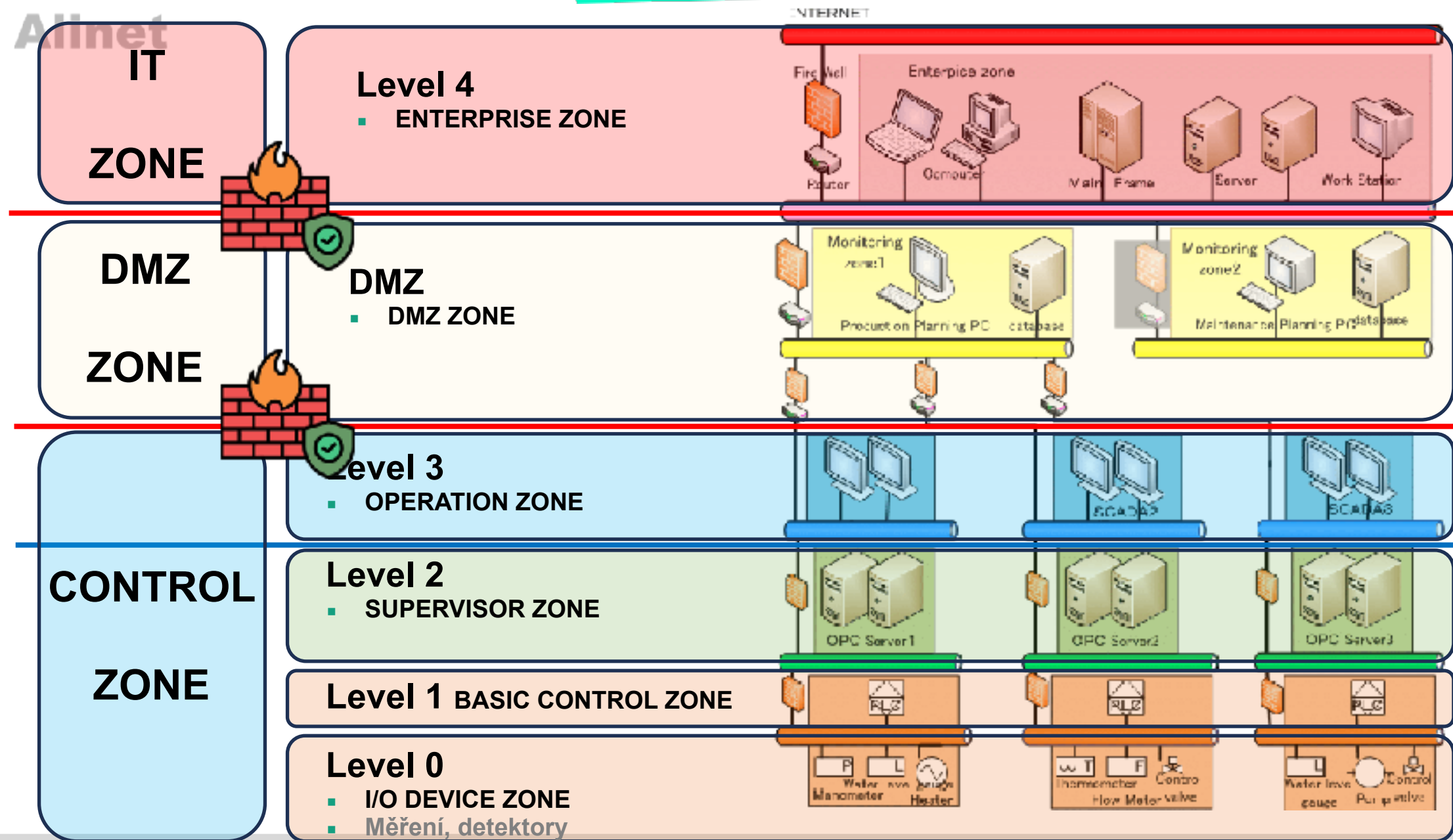
Level 0 ■ I/O DEVICE ZONE ■ Měření, detektory



Wide Area
Network



Wide Area
Network





Jak začít ?

Jak začít ?

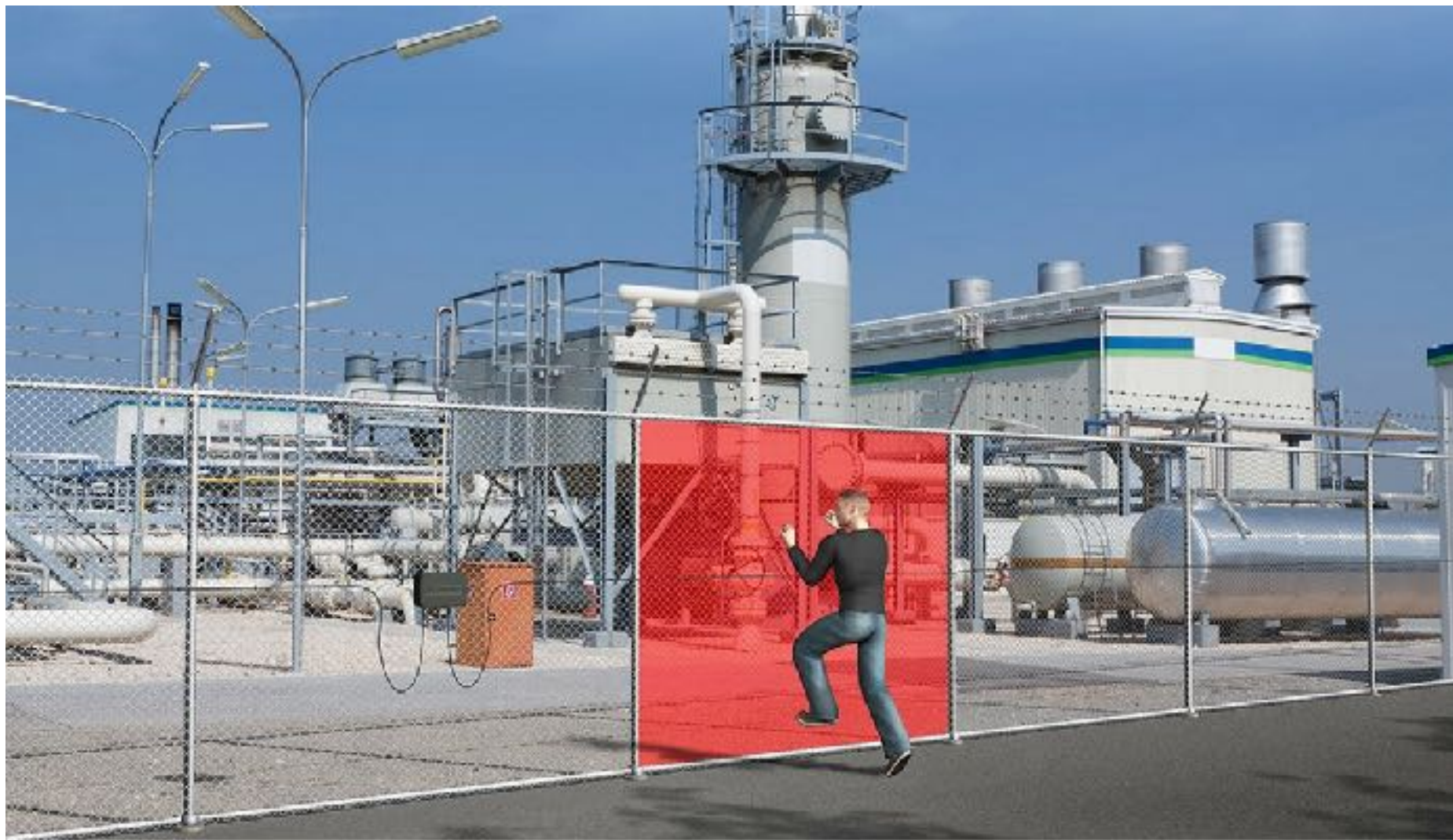
- ✓ **Identifikovat a klasifikovat** OT zařízení, díky které máte dostatečnou visibilitu
- ✓ **MIKROSEGMENTACE** sítě a síťových ZÓN
- ✓ **Začlenit OT systémy** do bezpečnostních operací a reakcí na bezpečnostní incidenty (SOC, DR a IR plány)
- ✓ Správně navržená **architektura OT**
- ✓ NEbýt REAKTIVNÍ ale **PROAKTIVNÍ**
- ✓ Ochrana zranitelností na perimetru **VŠECH** internetů
- ✓ **Přehledové testy zranitelností**/penetrační testy
- ✓ **Zálohy** konfigurací!



Jak **opravdu** začít ?



Ochrana perimetru





Potřebujete konzultaci ?
Otázky ?



Potřebujete ...

PAM,

SOC,

Konzultace kyberbezpečnosti

Zabezpečit OT systémy

Architekta kybernetické bezpečnosti

**Vyžádejte si s námi
schůzku již NYNÍ**

- ✓ Do chatu
- ✓ Napište klíčové slovo **ALINET**
spojíme se s Vámi
- ✓ Provedeme **SCAN PERIMETRU
ZDARMA**
- ✓ Zkonzultujeme Vaše potřeby



Alinet

Cyber Security, **Ransomware Incident Response**



Jakub Alimov

www.alinet.cz jakub.alimov@alinet.cz +420 774 077 108