Alinet

Ochrana proti kybernetickým útokům, bezpečnost IoT a OT systémů

21.1.2026

Alinet CZ s.r.o. **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Kdo jsem?

Alinet

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/

Alinet

Kdo je Alinet?

Alinet

DIGITAL FORENSICS AND INCIDENT RESPONSE

Jsme IT Security firma se specializací na kybernetické útoky.

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Kybernetické útoky v roce 2025

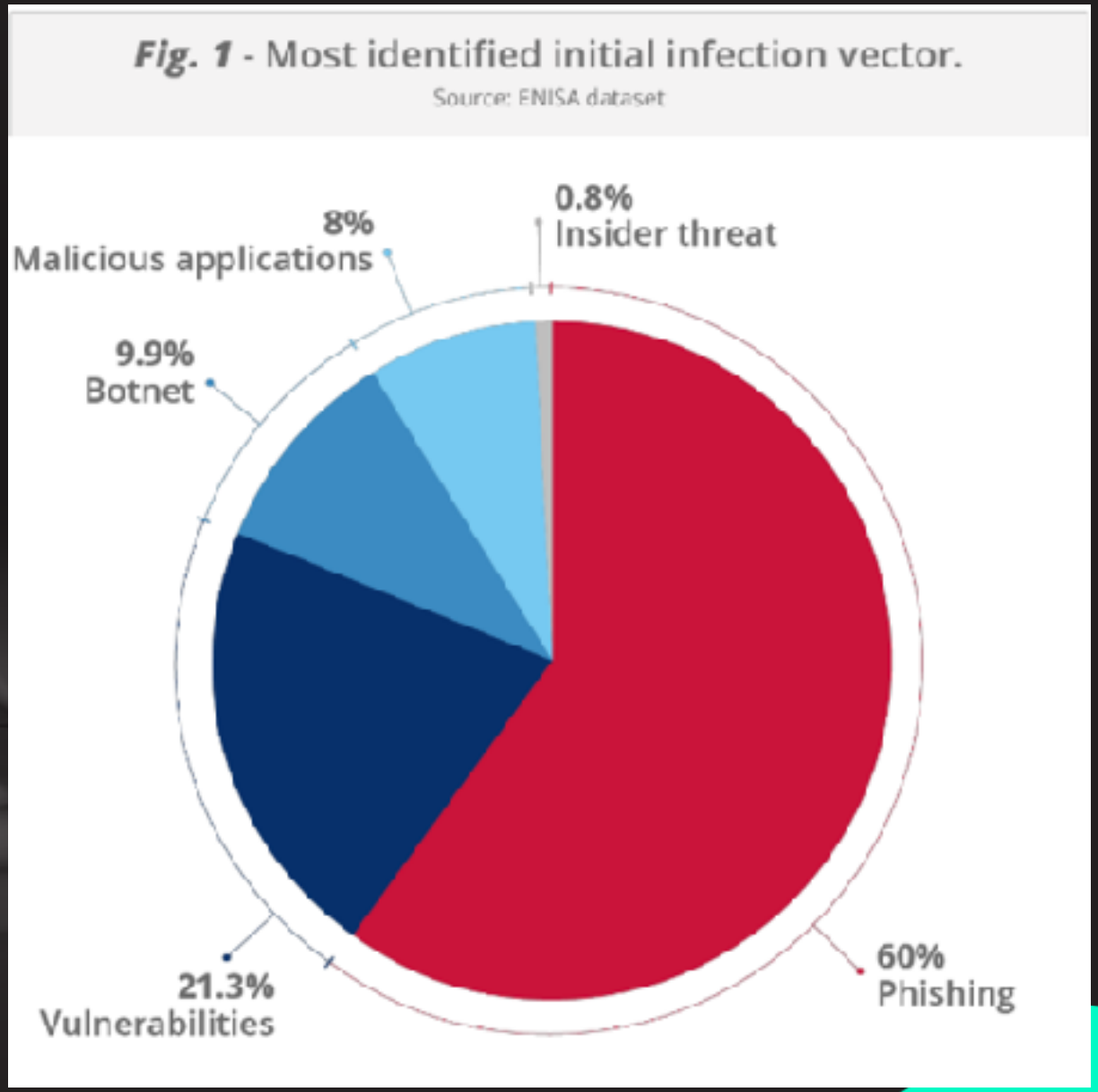
Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Kybernetické útoky v roce 2025?

Vektor útoku

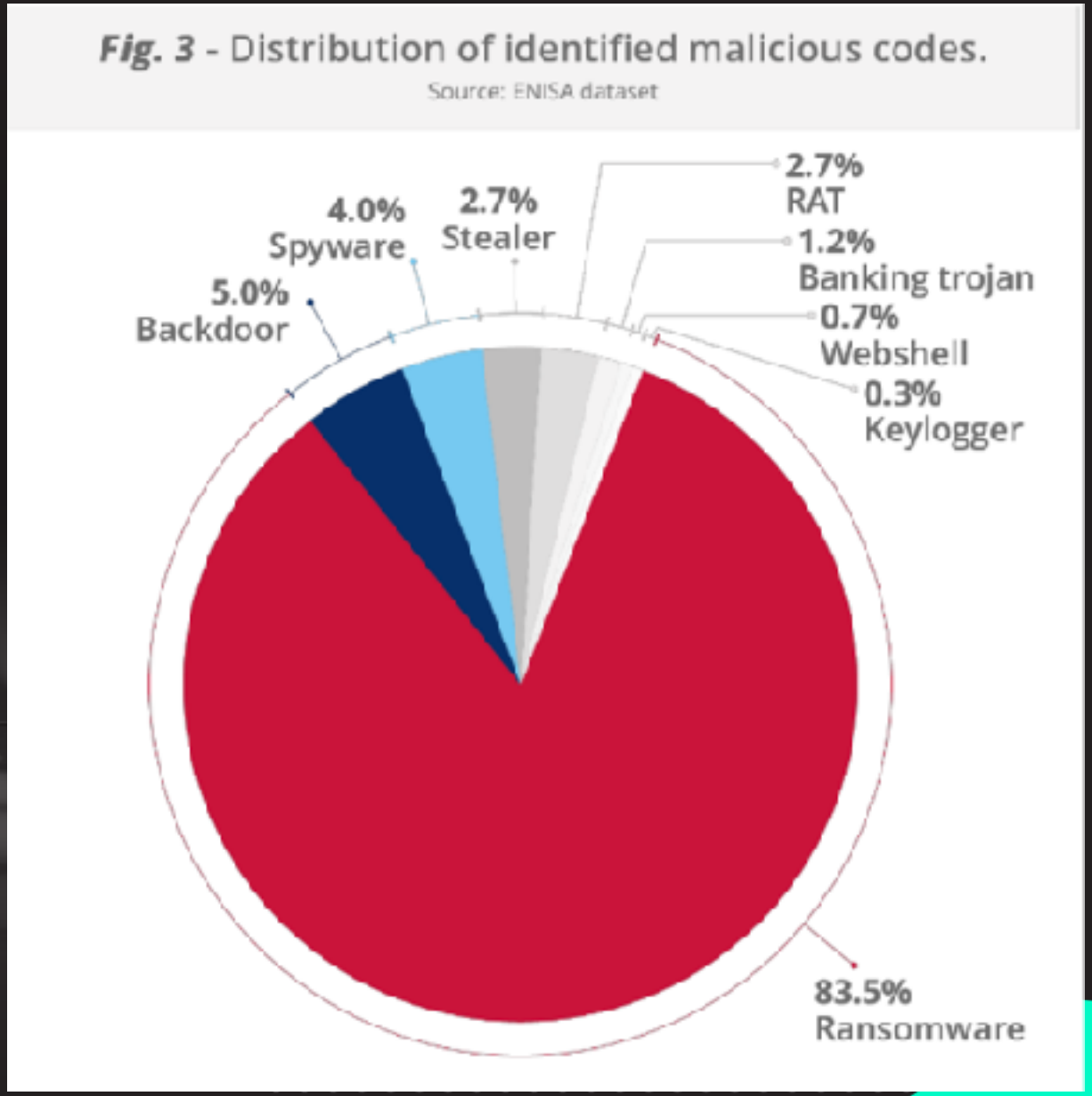


Zdroj: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

Alinet

Kybernetické útoky v roce 2025?

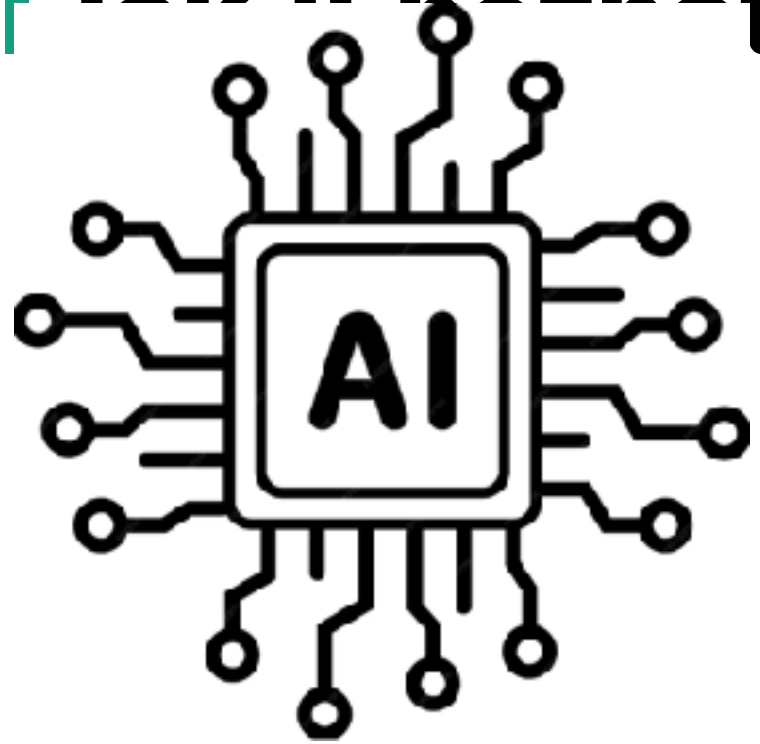
Typy útoků



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

Alinet

AI jak ji nepoznáte...



- ✓ Předvídatelný vývoj AI v kybernetických útocích
- ✓ AI jako nástroj k posílení a usnadnění aktivit útočníka
- ✓ více něž 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 infrastruktuře pro nesnadné odhalení

Alinet

Časová osa RANSOMWARE útoku ...

... ovládnutí sítě trvalo pouhých 88 minut !

Alinet

Časová osa RANSOMWARE útoku...

3:36
prvotní kontakt útočníka

3:54
enumerace administrátorů na DMZ serveru

4:10
reverzní she

4:25
vytvoření lokálního administrátorského účtu

5:04
eskalace oprávnění na **doménového administrátora**

9:52
Distribuce GPO šifrovací úlohy = **zašifrování server a stanic**

DNES díky AI ještě rychleji !!

...ovládnutí sítě trvalo pouhých 88 minut !

Alinet

Útočníci jsou rychlejší než kdykoliv dřív.

Alinet

Útočníci jsou rychlejší než kdykoliv dřív.

Obrana musí být stejně adaptivní!

Alinet

Obrana před kybernetickými útoky

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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.

Alinet

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, řídících a obdobných specifických technických aktiv** – ochrana OT/ICS systémů, průmyslových řídicích systémů a podobných technických prostředí.

Alinet

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, řídících a obdobných specifických technických aktiv** – ochrana OT/ICS systémů, průmyslových řídicích systémů a podobných technických prostředí.

Alinet

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, řídících a obdobných specifických technických aktiv** – ochrana OT/ICS systémů, průmyslových řídicích systémů a podobných technických prostředí.

Alinet

Zabezpečení privilegovaných účtů = PAM

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ
mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

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**

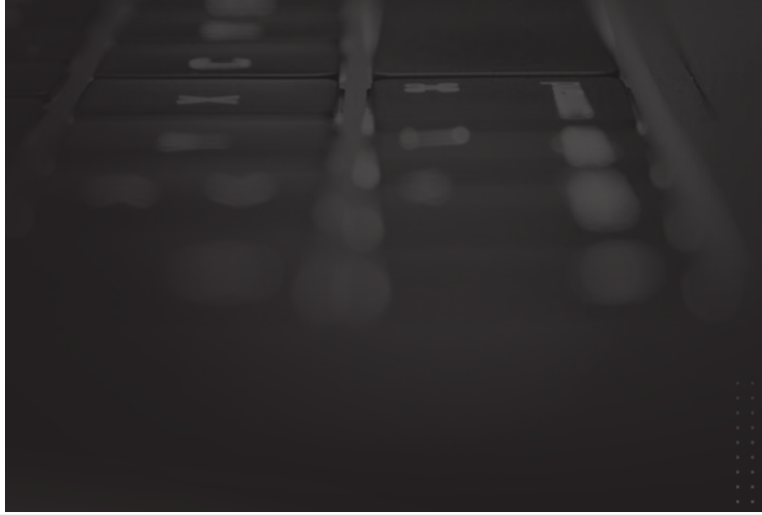
Alinet

Co jsme udělali …

Alinet

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**

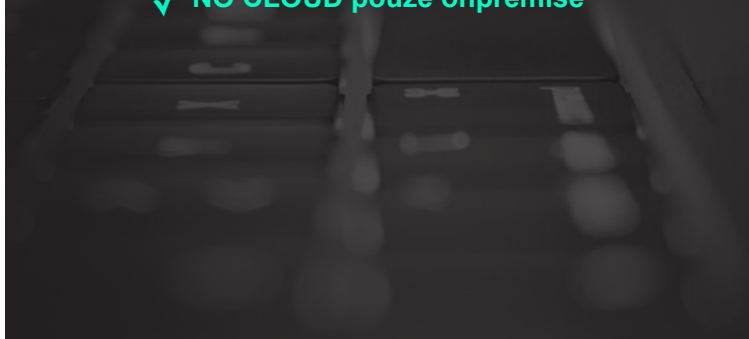


Alinet

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



Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Proaktivní monitoring kybernetické bezpečnosti = SOC

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Proaktivní monitoring

SOC

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

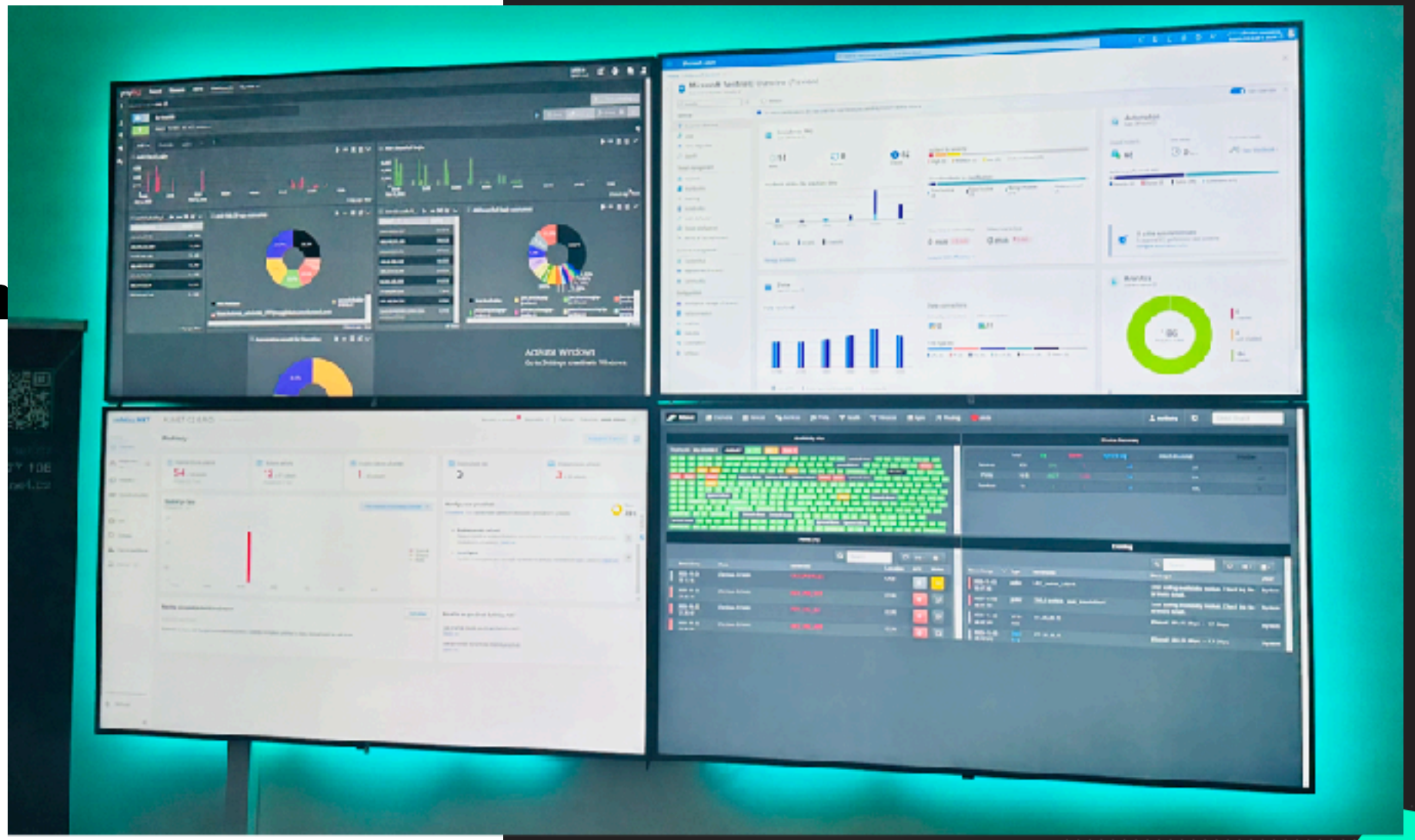
Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

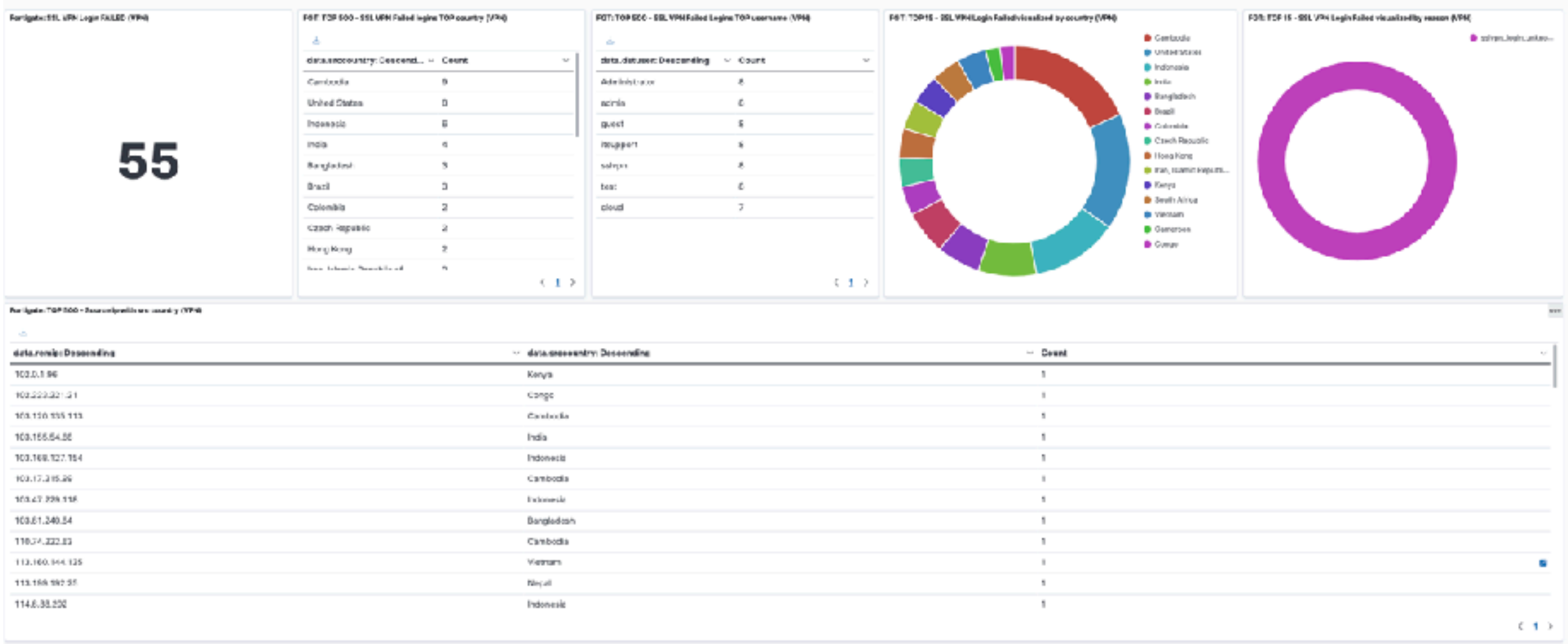
Proaktivní m

SOC



Proaktivní monitoring –

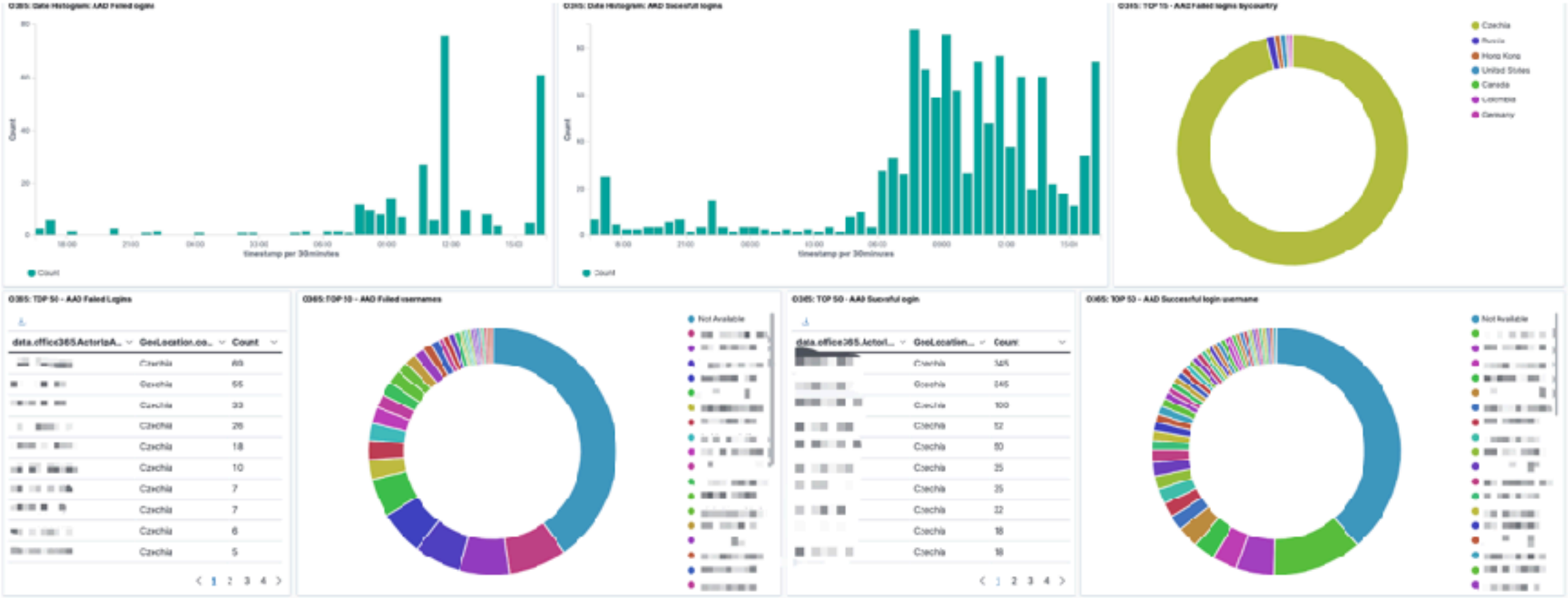
Neúspěšné přihlášení VPN



Alinet

Proaktivní monitoring –

AAD neúspěšné přihlášení

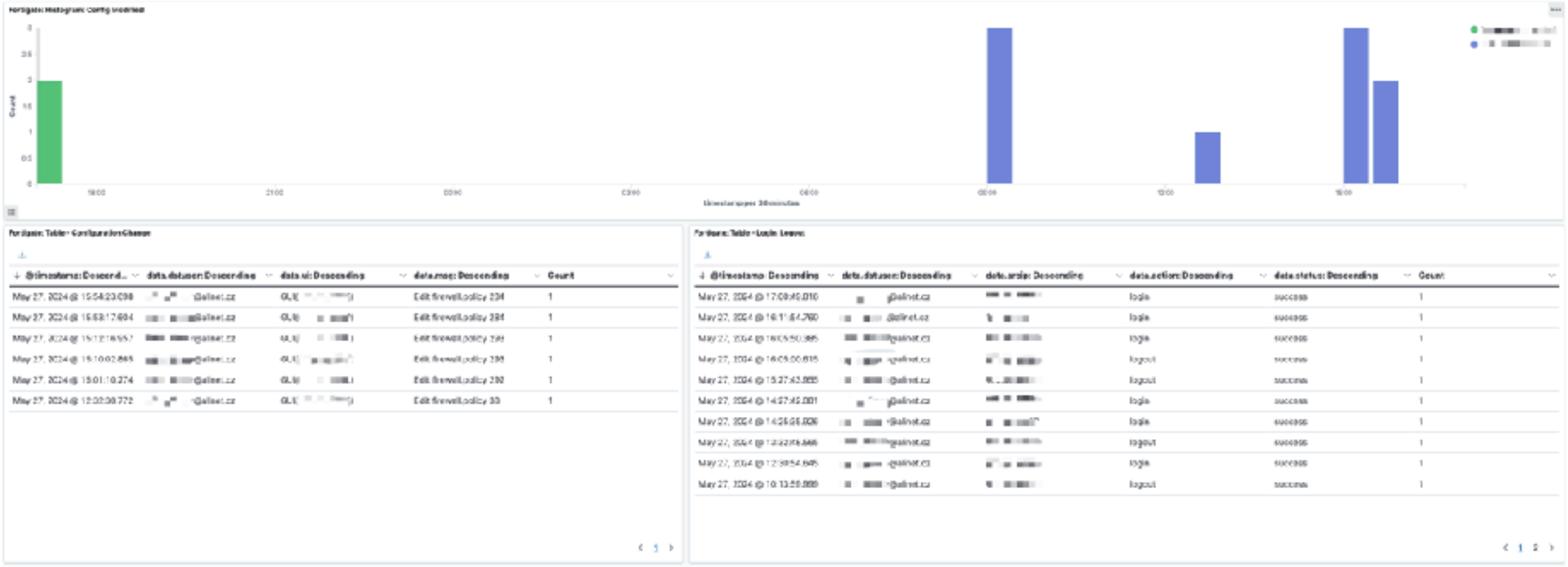


Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Proaktivní monitoring –

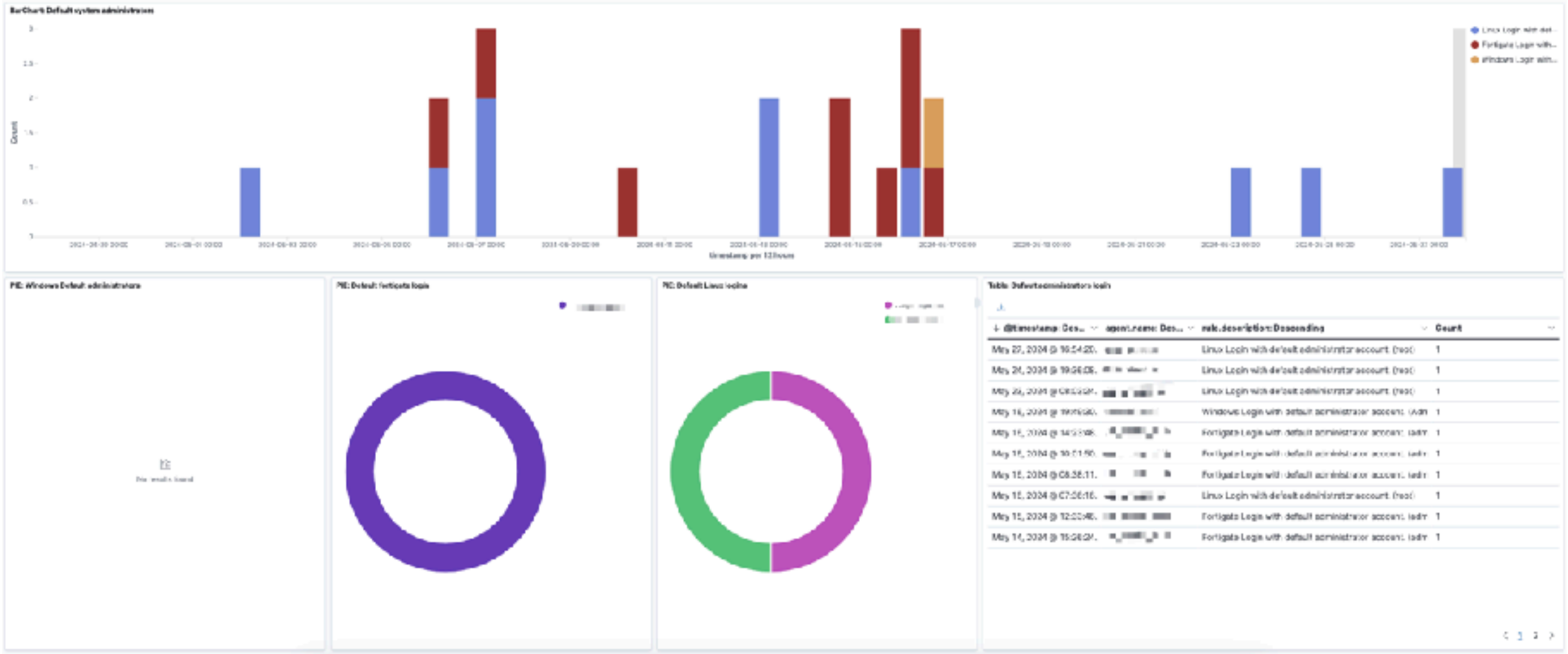
Monitoring změn FW



Alinet

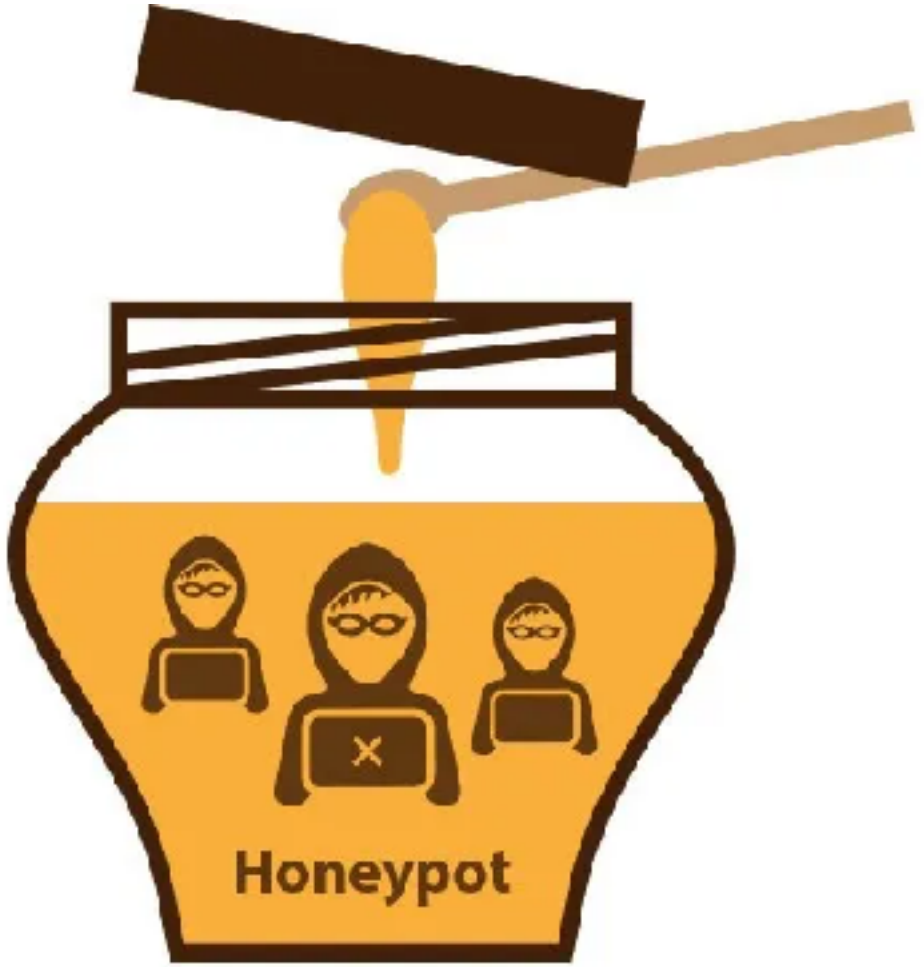
Proaktivní monitoring –

Defaultní administrátoři



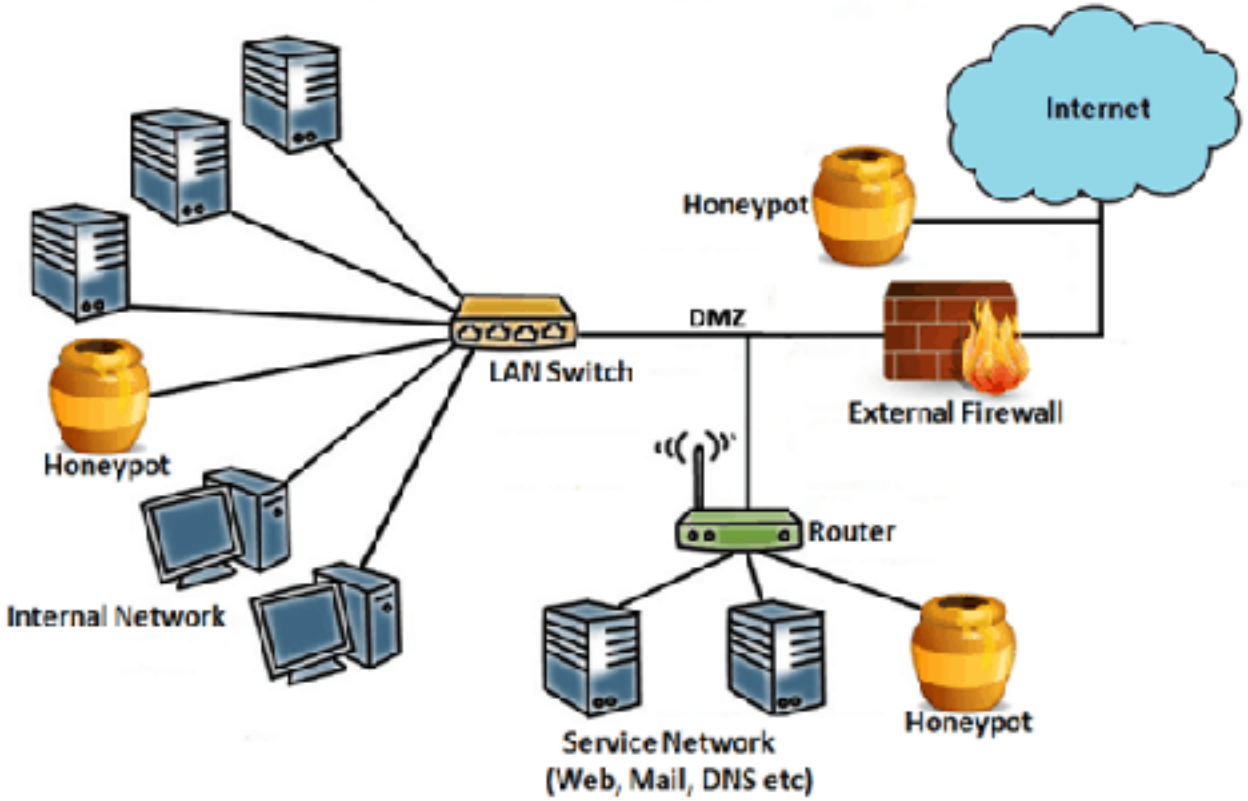
Alinet

Honeypots



Alinet

Honeypots

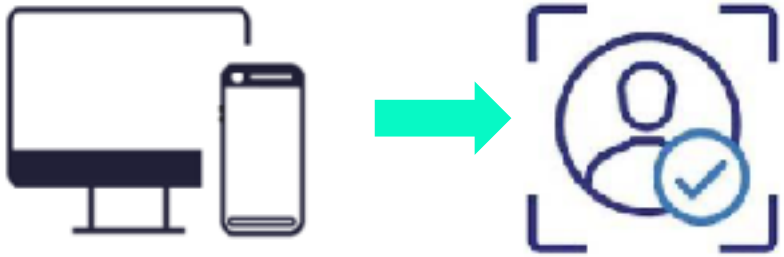


Alinet

Jak by to mělo dnes vypadat?

Alinet

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**

Alinet

Administrátor
nebo dodavatel

PAM appliance

JUMP server

Interní služby

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

Alinet

SOC

Administrátor
nebo dodavatel

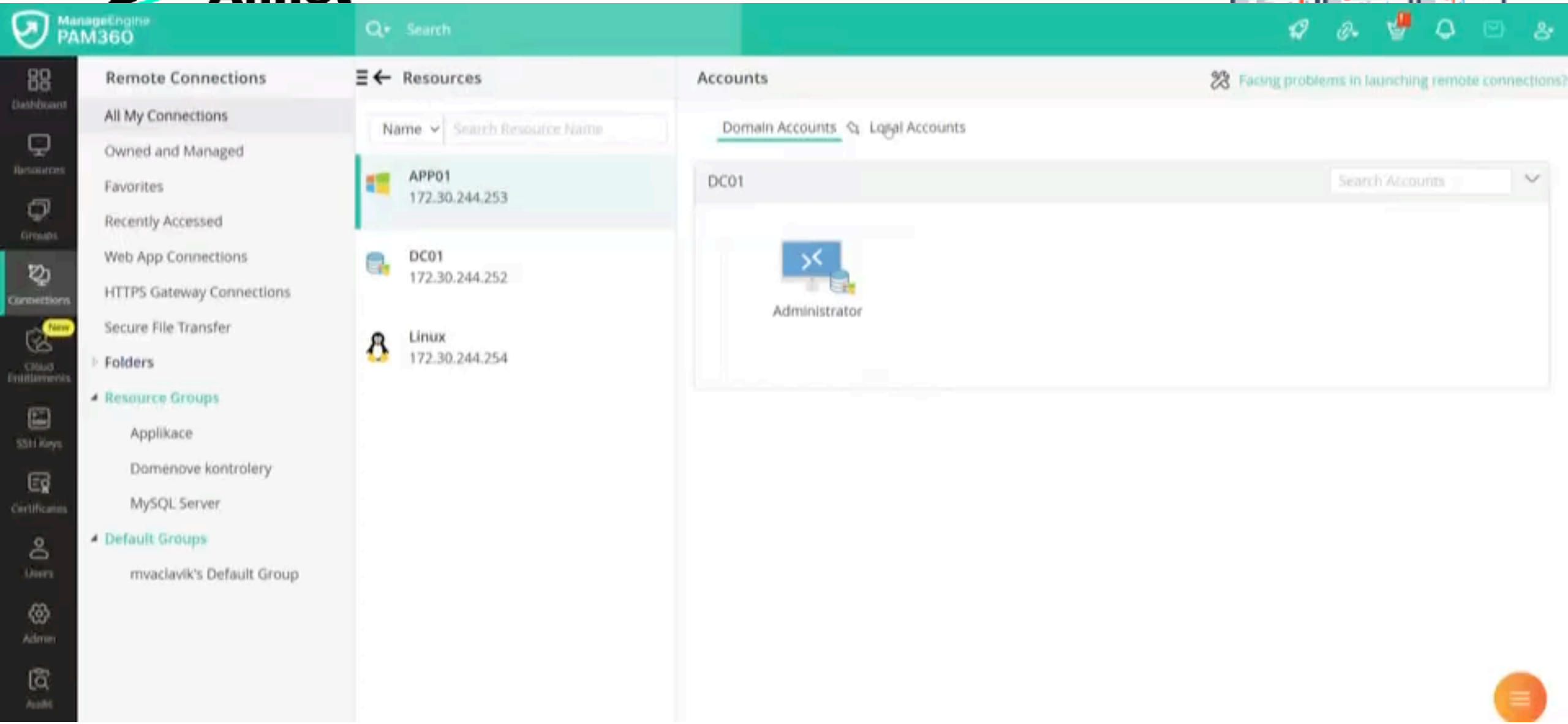
PAM appliance

JUMP server

Interní služby

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

Alinet


ManageEngine
PAM360
Search
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
Search Resource Name
APP01
172.30.244.253
DC01
172.30.244.252
Linux
172.30.244.254
Accounts
Facing problems in launching remote connections?
Domain Accounts
Local Accounts
DC01
Search Accounts
Administrator

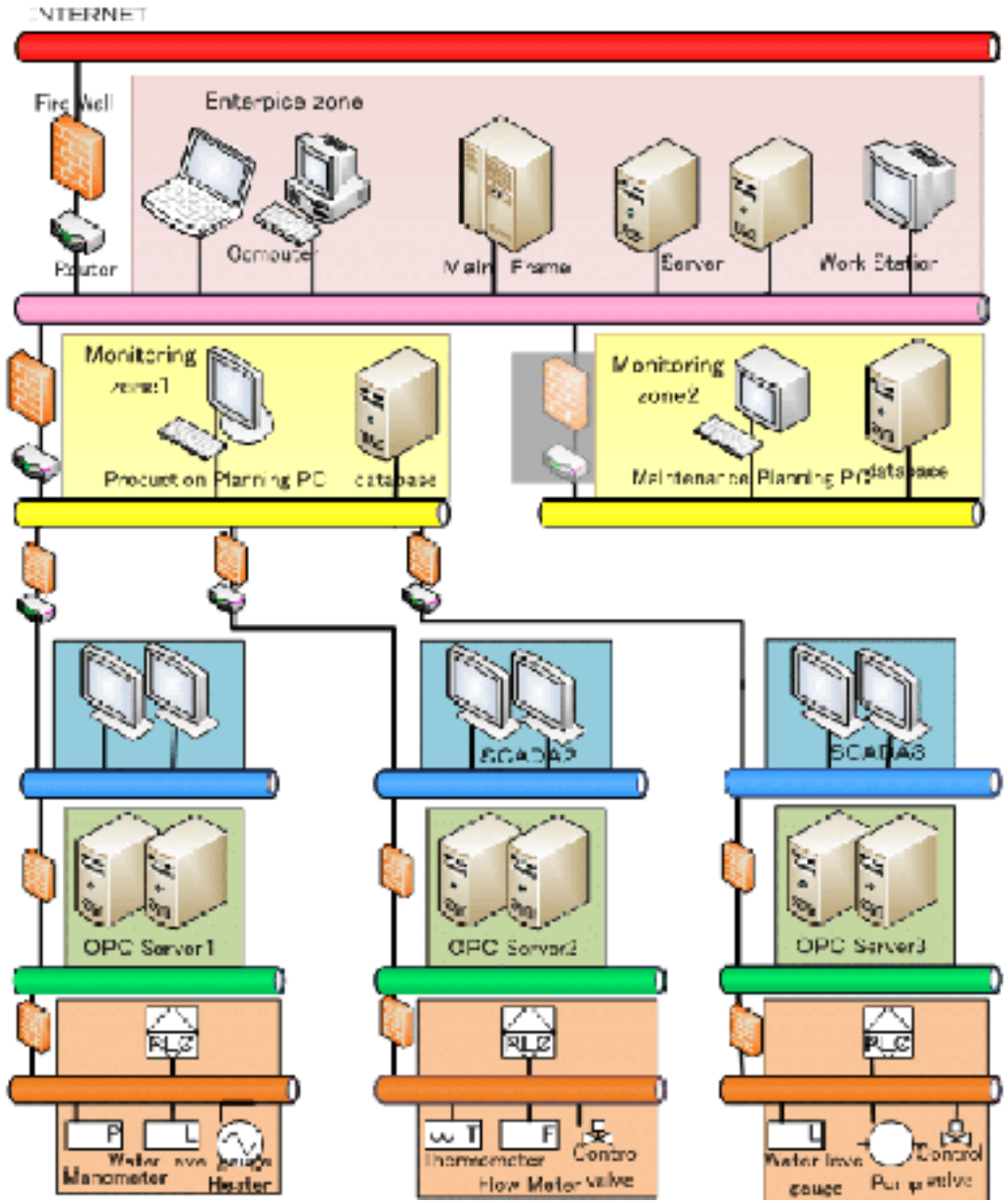
Alinet

Jak zabezpečit IoT OT systémy?

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

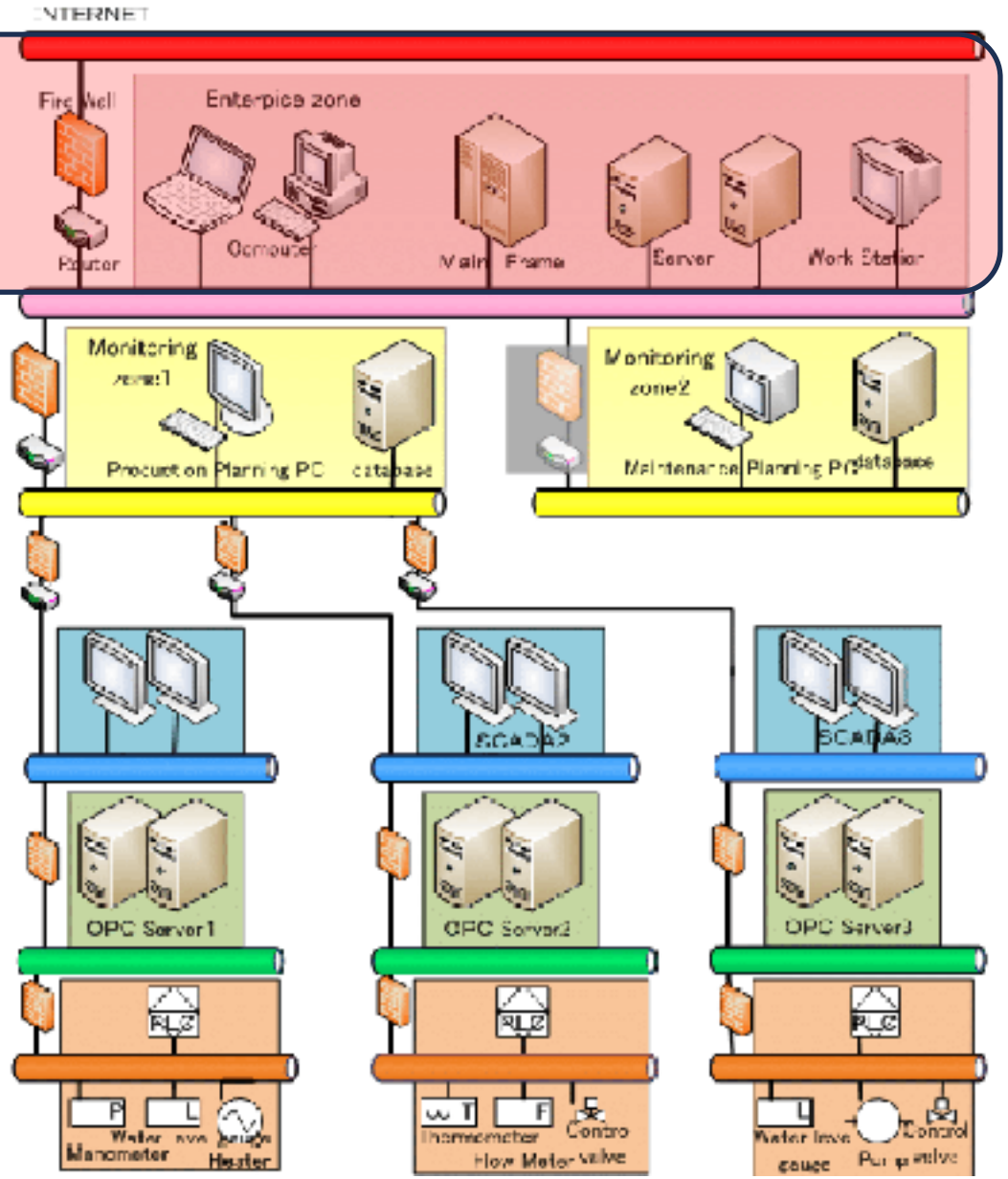
Alinet


Enterpice zone
Monitoring
Monitoring
zone2
OPC Server1
OPC Server2
OPC Server3
PLC
PLC
PLC
Heater
Control

Alinet

Level 4

- **ENTERPRISE ZONE**



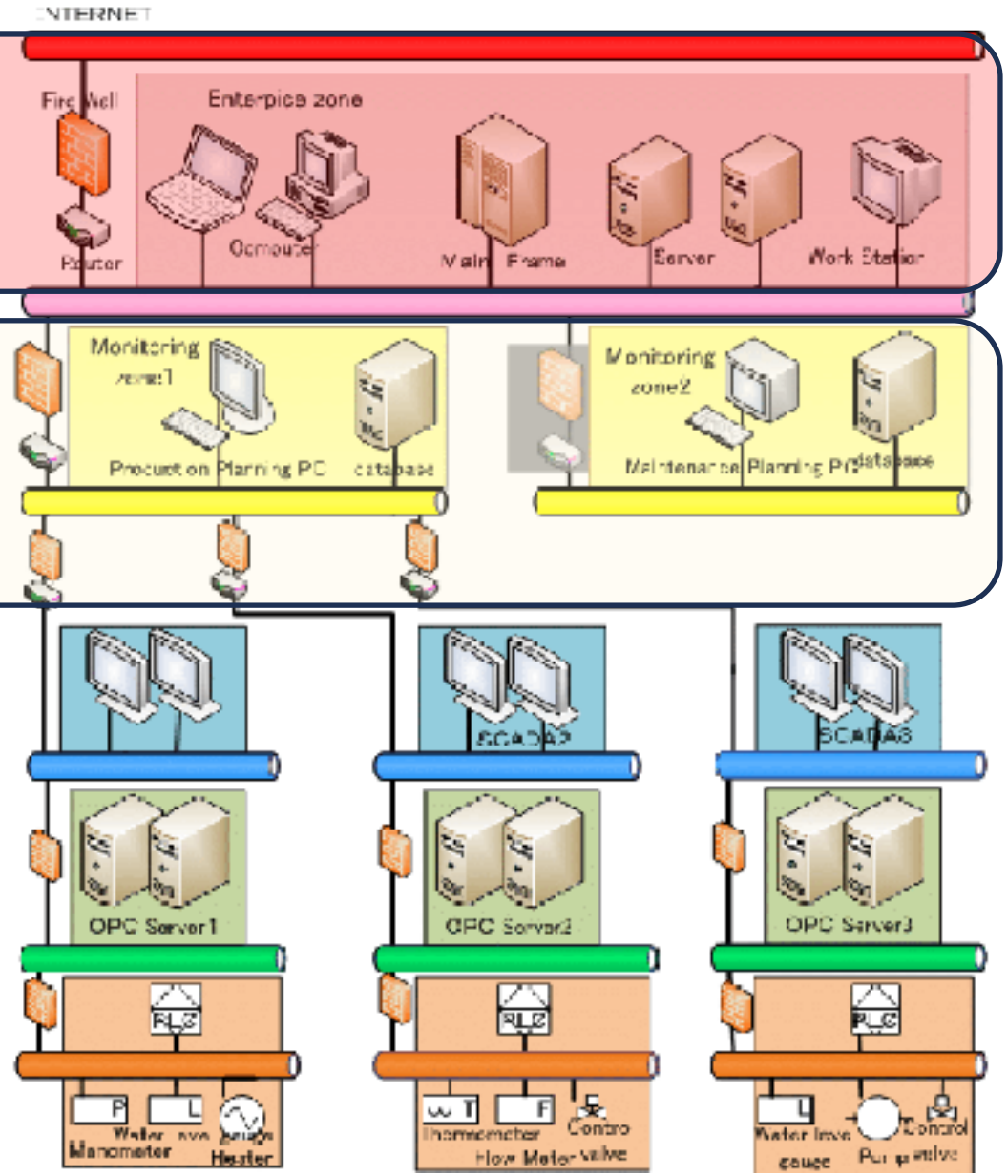
Alinet

Level 4

- **ENTERPRISE ZONE**

DMZ

- **DMZ ZONE**



Alinet

Level 4

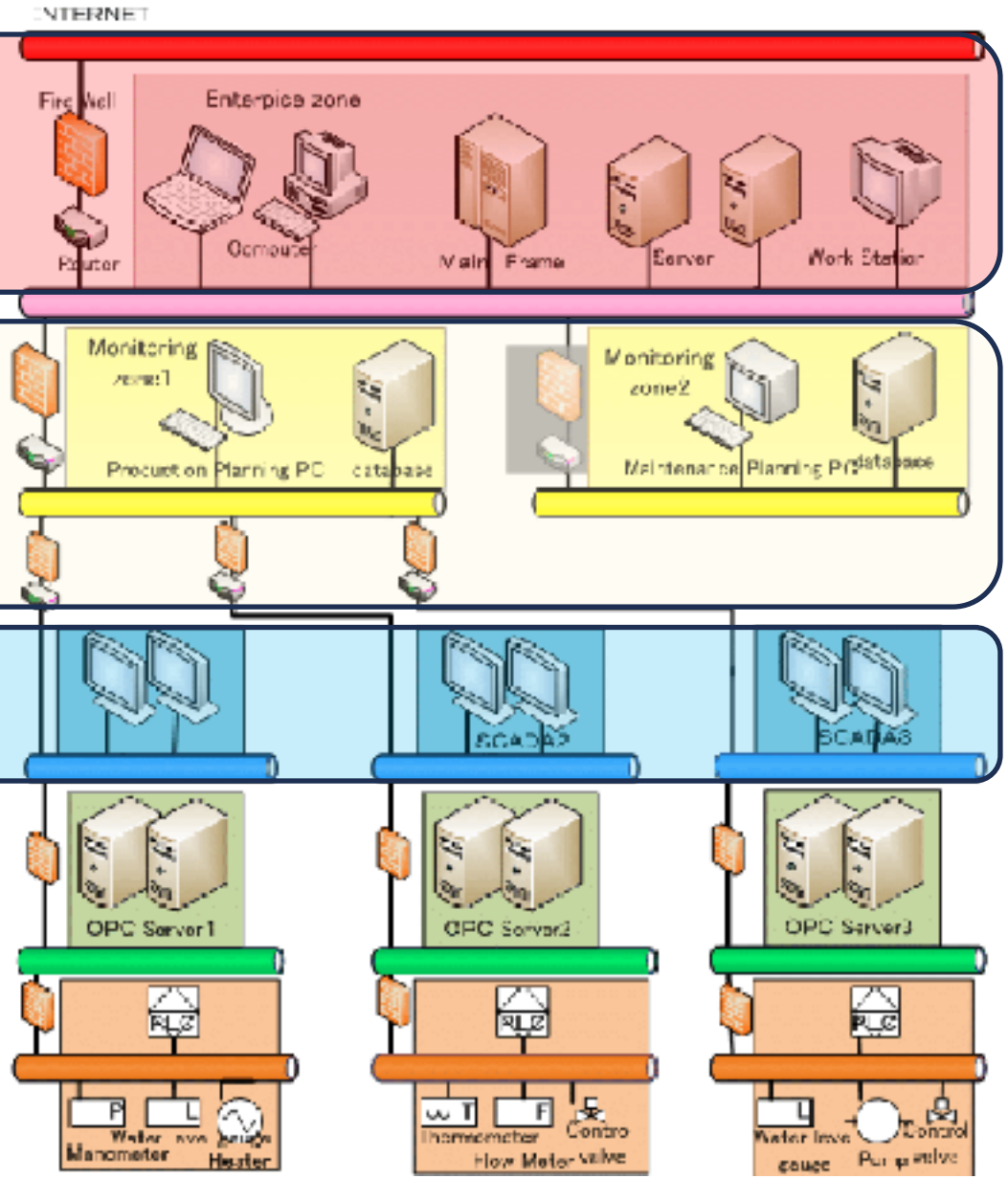
- ENTERPRISE ZONE

DMZ

- DMZ ZONE

Level 3

- OPERATION ZONE



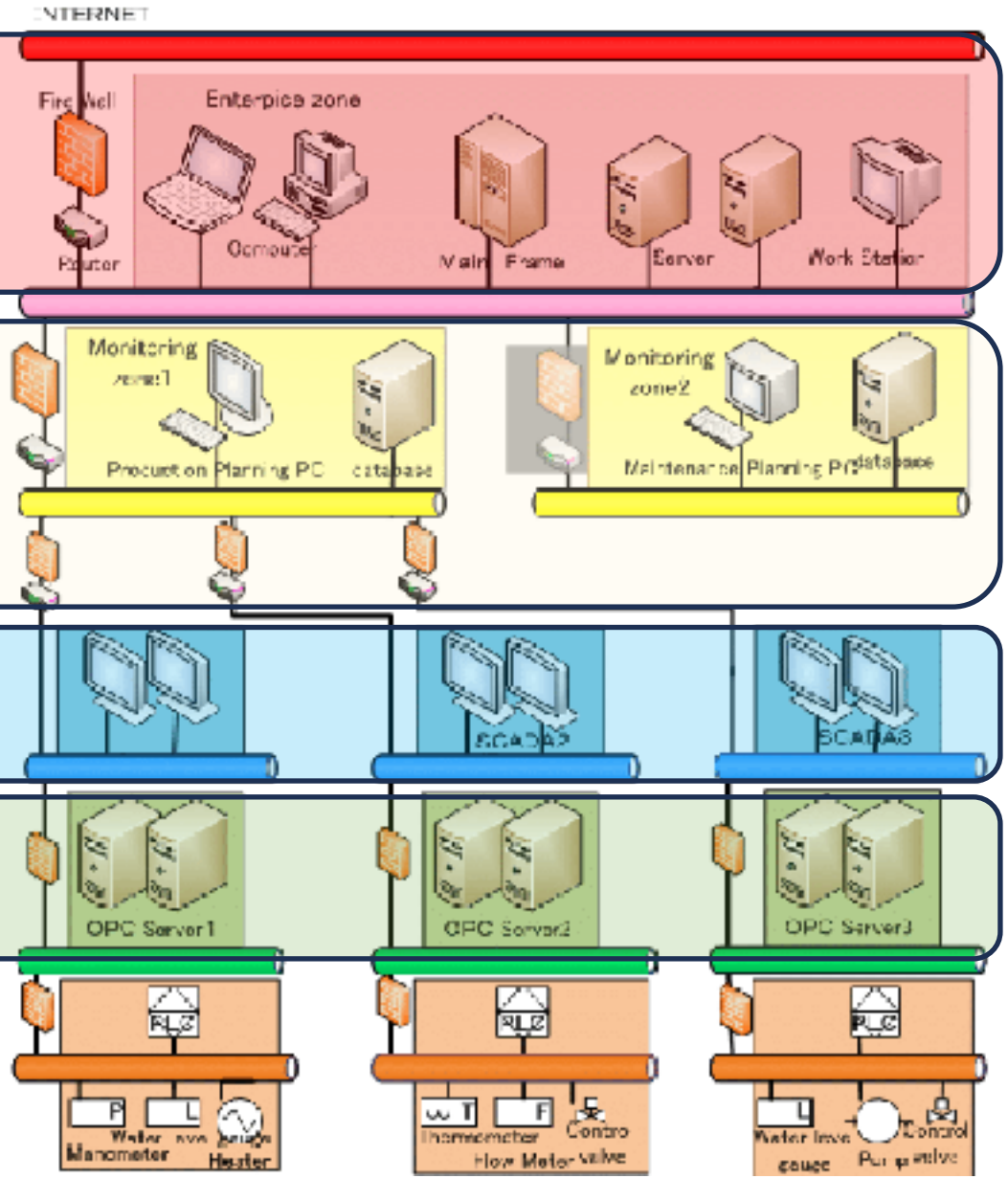
Alinet

Level 4
- ENTERPRISE ZONE

DMZ
- DMZ ZONE

Level 3
- OPERATION ZONE

Level 2
- SUPERVISOR ZONE



Alinet

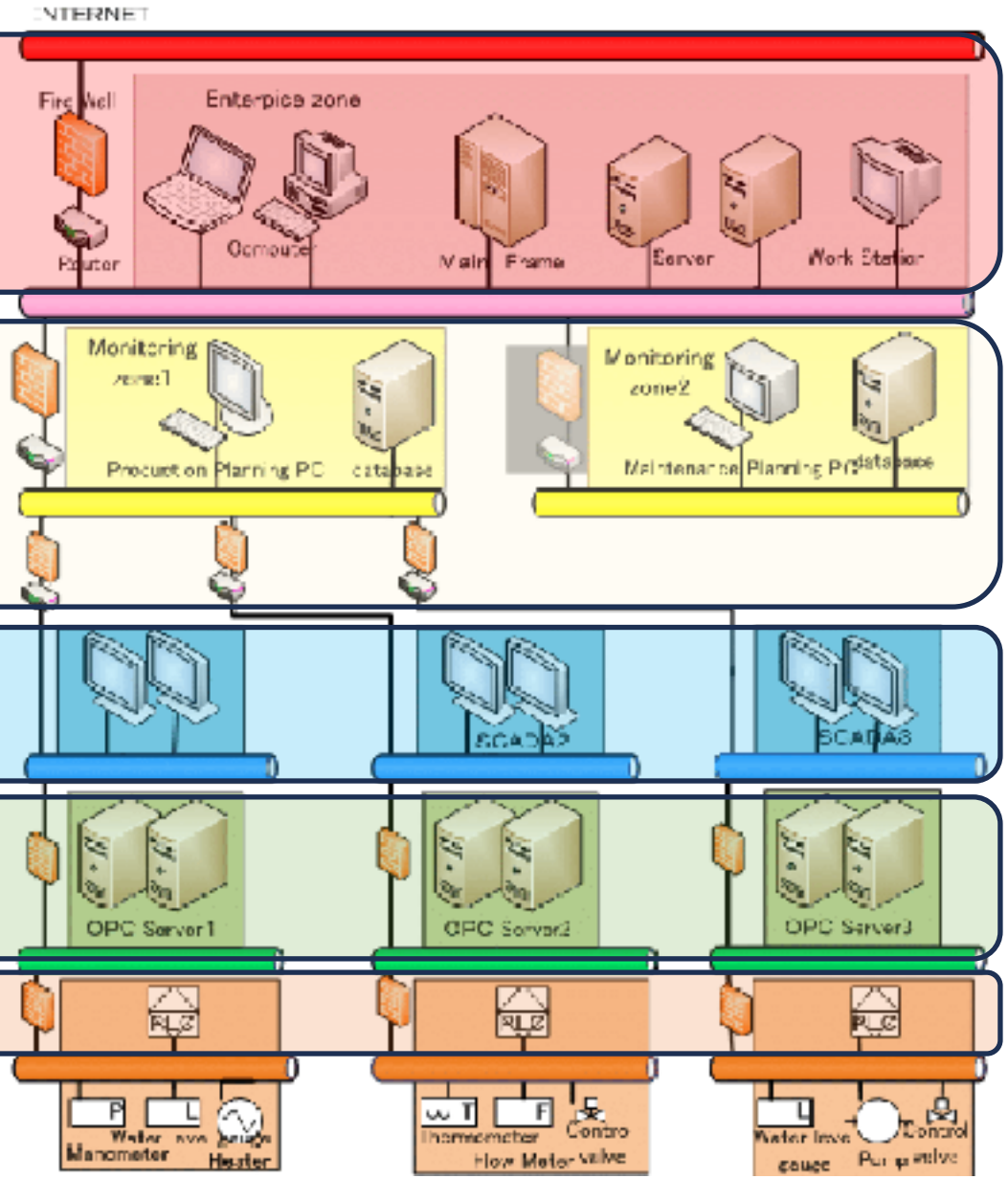
Level 4
- ENTERPRISE ZONE

DMZ
- DMZ ZONE

Level 3
- OPERATION ZONE

Level 2
- SUPERVISOR ZONE

Level 1 BASIC CONTROL ZONE



Alinet

Level 4
- ENTERPRISE ZONE

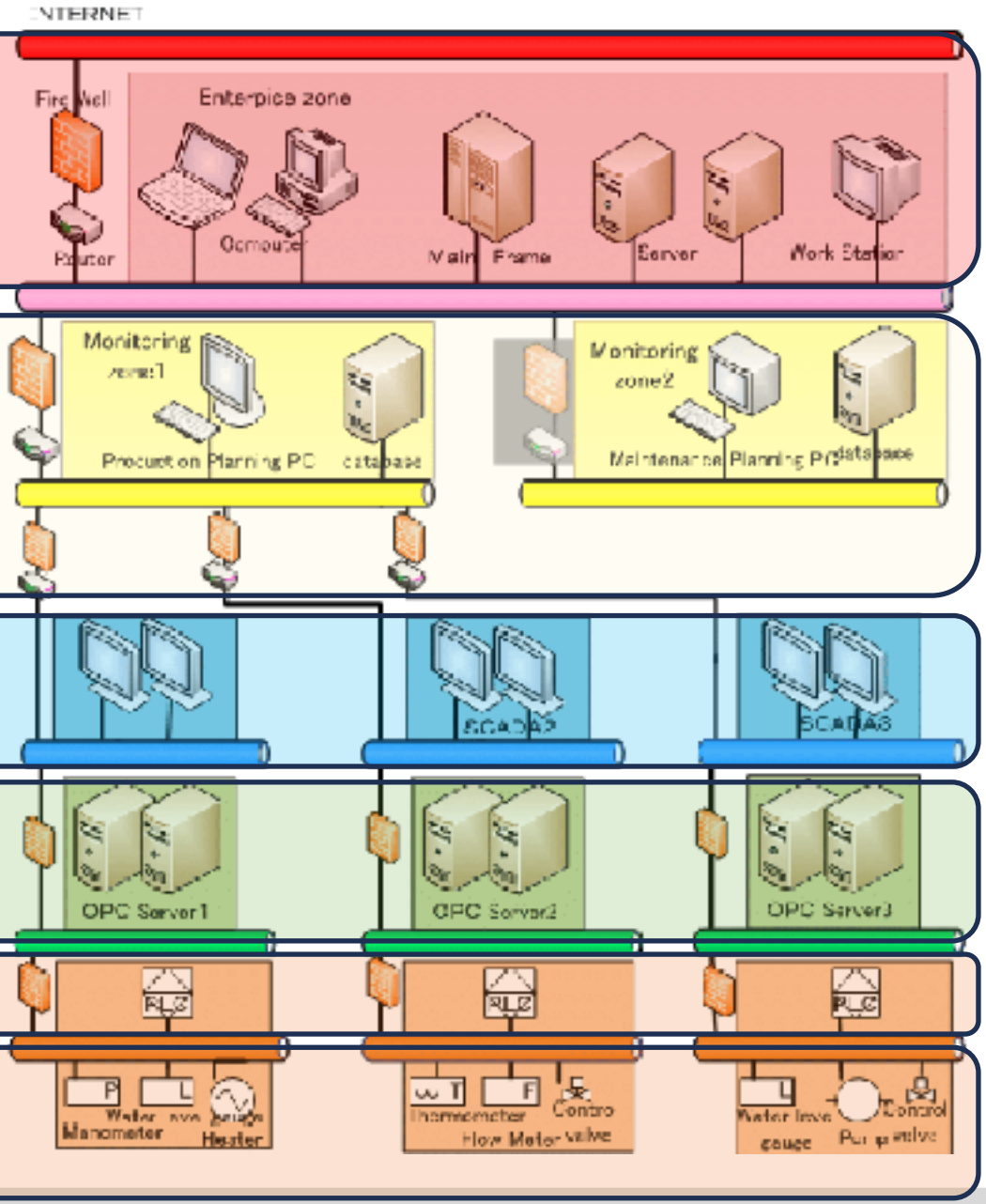
DMZ
- DMZ ZONE

Level 3
- OPERATION ZONE

Level 2
- SUPERVISOR ZONE

Level 1 BASIC CONTROL ZONE

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



IT ZONE

DMZ ZONE

CONTROL ZONE

Level 4
- ENTERPRISE ZONE

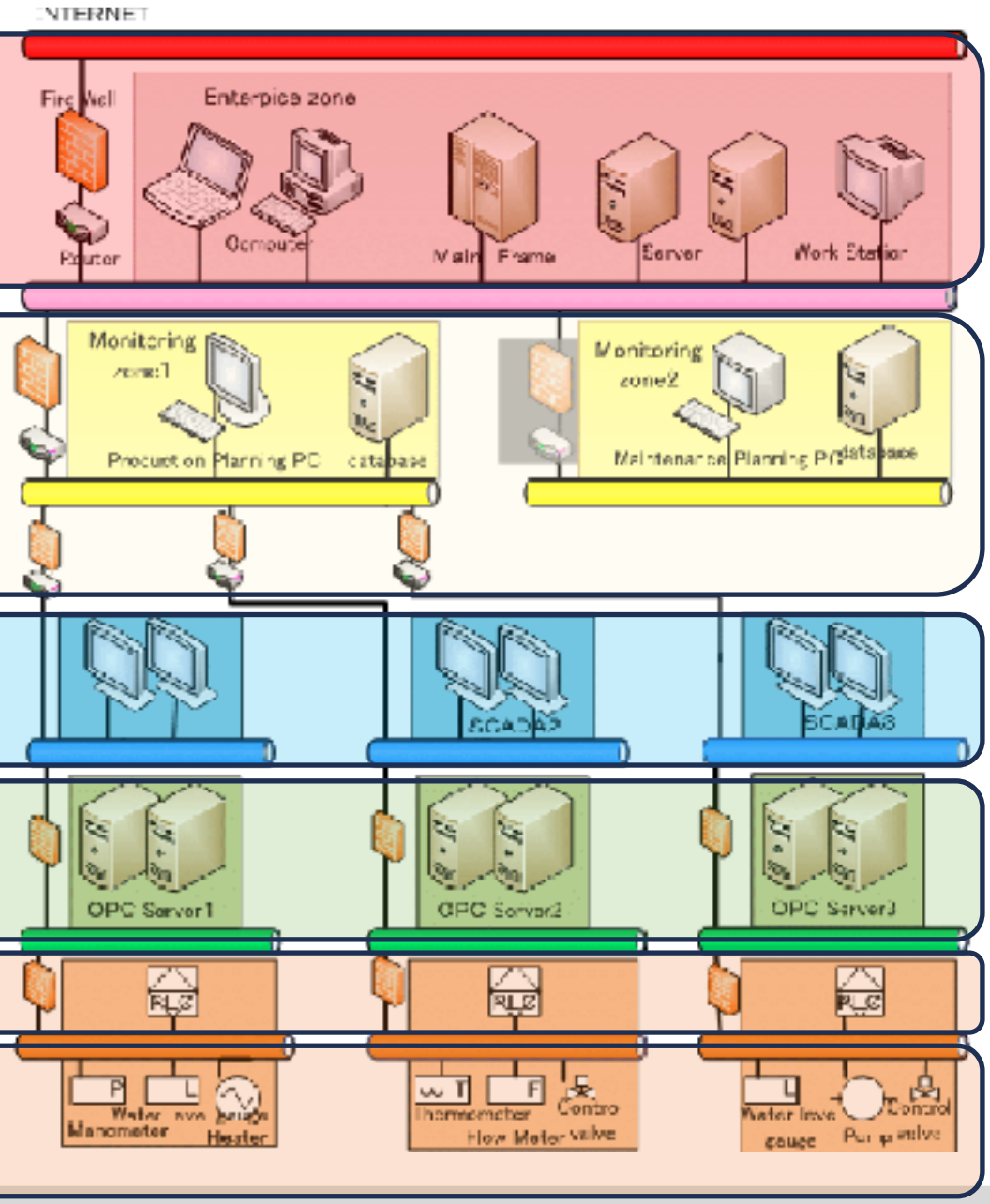
DMZ
- DMZ ZONE

Level 3
- OPERATION ZONE

Level 2
- SUPERVISOR ZONE

Level 1 BASIC CONTROL ZONE

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



IT ZONE

DMZ ZONE

CONTROL ZONE

Wide Area Network

Level 4
- ENTERPRISE ZONE

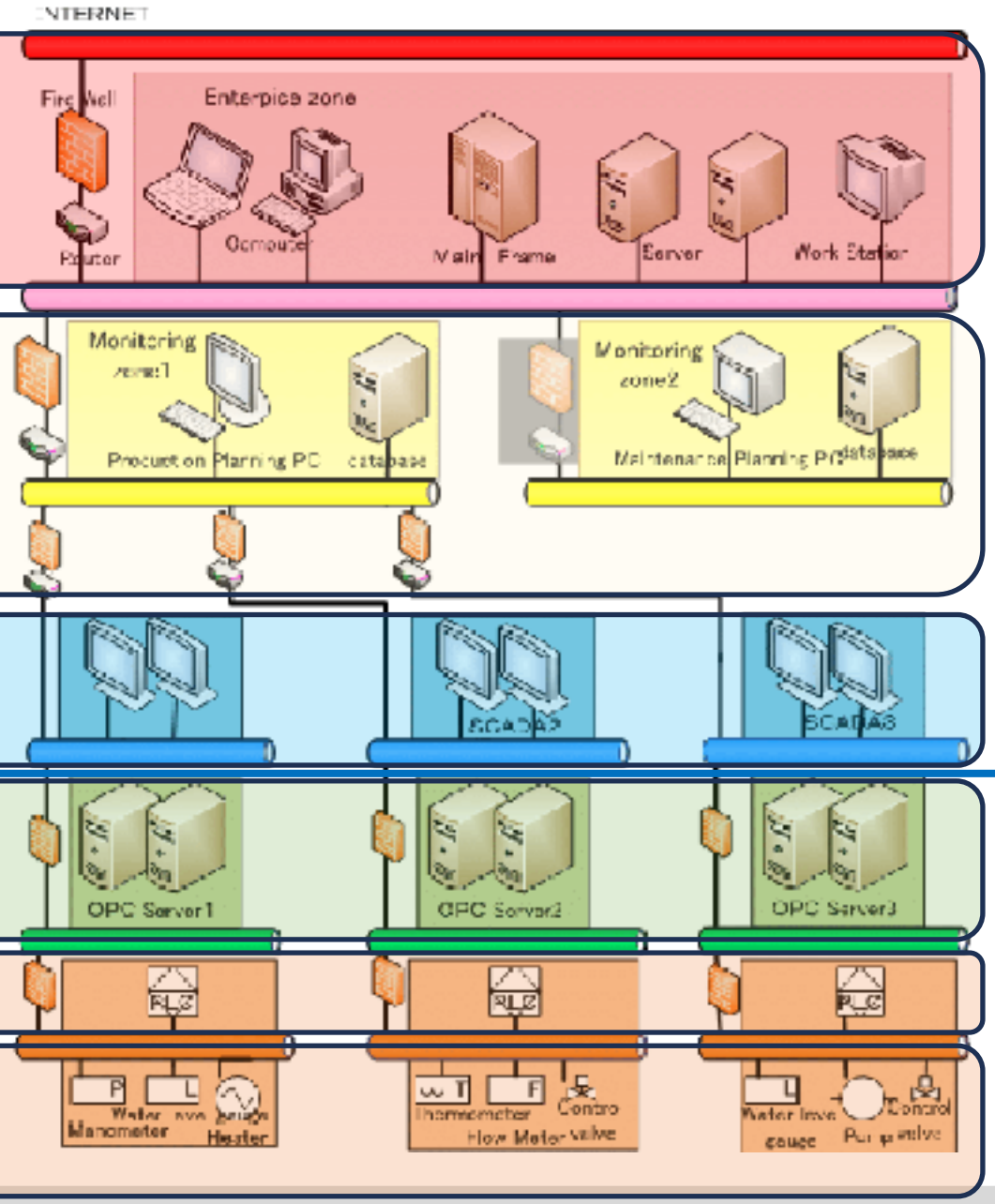
DMZ
- DMZ ZONE

Level 3
- OPERATION ZONE

Level 2
- SUPERVISOR ZONE

Level 1 BASIC CONTROL ZONE

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



IT ZONE

DMZ ZONE

CONTROL ZONE

Wide Area Network

Level 4
- ENTERPRISE ZONE

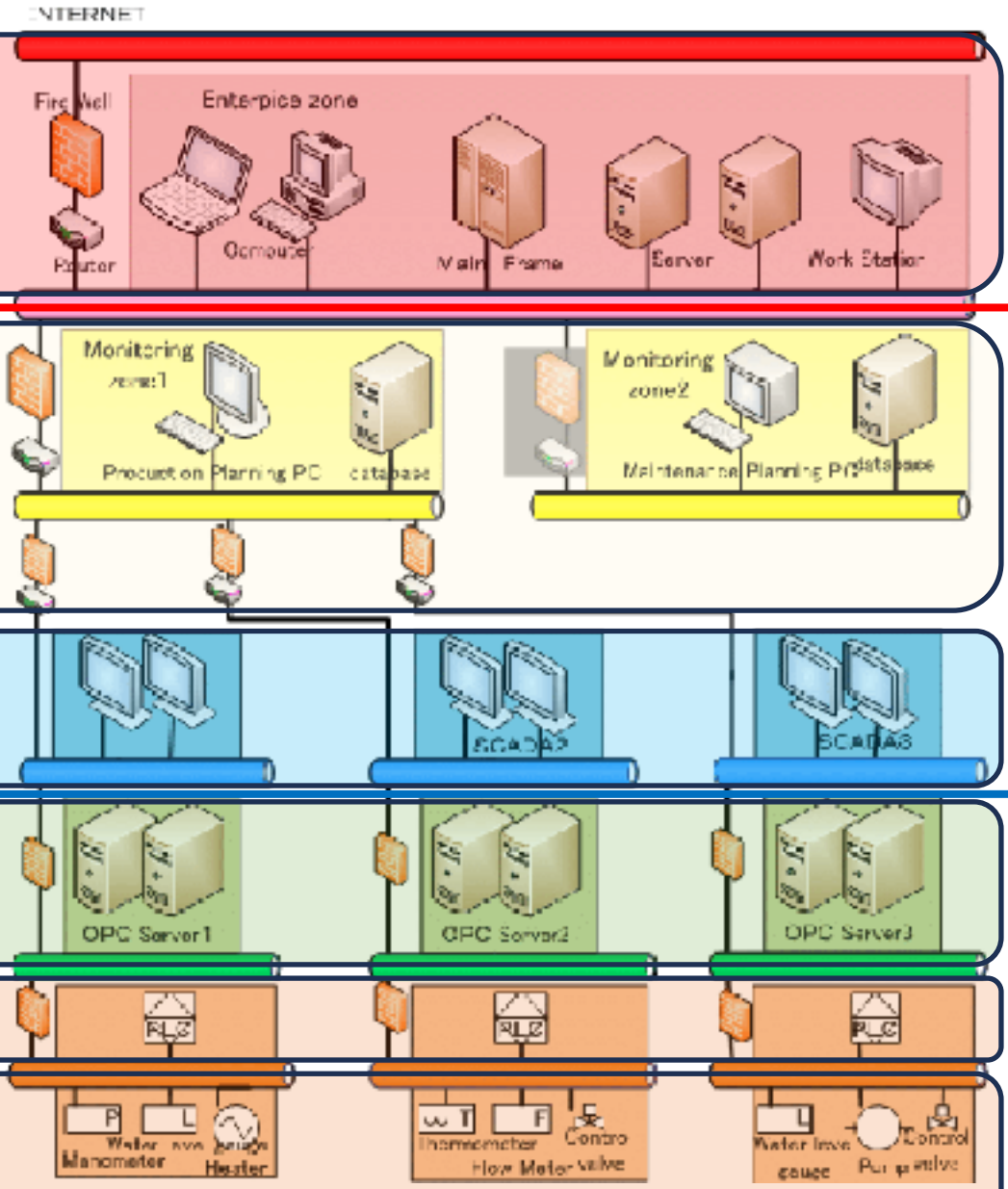
DMZ
- DMZ ZONE

Level 3
- OPERATION ZONE

Level 2
- SUPERVISOR ZONE

Level 1 BASIC CONTROL ZONE

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



IT ZONE

DMZ ZONE

CONTROL ZONE

Wide Area Network

Level 4
- ENTERPRISE ZONE

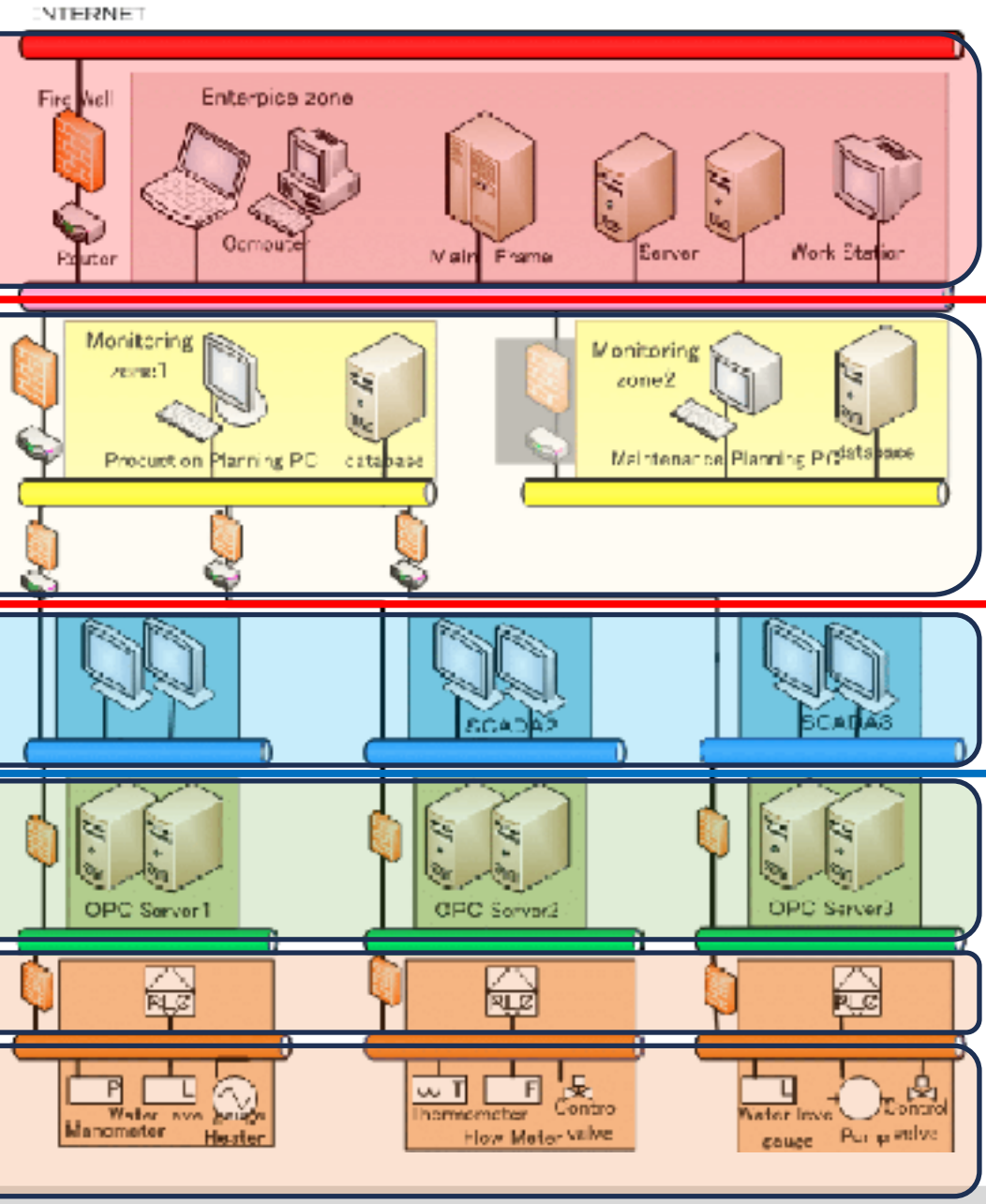
DMZ
- DMZ ZONE

Level 3
- OPERATION ZONE

Level 2
- SUPERVISOR ZONE

Level 1 BASIC CONTROL ZONE

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



Alinet

Jak začít ?

Alinet

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!**

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ **mobil:** +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Jak opravdu začít ?

Alinet

Ochrana perimetru

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Alinet

Potřebujete konzultaci ?

Otázky ?

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Potřebujete ...

PAM,

SOC,

Konzultace kyberbezpečnosti

Zabezpečit OT systémy

Architekta kybernetické bezpečnosti

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Vyžádejte si s námi schůzku již NYNÍ

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

Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Cyber Security, Ransomware Incident Response

Jakub Alimov

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