Alinet

Útoky a zabezpečení OT systémů

14.5.2025

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

Lead Auditor

architekt kybernetické bezpečnosti,

RANSOMWARE hunter,

konzultant informační bezpečnosti,

více jak 15+ let prokazatelných zkušeností s kybernetickou bezpečností

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

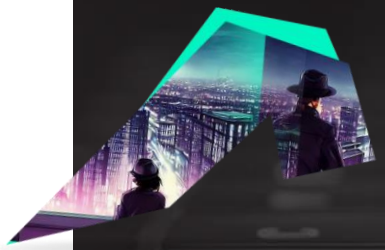
Alinet

Kdo je Alinet?

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



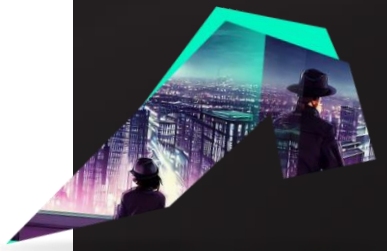
DIGITAL FORENSICS AND INCIDENT RESPONSE

Jsme progresivní IT 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

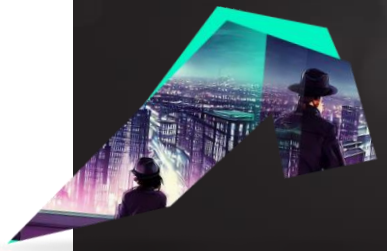
Alinet



DIGITAL FORENSICS AND INCIDENT RESPONSE

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

Jsme progresivní IT 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

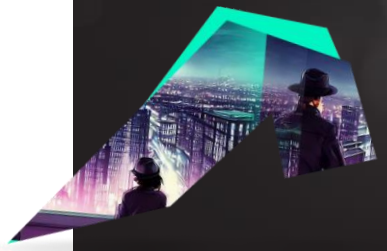
Alinet

Jsme progresivní IT 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

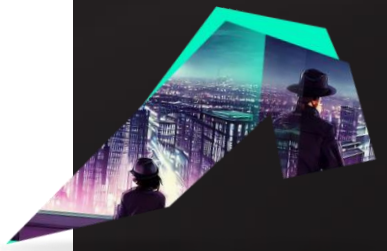


Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

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

Alinet

Jsme progresivní IT firma se specializací na kybernetické útoky.

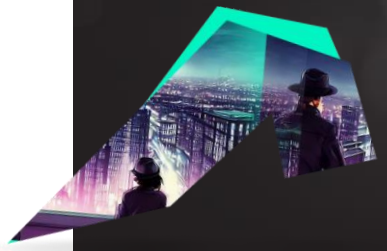


DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ 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

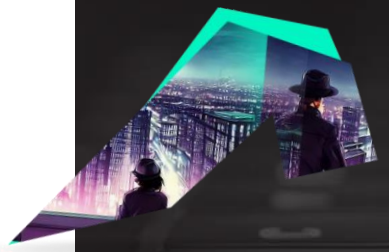
mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Jsme progresivní IT 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

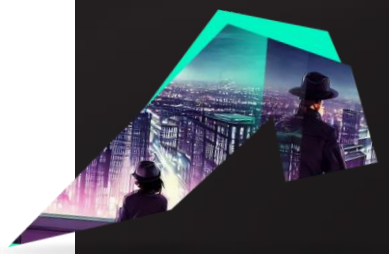
SLUŽBA DETEKCE KYBERNETICKÝCH UDÁLOSTÍ

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 progresivní IT 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

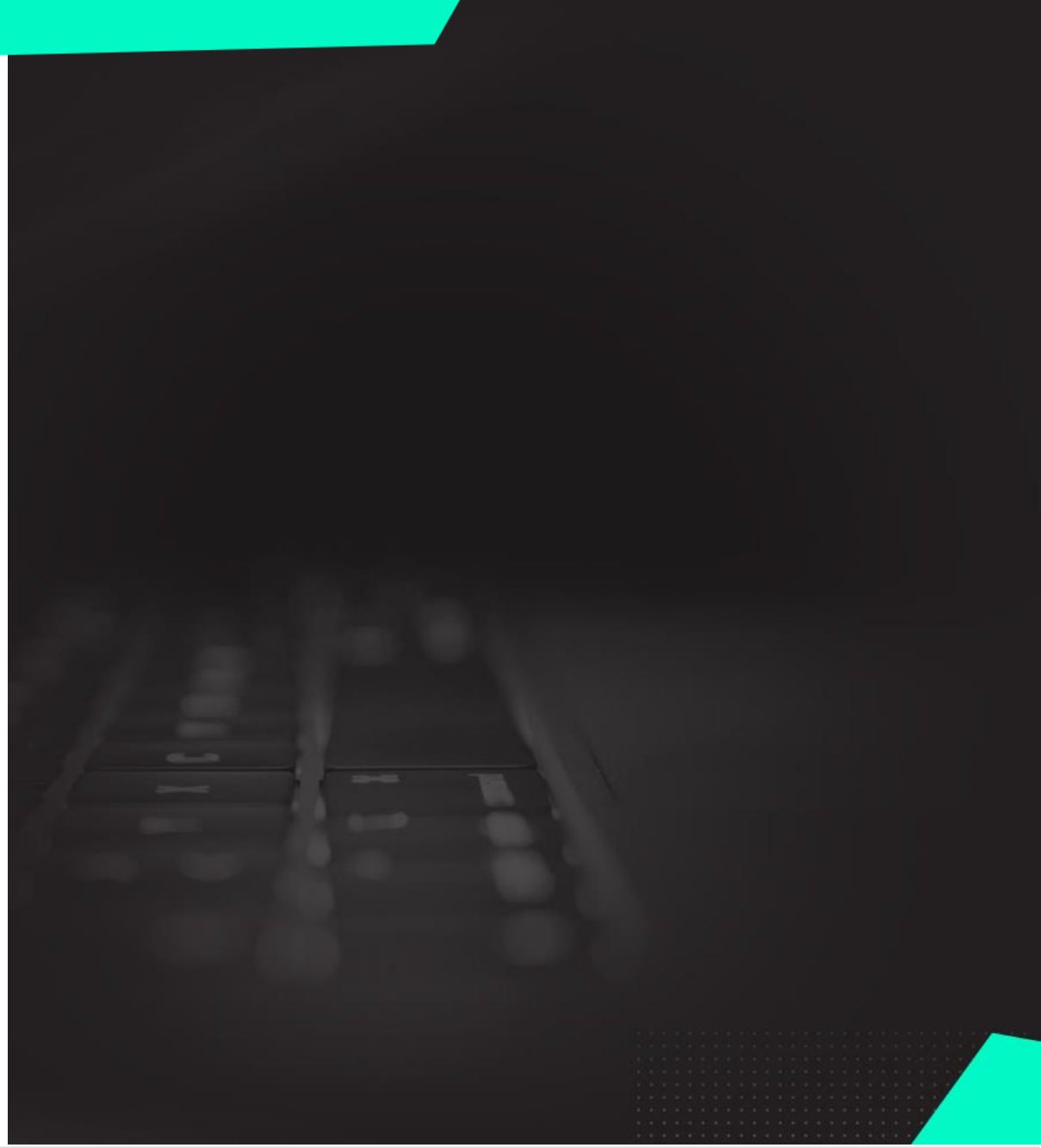
mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Otázka na úvod?

Alinet

Kdo je u Vás zodpovědný za provoz a údržbu OT systémů z pohledu IT?

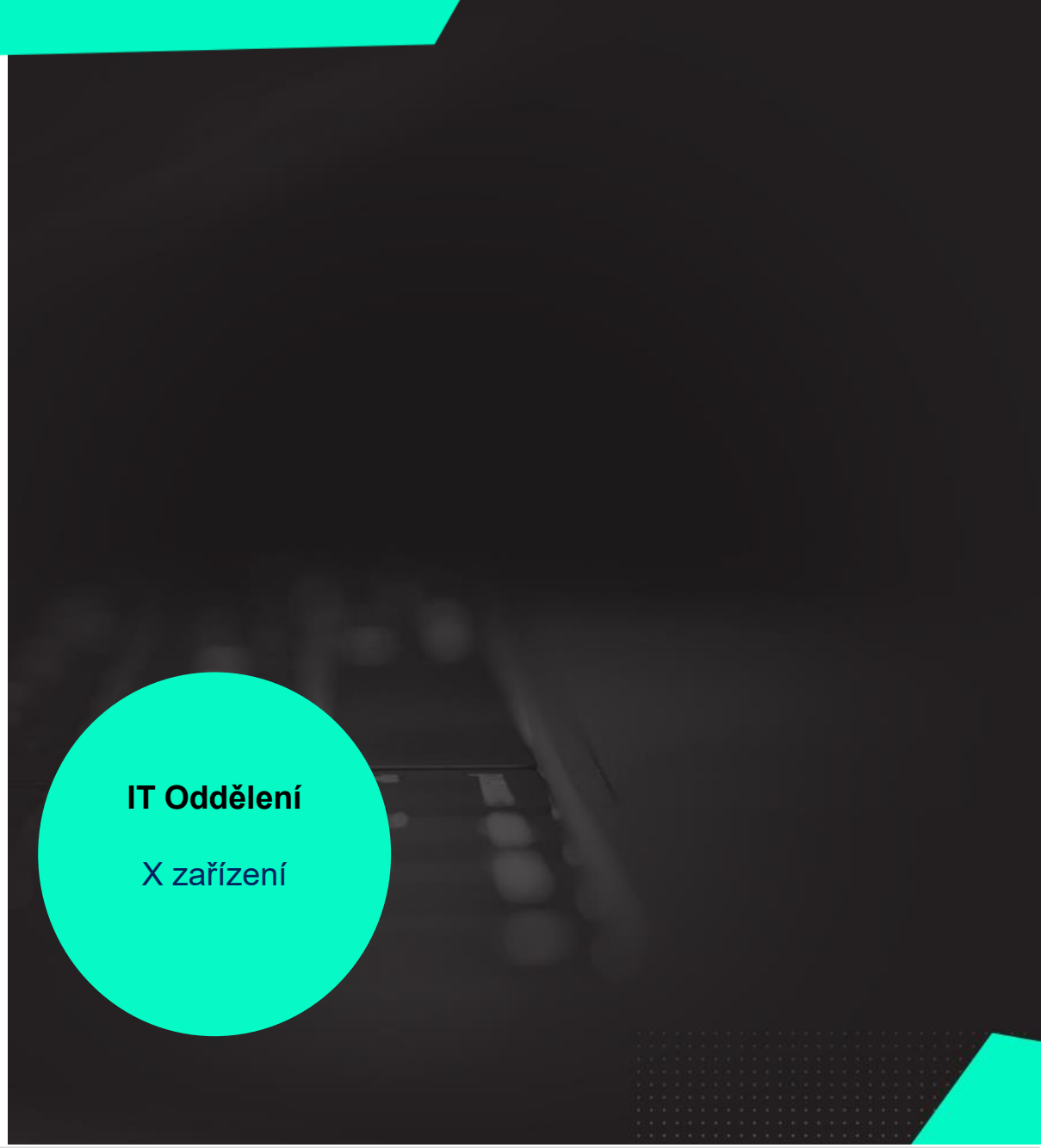


Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

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

Alinet

Kdo je u Vás zodpovědný za provoz a údržbu OT systémů z pohledu IT?

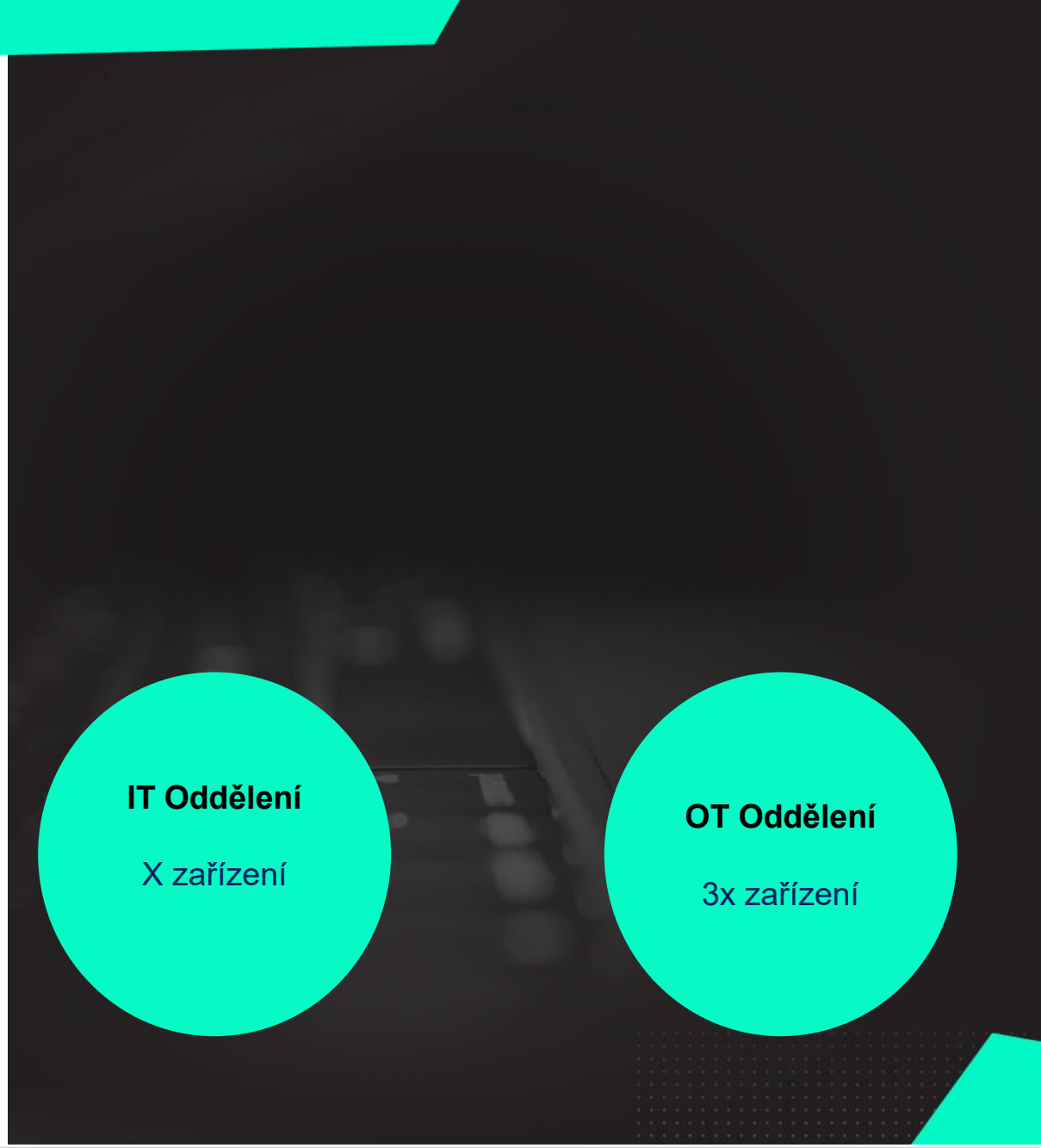


Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

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

Alinet

Kdo je u Vás zodpovědný za provoz a údržbu OT systémů z pohledu IT?

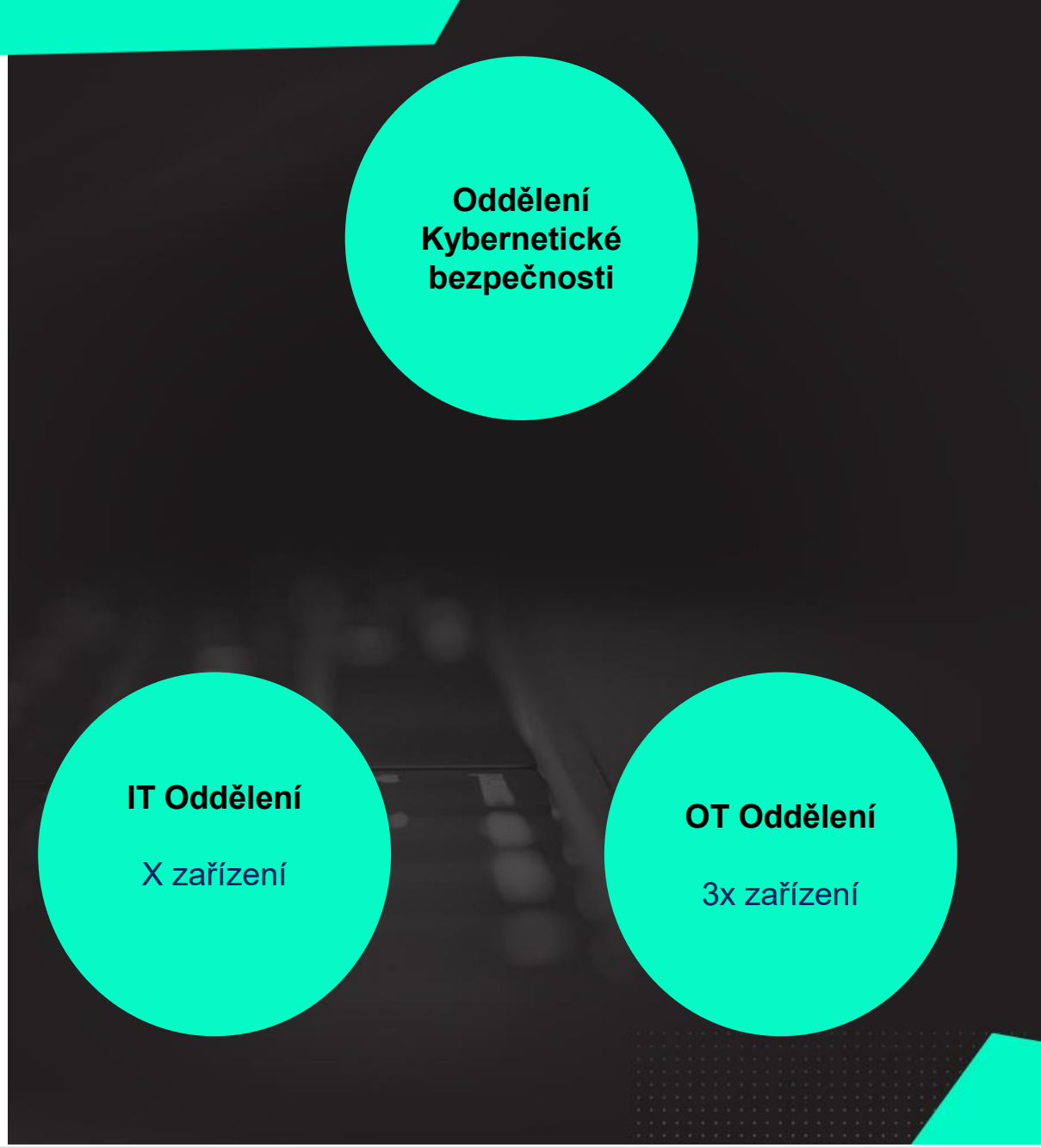


Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

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

Alinet

Kdo je u Vás zodpovědný za provoz a údržbu OT systémů z pohledu IT?



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

Kdo je u Vás zodpovědný za provoz a údržbu OT systémů z pohledu IT?

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

Kdo je u Vás zodpovědný za provoz a údržbu OT systémů z pohledu IT?

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

Kdo je u Vás zodpovědný za provoz a údržbu OT systémů z pohledu IT?

Alinet

Útoky na Operační Technologie

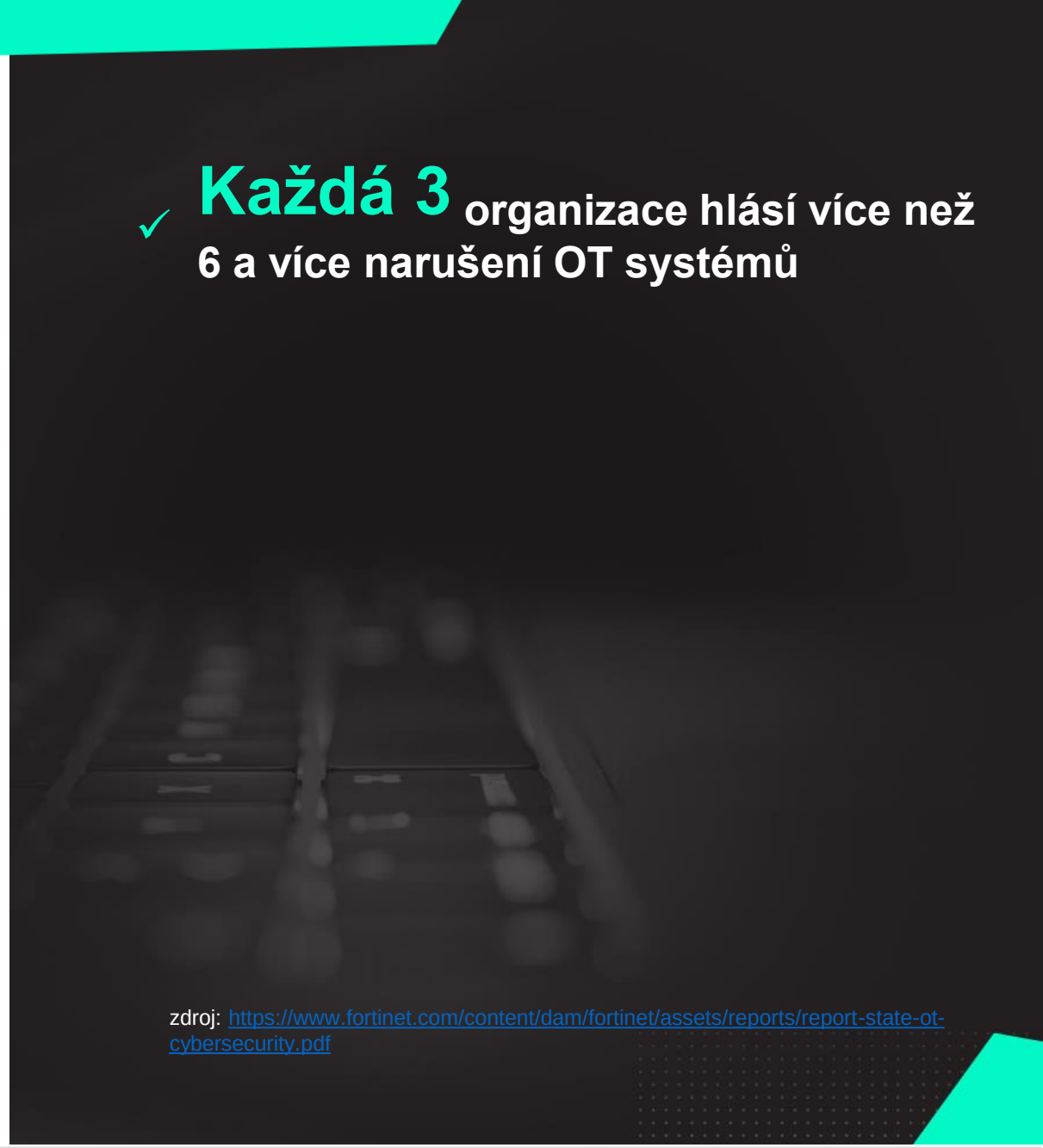
Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

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

Alinet

OT útoky v roce 2024?

✓ **Každá 3** organizace hlásí více než 6 a více narušení OT systémů



zdroj: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf

Alinet

OT útoky v roce 2024?

- **Každá 3** organizace hlásí více než 6 a více narušení OT systémů
- **55%** OT organizací zaznamenalo **výpadek** systému s kybernetickým útokem

zdroj: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf

Alinet

OT útoky v roce 2024?

- ✓ **Každá 3** organizace hlásí více než 6 a více narušení OT systémů
- ✓ **55%** OT organizací zaznamenalo **výpadek** systému s kybernetickým útokem
- ✓ **43 %** OT organizací přišlo o kritický data

zdroj: https://www.fortinet.com/content/dam/fortinet/assets/reports/report-state-ot-cybersecurity.pdf

Alinet

Reálné útoky v roce 2024?

Chtěl bych se s Vámi podělit o několik skutečných příběhů z forenzního vyšetřování z minulého roku.

- ✓ **Útok na nezabezpečené zařízení vzdálené správy OT zařízení, exploitace a následné proniknutí do jiné vrstvy podnikové sítě**
- ✓ **Neaktualizovaná webová služba umožnila přístup komukoliv do interní firemní sítě**
- ✓ **Síťově spojené IT a OT prostředí zašifrovalo výrobní společnost**
- ✓ **Dělali jsme audit IT prostředí OT prostředí audit nelze co kdyby náhodou to přestalo fungovat ? :)**

Alinet

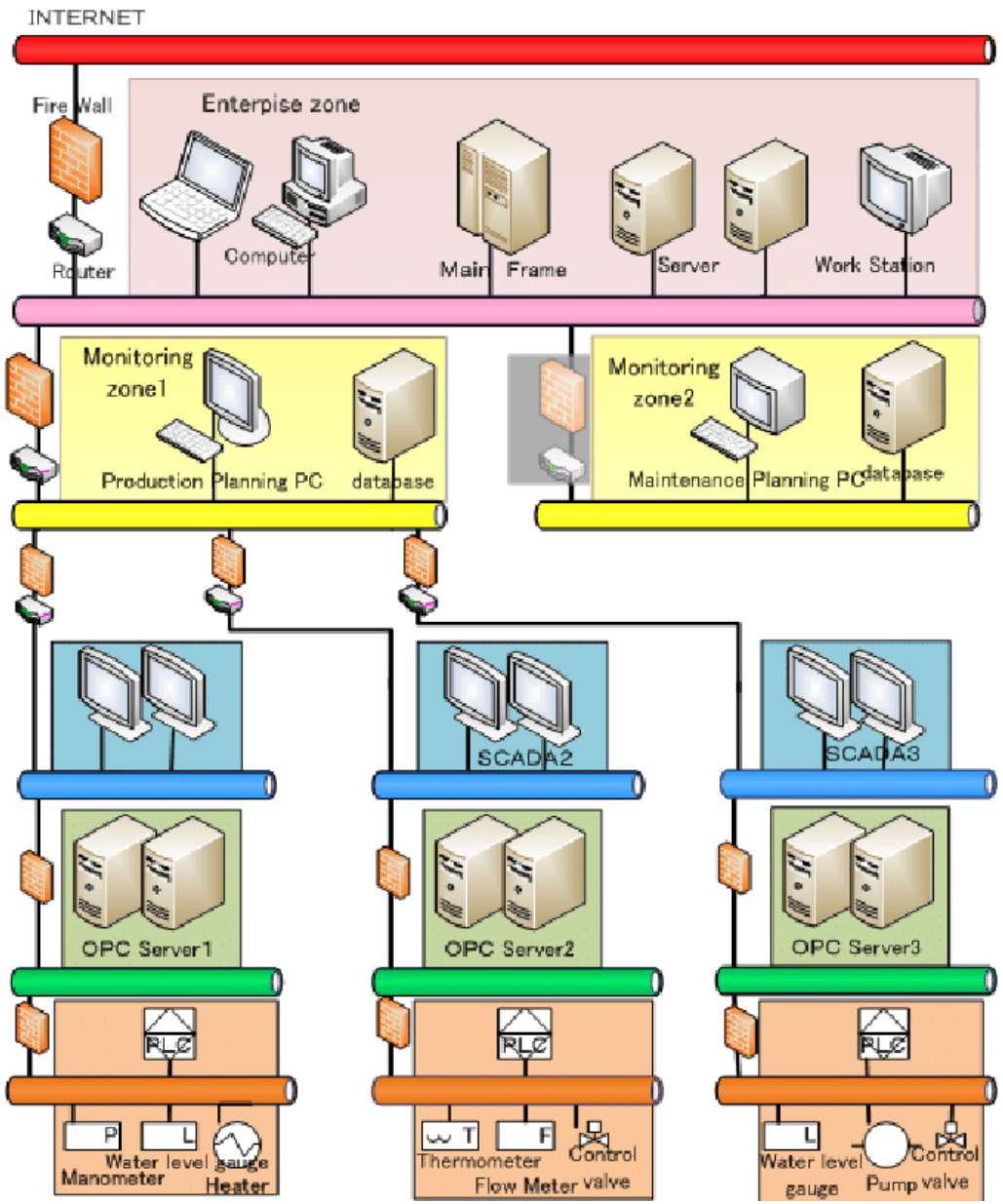
Proč útoky na operační technologie?

- ✓ Protože OT systémy vždy byly navrženy pouze pro **funkčnost** nikoliv kybernetickou bezpečnost
- ✓ Protože životnost OT systému je 10-**30 let!**
- ✓ Protože OT systémy je **heterogení prostředí**, kde je peer systém dodavatel, peer dodavatel vlastní 5G mobilní připojení ideálně rovnou do sítě internet
- ✓ Protože hrozba útoku přes **dodavatelský řetězec** je velmi častá a bohužel i reálná
- ✓ Protože OT kybernetická bezpečnost DNES = IT kybernetická bezpečnost **před 15 ti lety!**
- ✓ Protože jsou zranitelnosti ve Firmware a Software update a je složitý někdy až **nemožný**

Alinet

Jak by to mělo dnes vypadat?

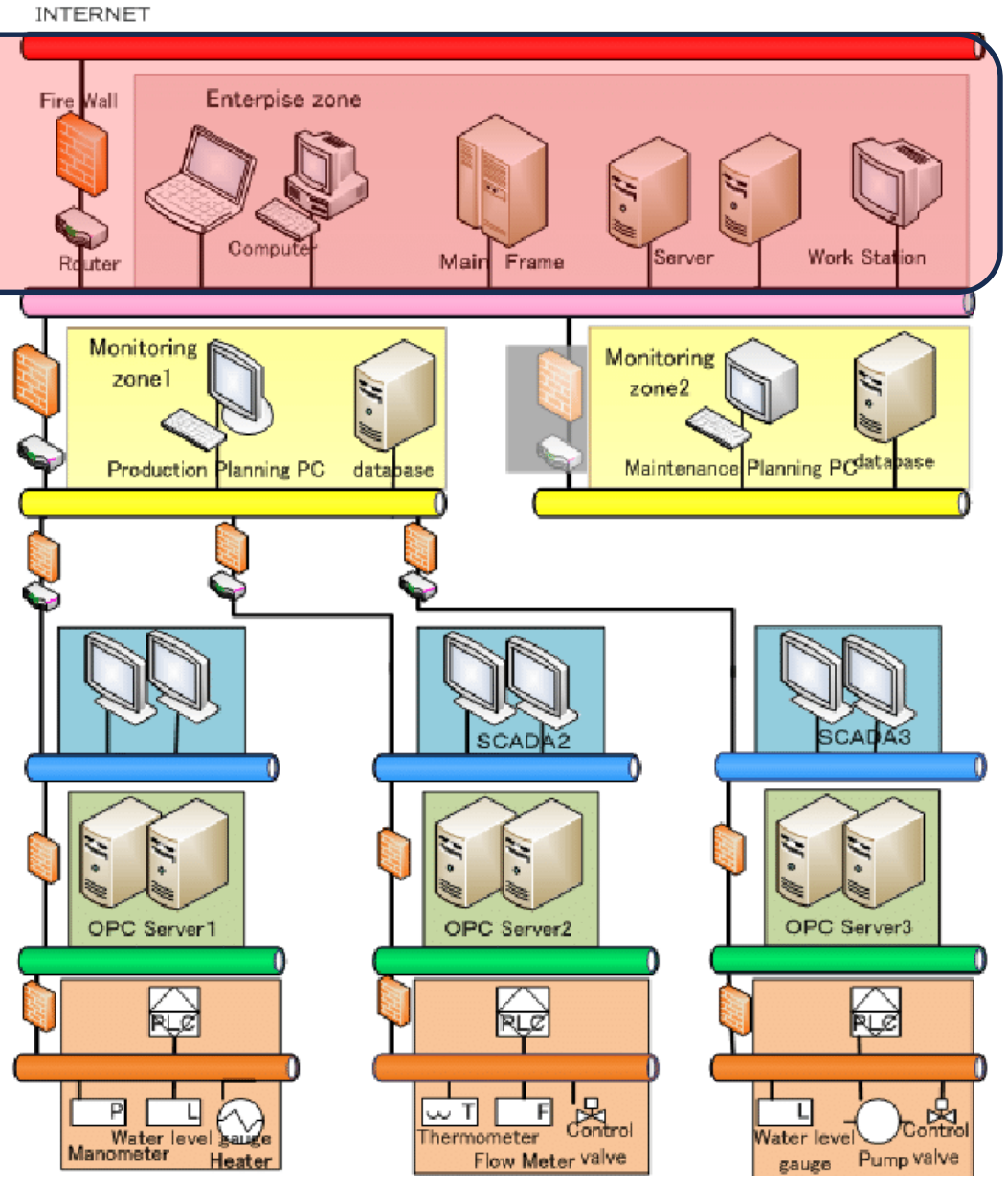
Alinet


INTERNET
Fire Wall
Enterpise zone
Router
Computer
Main Frame
Server
Work Station
Monitoring zone1
Production Planning PC
database
Monitoring zone2
Maintenance Planning PC
database
SCADA2
SCADA3
OPC Server1
OPC Server2
OPC Server3
PLC
P
Manometer
L
Water level gauge
Heater
T
Thermometer
F
Flow Meter
Control valve
L
Water level gauge
Control Pump valve

Alinet

Level 4

- **ENTERPRISE ZONE**



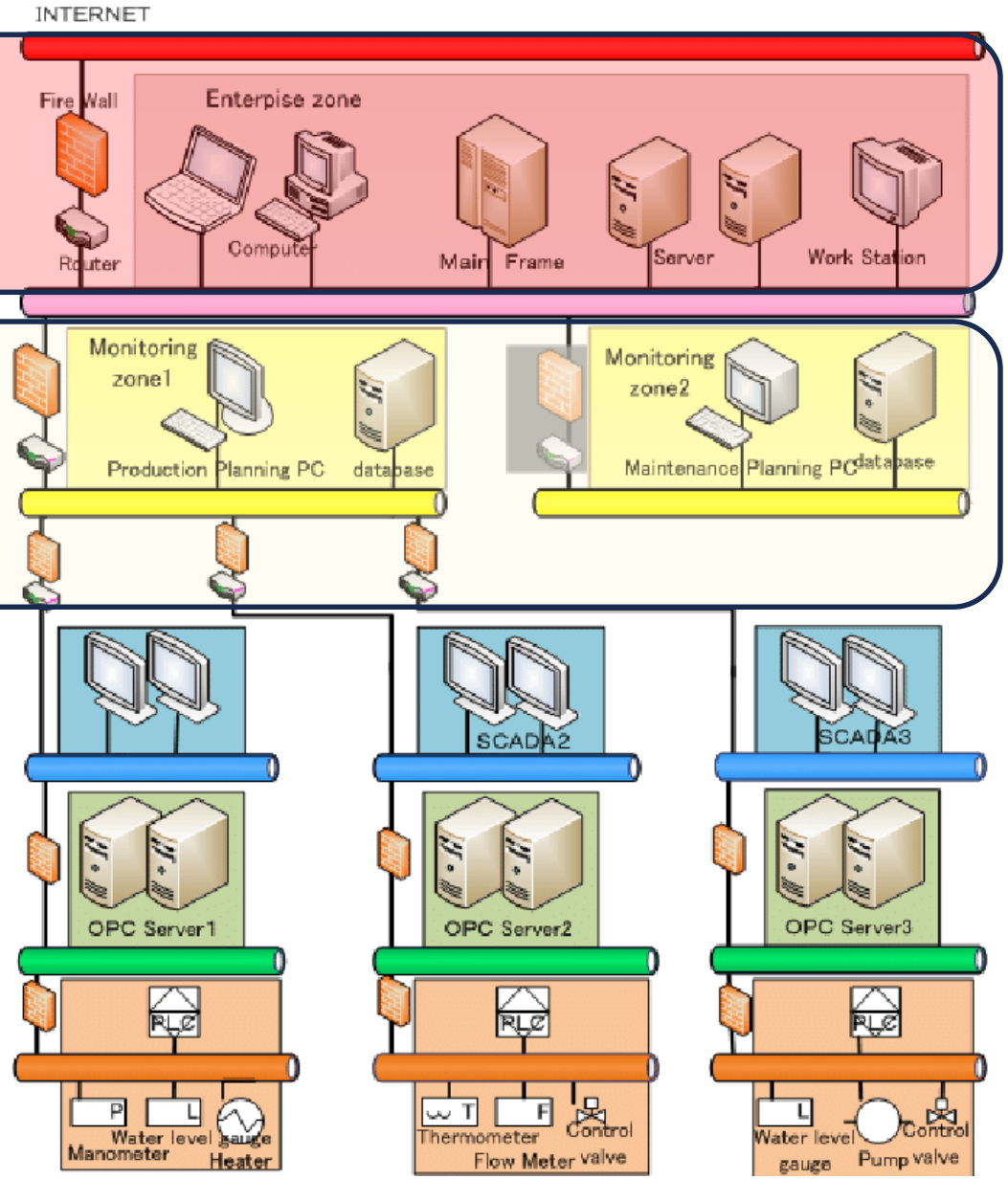
Alinet

Level 4

- **ENTERPRISE ZONE**

DMZ

- **DMZ ZONE**



Alinet

Level 4

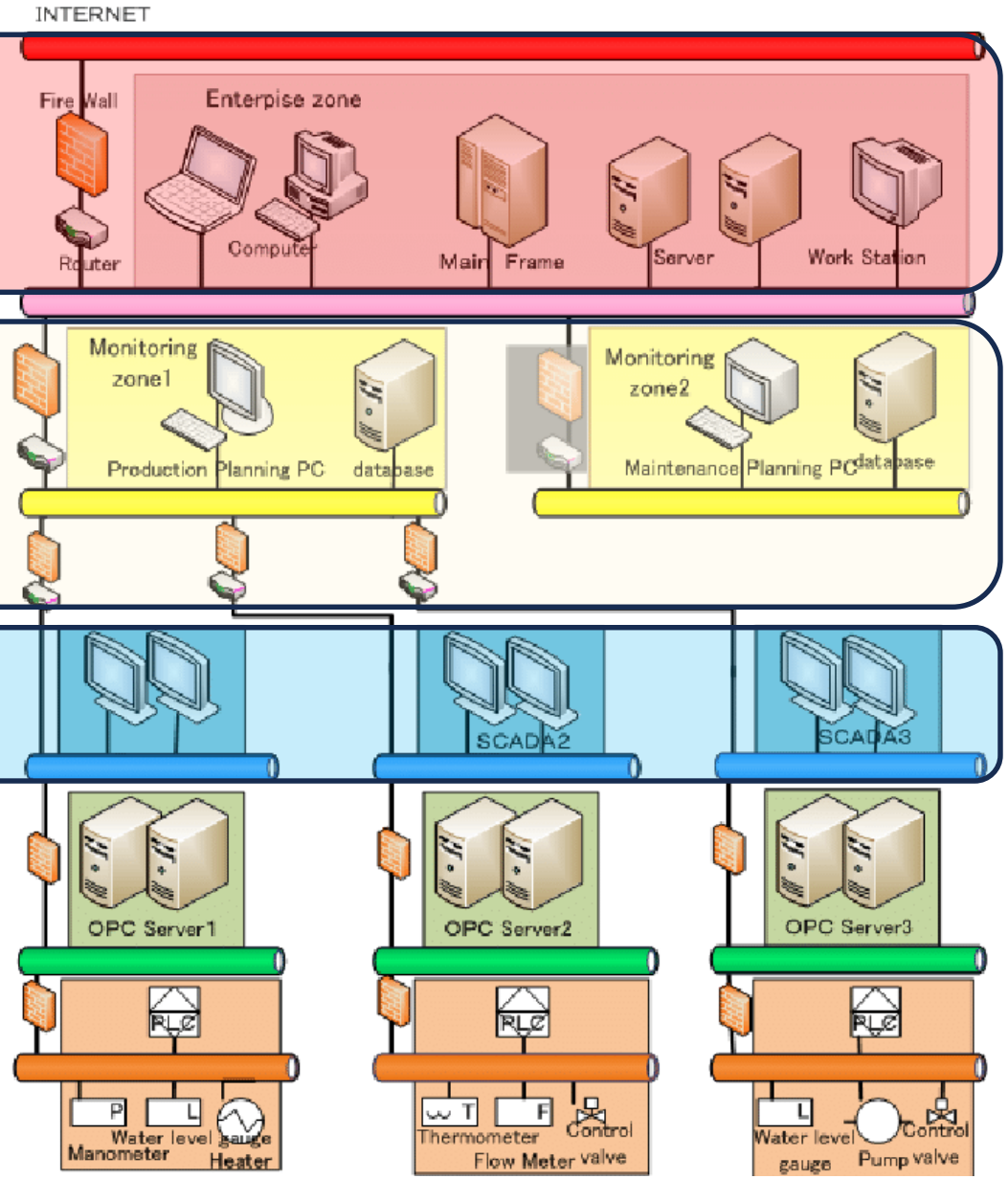
- ENTERPRISE ZONE

DMZ

- DMZ ZONE

Level 3

- OPERATION ZONE



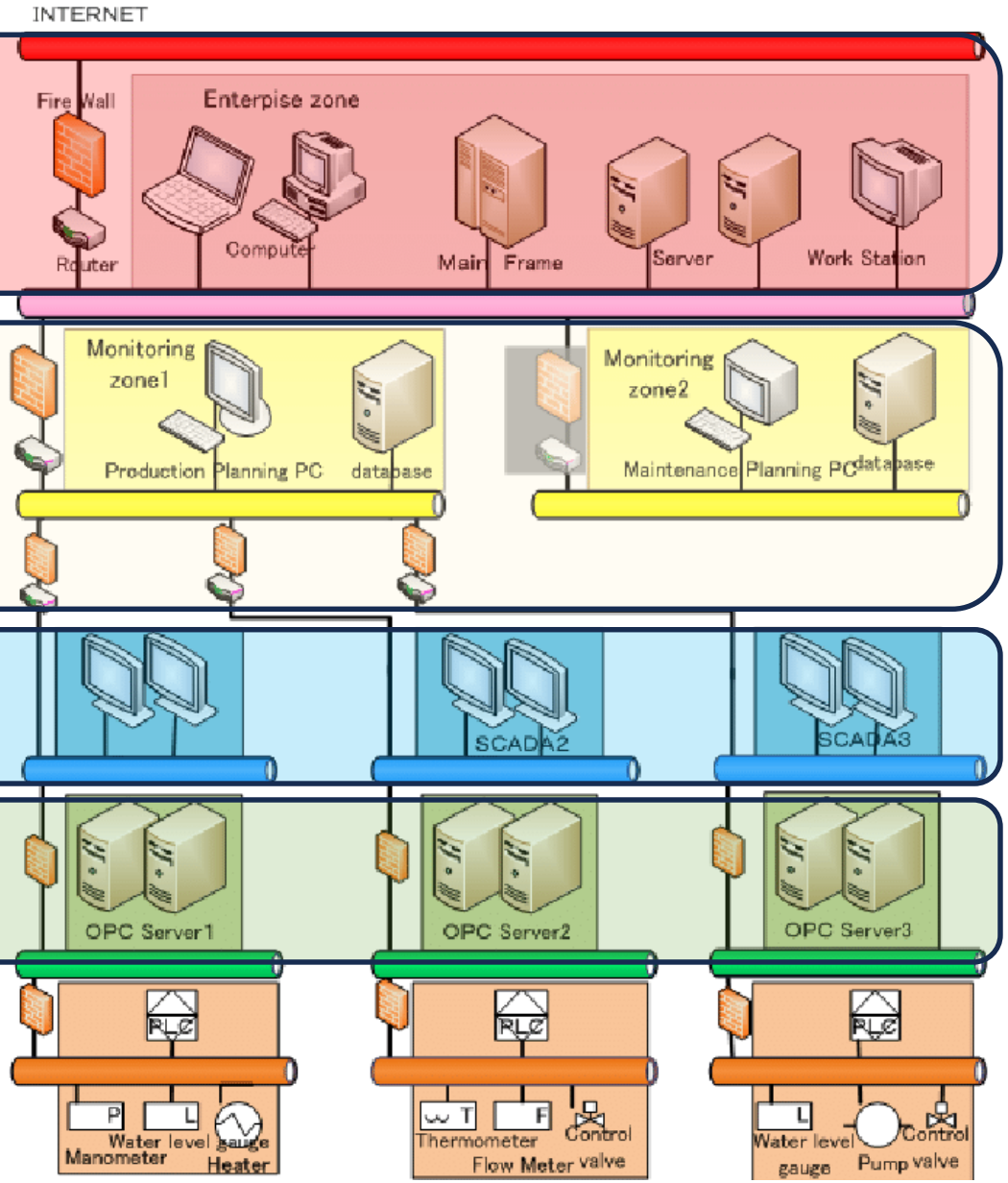
Alinet

Level 4
- ENTERPRISE ZONE

DMZ
- DMZ ZONE

Level 3
- OPERATION ZONE

Level 2
- SUPERVISOR ZONE



Alinet

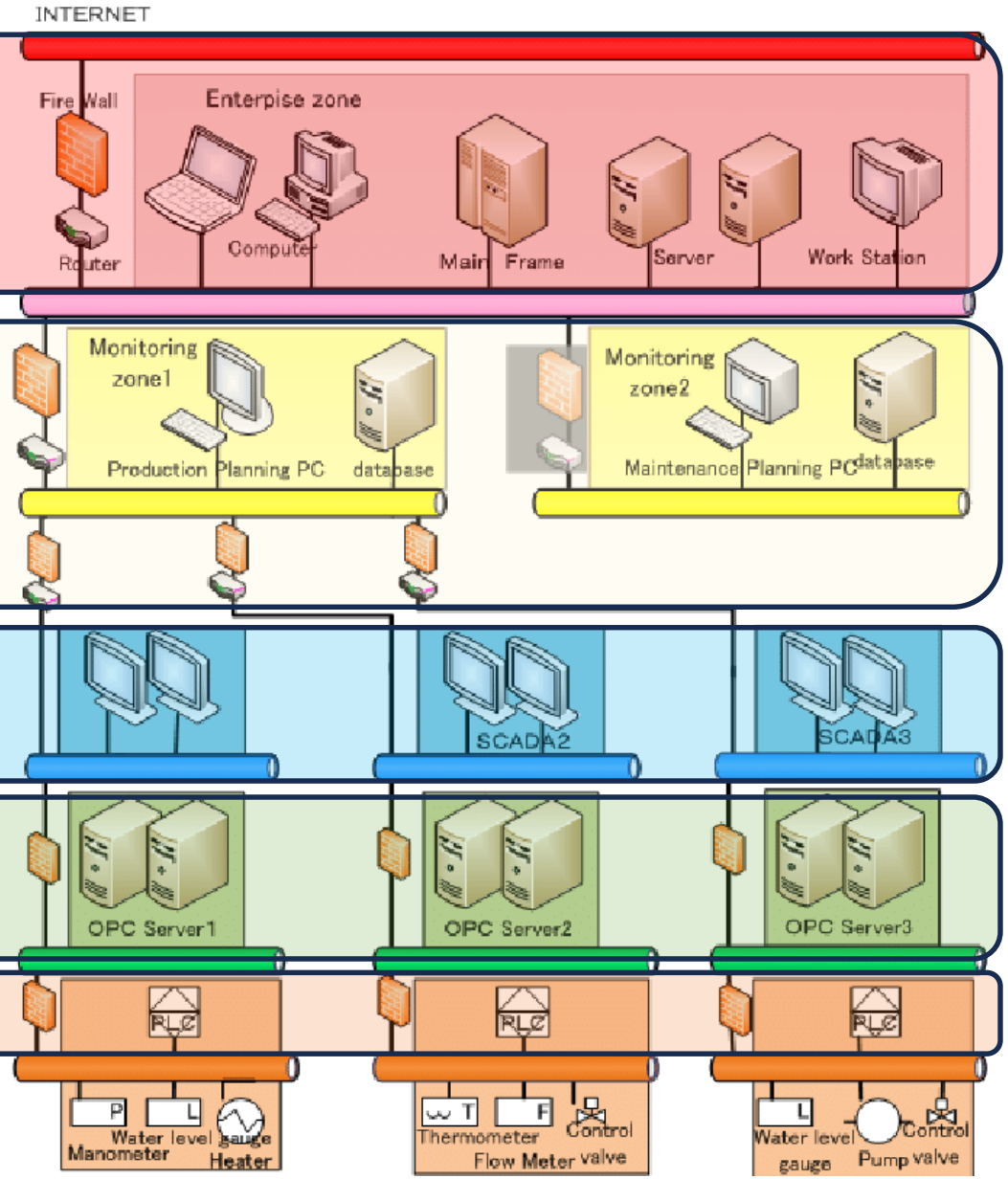
Level 4
- ENTERPRISE ZONE

DMZ
- DMZ ZONE

Level 3
- OPERATION ZONE

Level 2
- SUPERVISOR ZONE

Level 1 BASIC CONTROL ZONE



Alinet

Level 4
- ENTERPRISE ZONE

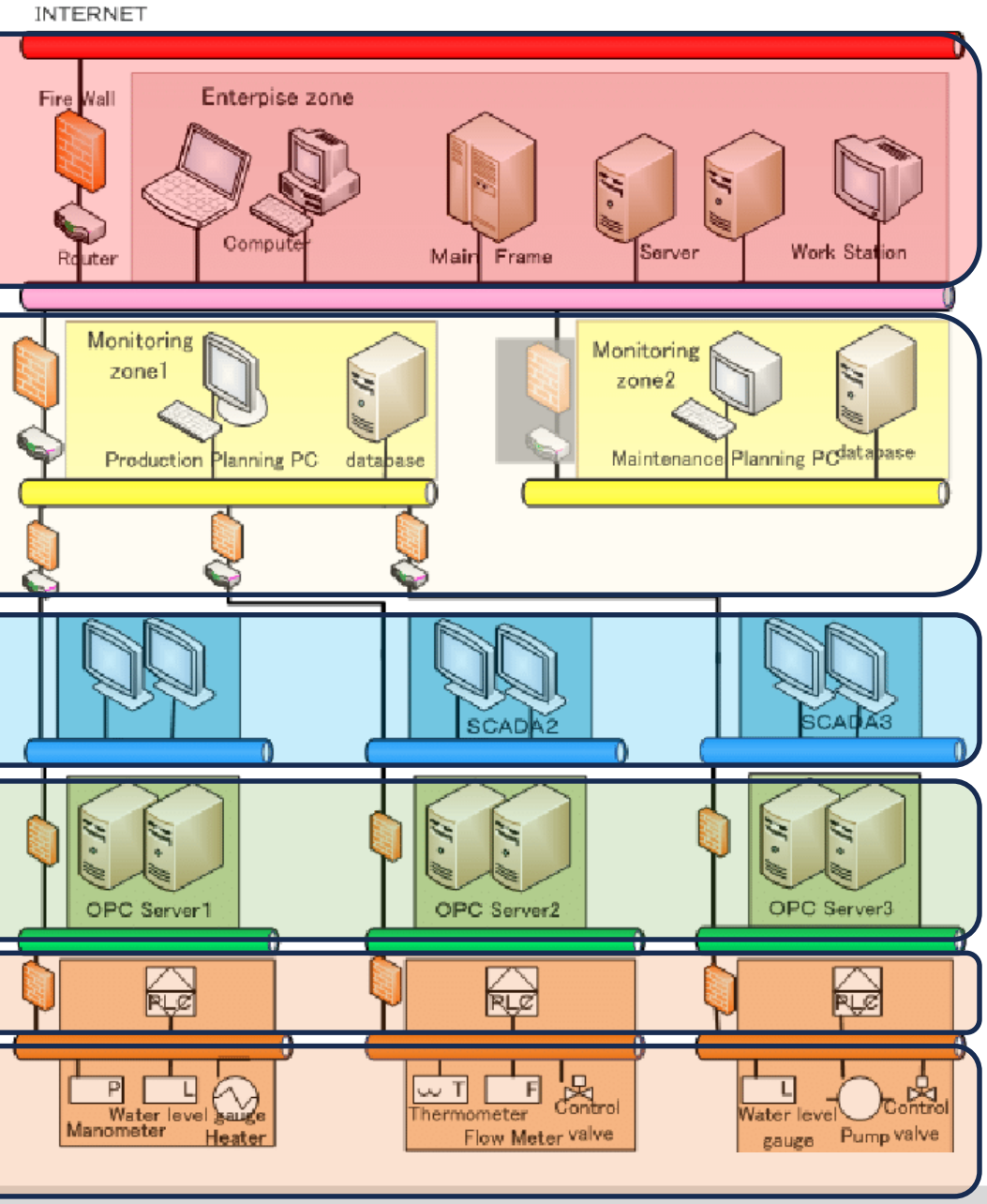
DMZ
- DMZ ZONE

Level 3
- OPERATION ZONE

Level 2
- SUPERVISOR ZONE

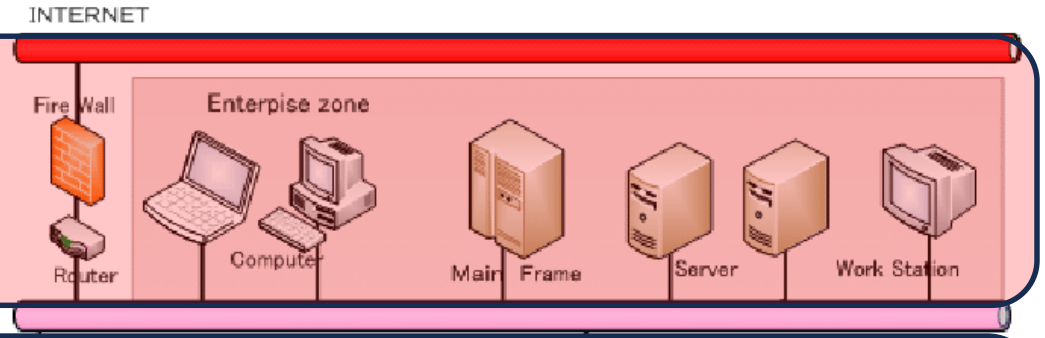
Level 1 BASIC CONTROL ZONE

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



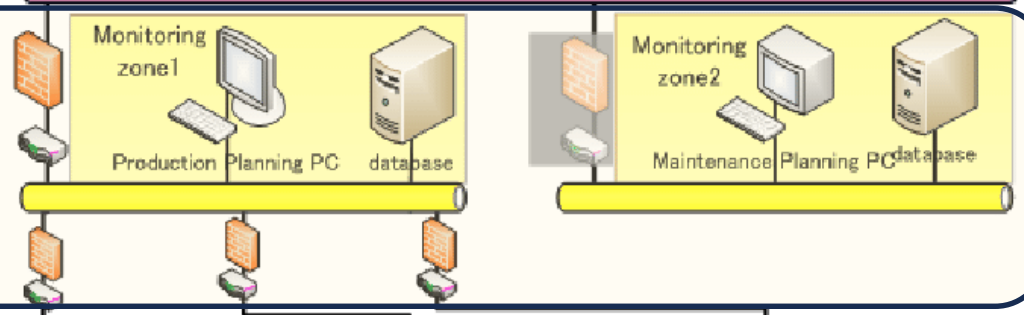
IT ZONE

Level 4
- ENTERPRISE ZONE



DMZ ZONE

DMZ
- DMZ ZONE

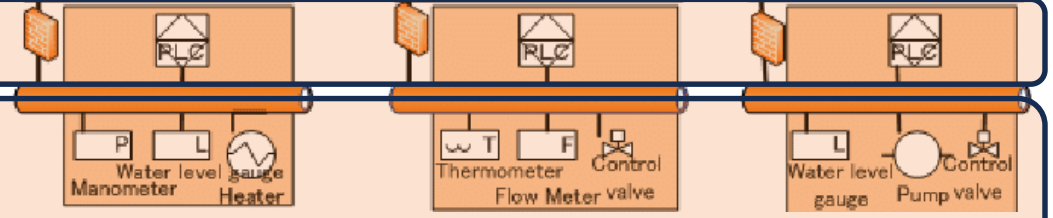


CONTROL ZONE

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

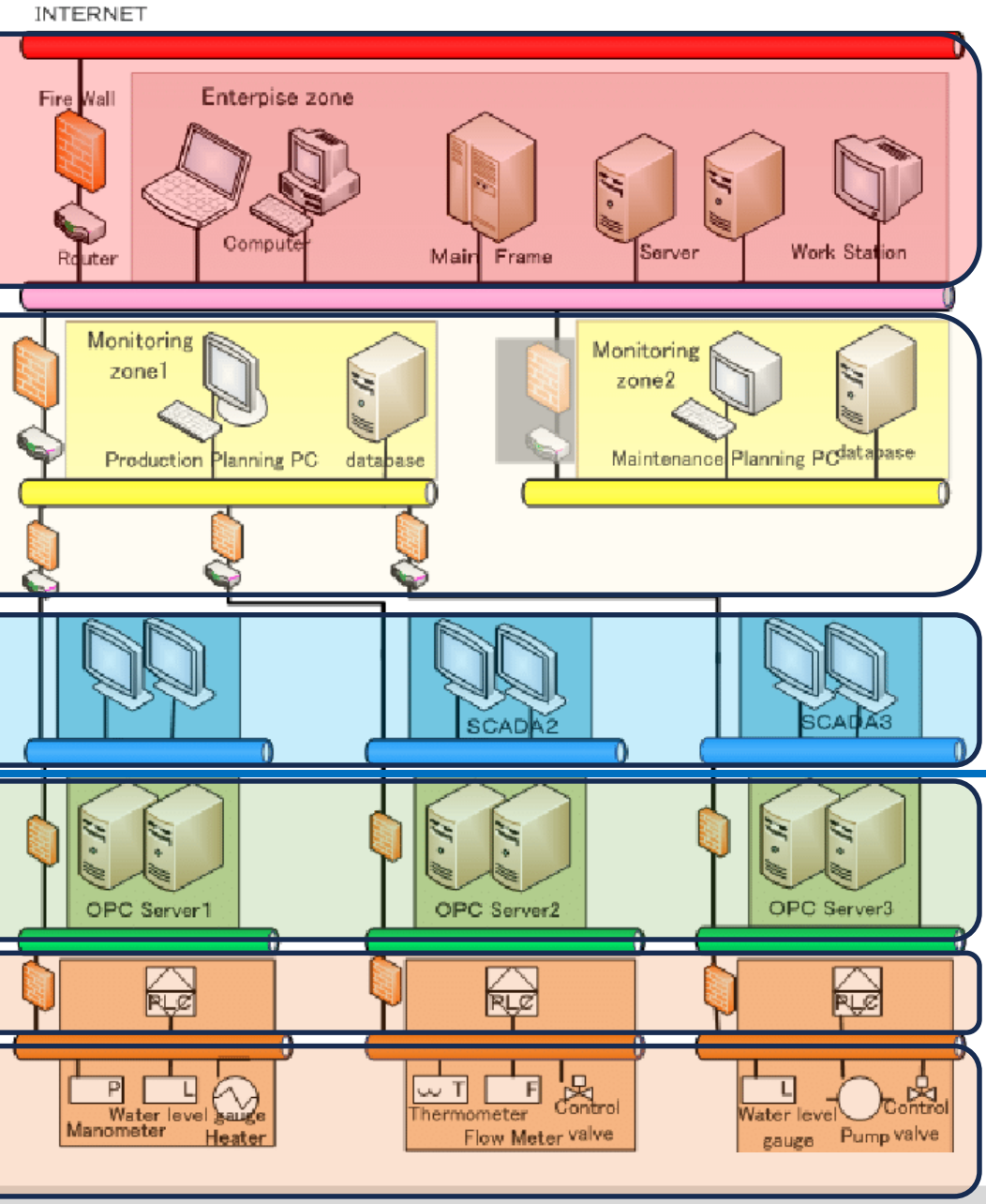
DMZ
- DMZ ZONE

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

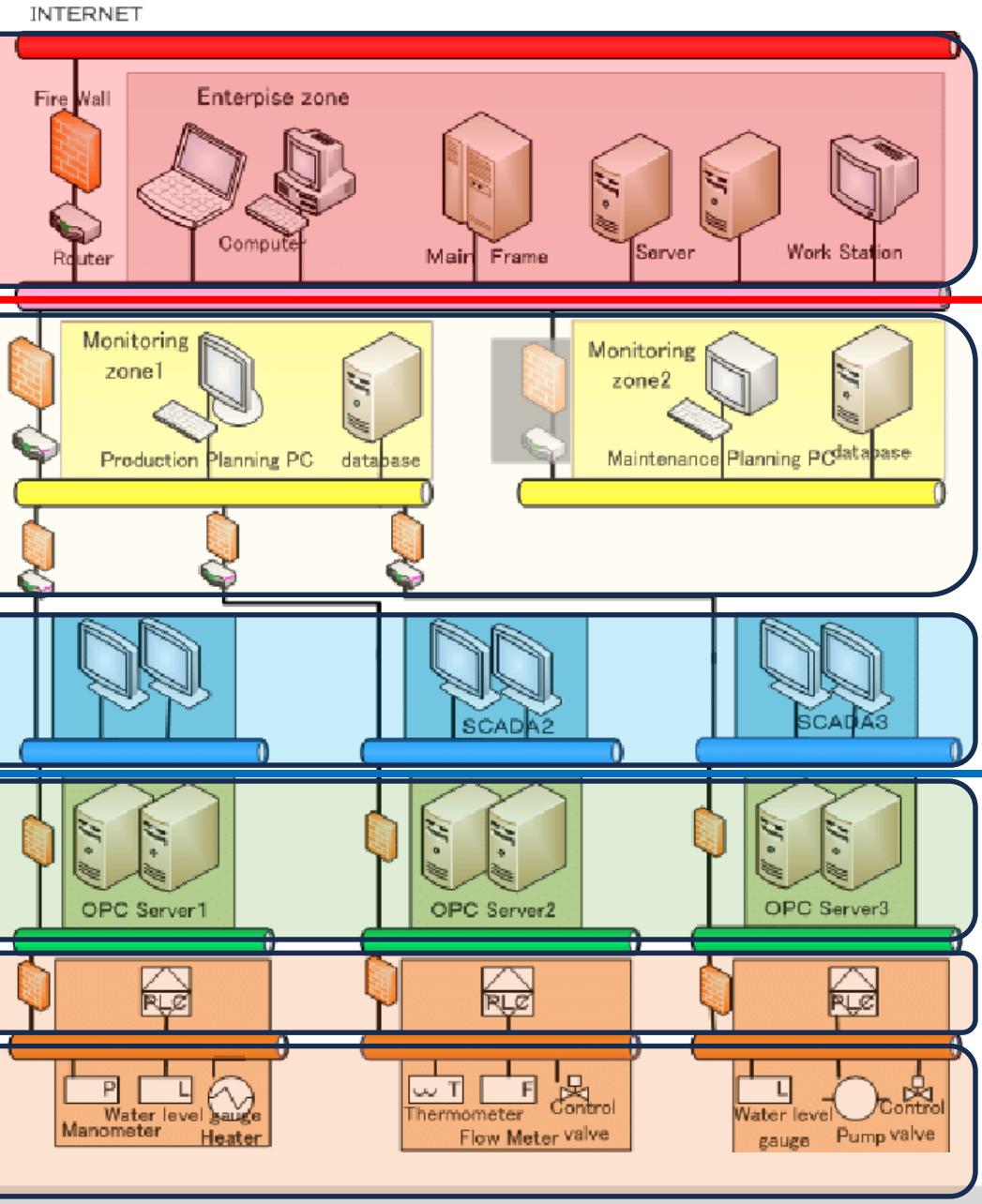
DMZ
- DMZ ZONE

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

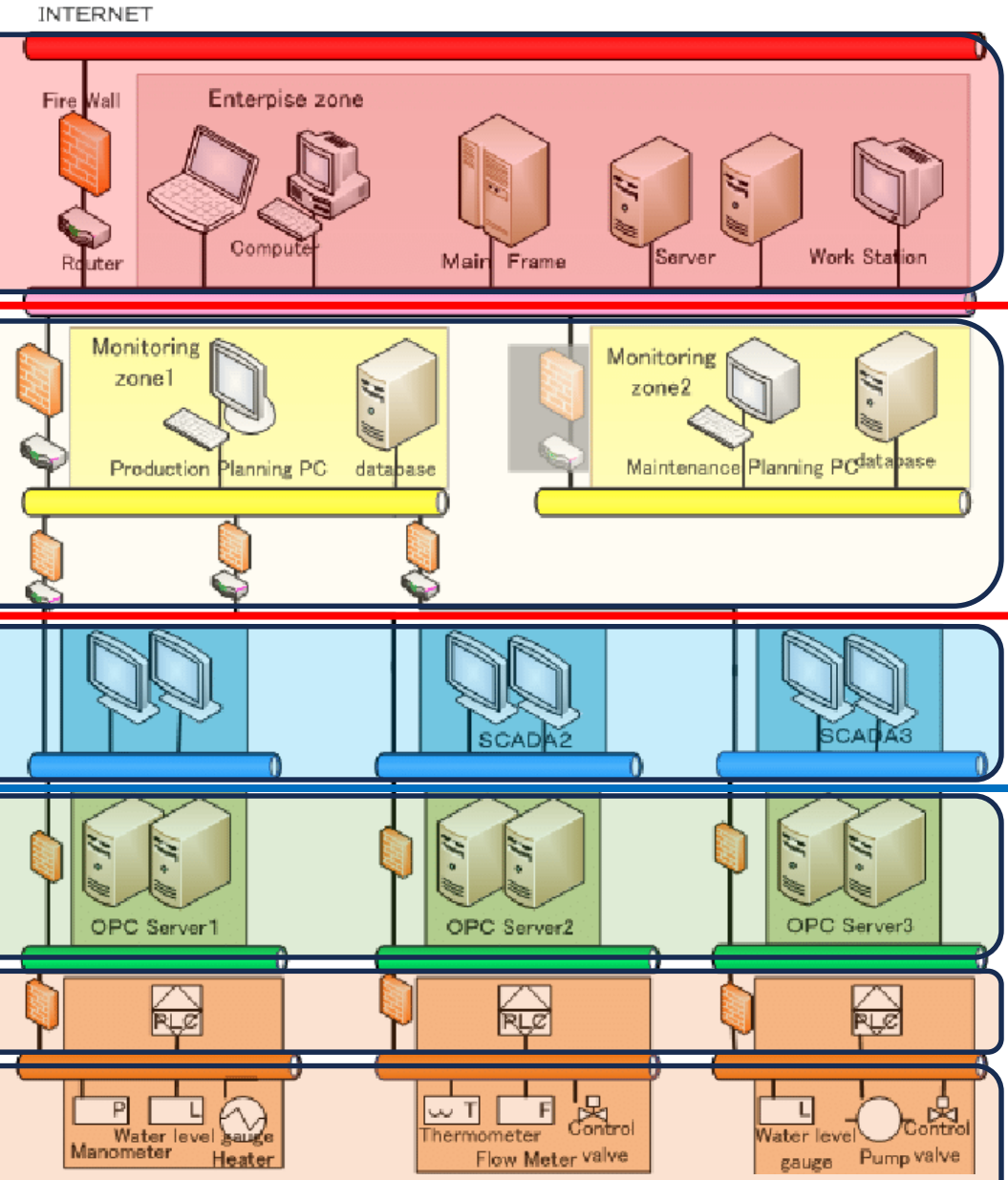
DMZ
- DMZ ZONE

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

Jak opravdu začít ?

Alinet

Ochrana perimetru

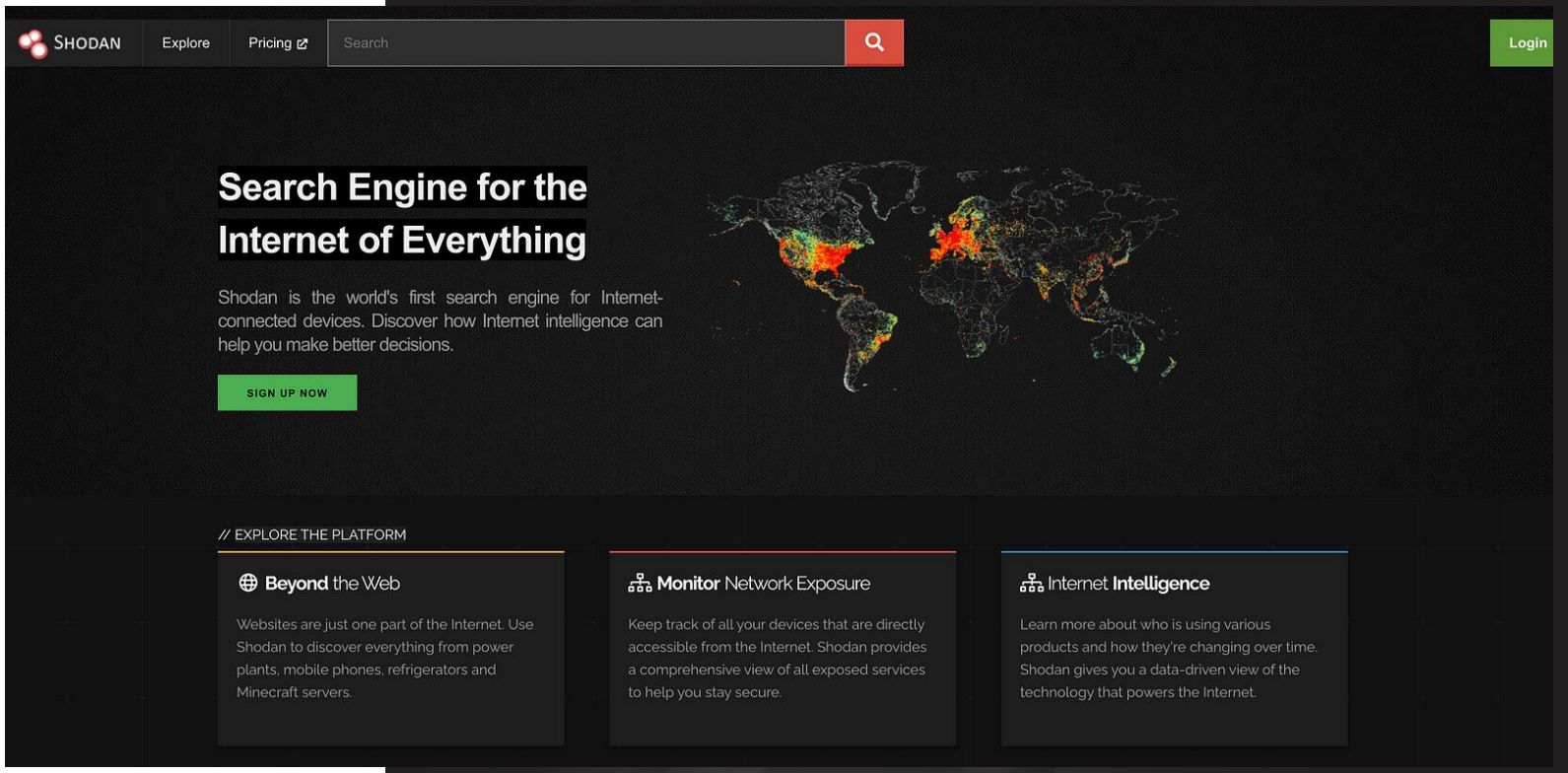
Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

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

Alinet

Alinet

Shodan.io



Zdroj: https://www.shodan.io/

Alinet

Potřebujete pomoci ?

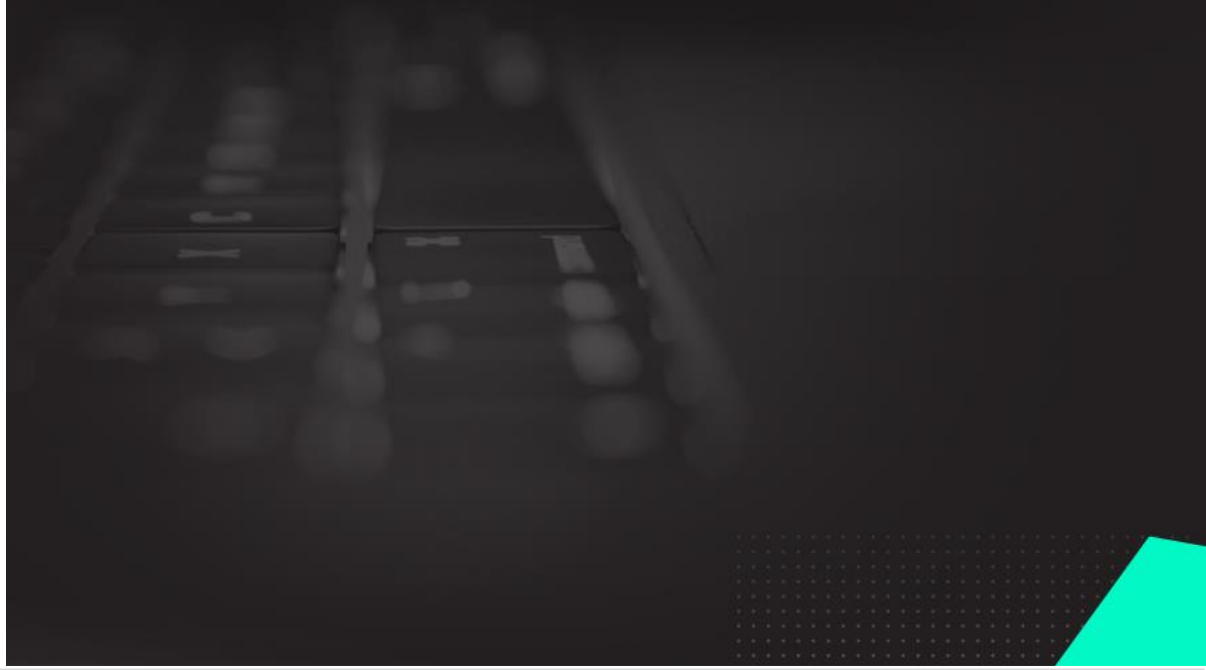
Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

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 spojime se s Vami
- ✓ 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

Bezpečnostní upozornění na závěr

Alinet

FORTINET®

15.1.2025

Password DUMP

Authentication bypass
CVE-2024-55591

- ✓ 15 474 Fortigate celý svět (136 CZ a 11 SK)
- ✓ Seznam je už z roku 2022 !!
  - ✓ založený na zranitelnosti CVE-2022-40684
  - ✓ Aktualizovaný 1/2024
  - ✓ Seřazen podle zemí RU
- ✓ Uživatelské jména
- ✓ Hesla (samozřejmě v plaintextu)
- ✓ Full config fortigate (včetně certifikátů)

Zdroj: https://www.heise.de/en/news/Unknown-group-releases-Fortinet-config-files-and-VPN-passwords-to-the-darknet-10244238.html

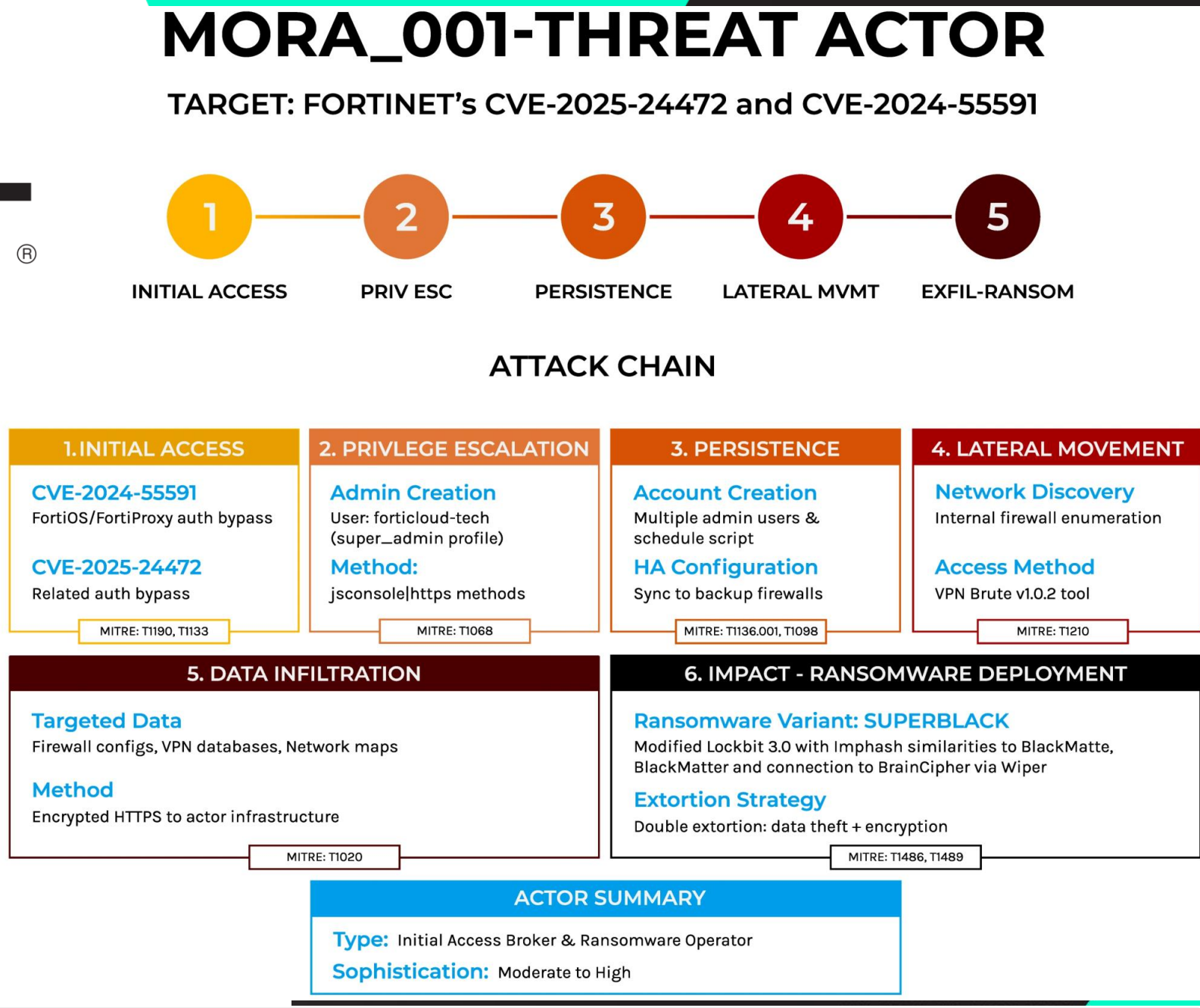
Alinet

FORTINET

15.1.2025

Password DUMP

Authentication bypass
CVE-2024-55591



Zdroj: https://www.heise.de/en/news/Unknown-grou
releases-Fortinet-config-files-and-VPN-passwords-t
darknet-10244238.html

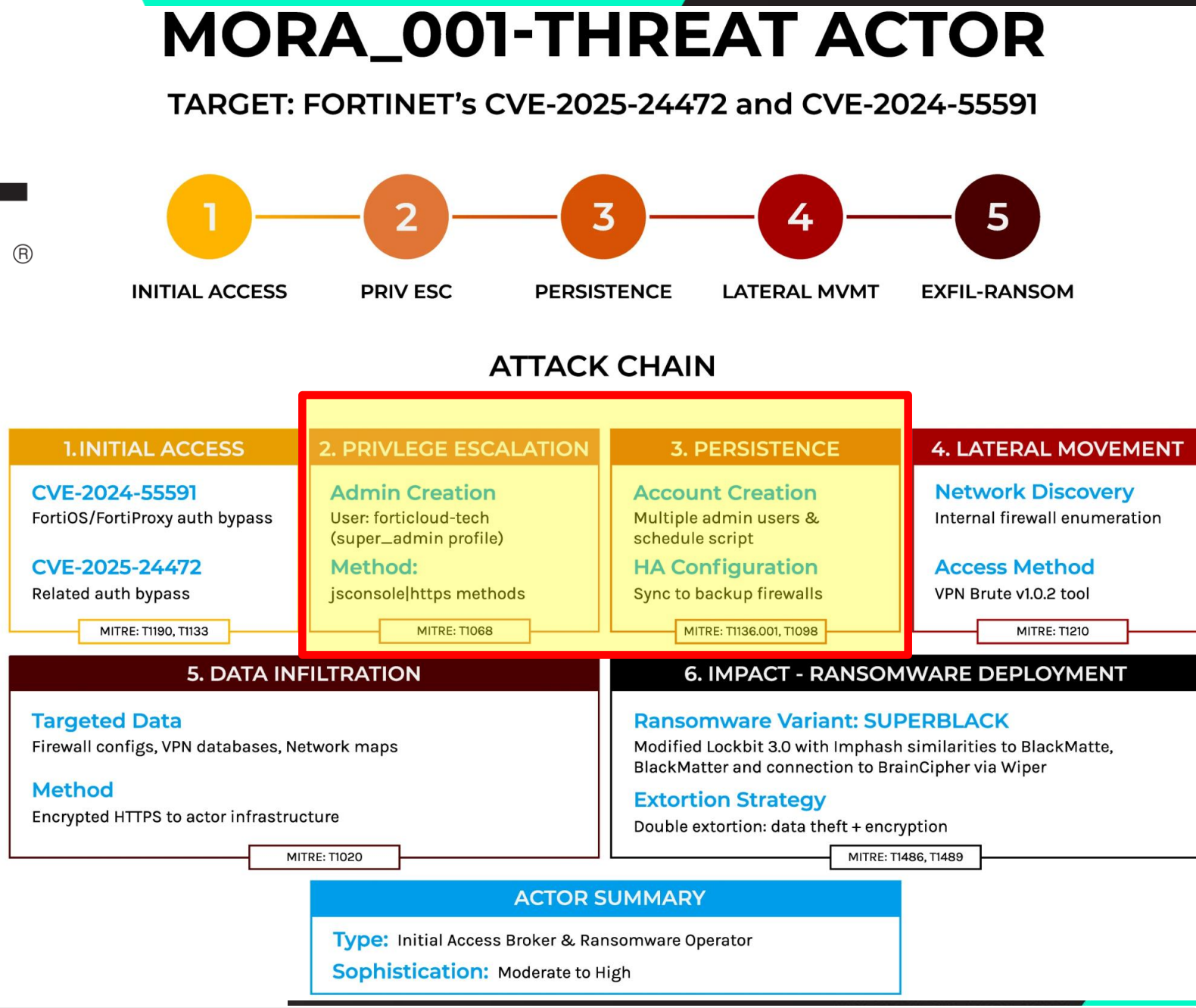
Alinet

FORTINET

15.1.2025

Password DUMP

Authentication bypass
CVE-2024-55591



Zdroj: https://www.heise.de/en/news/Unknown-group releases-Fortinet-config-files-and-VPN-passwords-to darknet-10244238.html

Alinet

Cyber Security, **Ransomware Incident Response**

Jakub Alimov

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