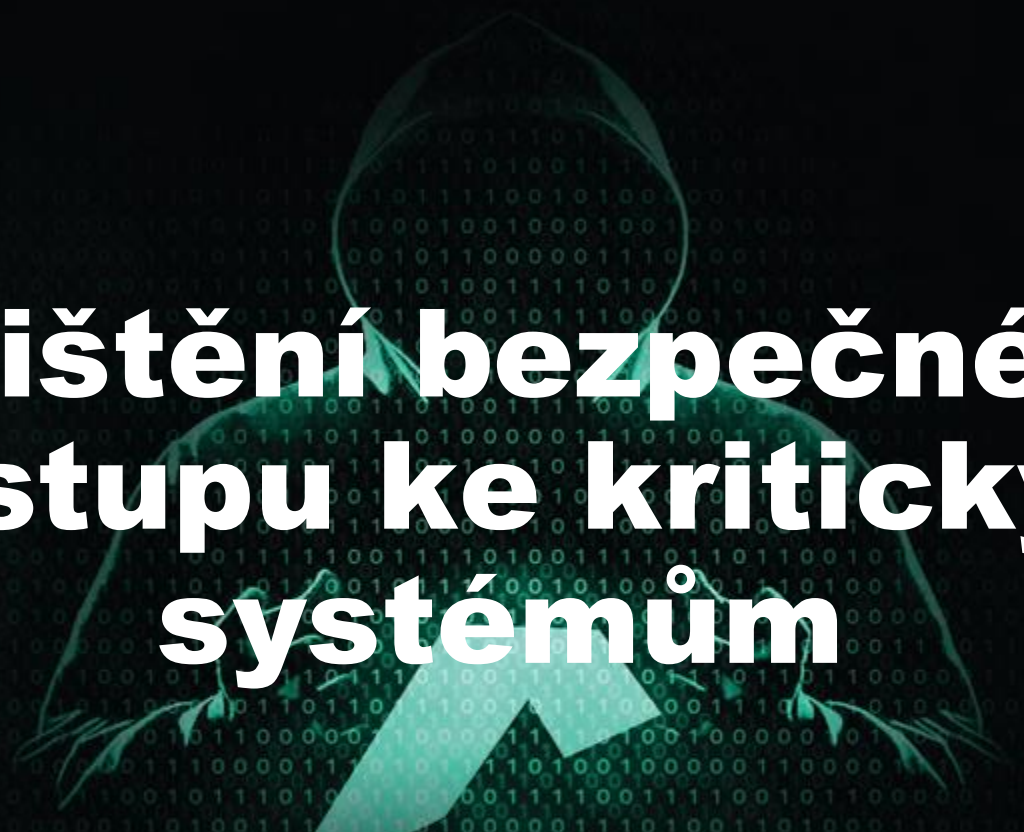
Alinet



Zajištění bezpečného přístupu ke kritickým systémům

19.11.2025

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

Kdo jsem?

Alinet

Kdo jsem?

Jakub Alimov, CEH, CHFI

Lead Auditor

architekt kybernetické bezpečnosti,

RANSOMWARE hunter,

konzultant informační bezpečnosti,

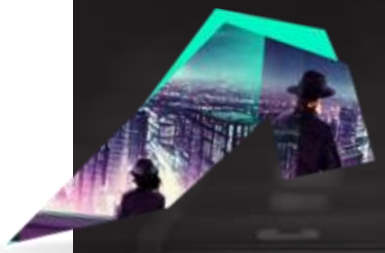
více jak 15+ let prokazatelných zkušeností s kybernetickou bezpečností

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

Alinet

Kdo je Alinet?

Alinet



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

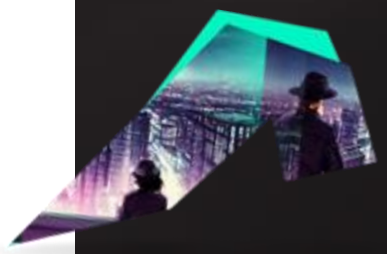
SLUŽBY KYBERNETICKÉ BEZPEČNOSTI

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

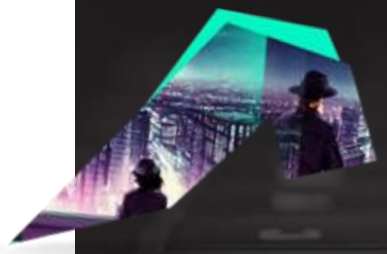
Alinet

Jsme progresivní IT firma se specializací na kybernetické útoky.



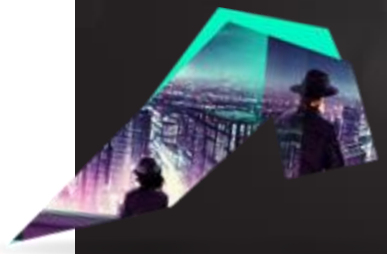
DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ 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

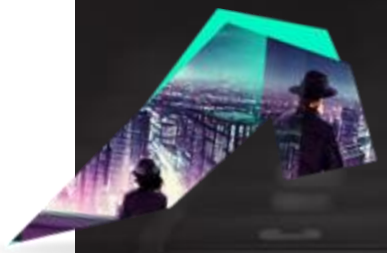
mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Jsme progresivní IT firma se specializací na kybernetické útoky.

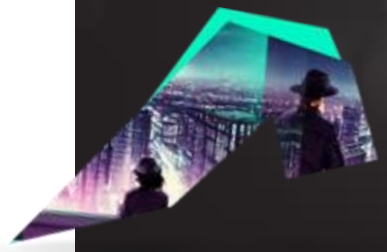
DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ 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

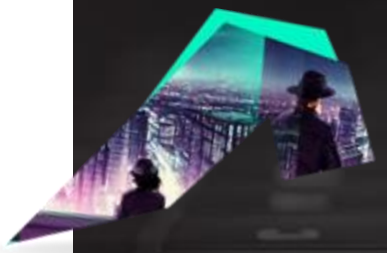
mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Alinet

Jsme progresivní IT firma se specializací na kybernetické útoky.

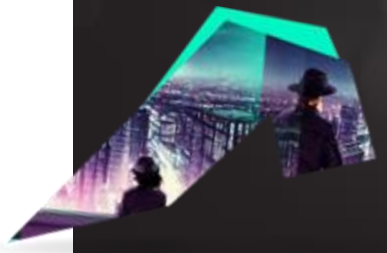
DIGITAL FORENSICS AND INCIDENT RESPONSE

- ✓ 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

Z reálných útoků 2025

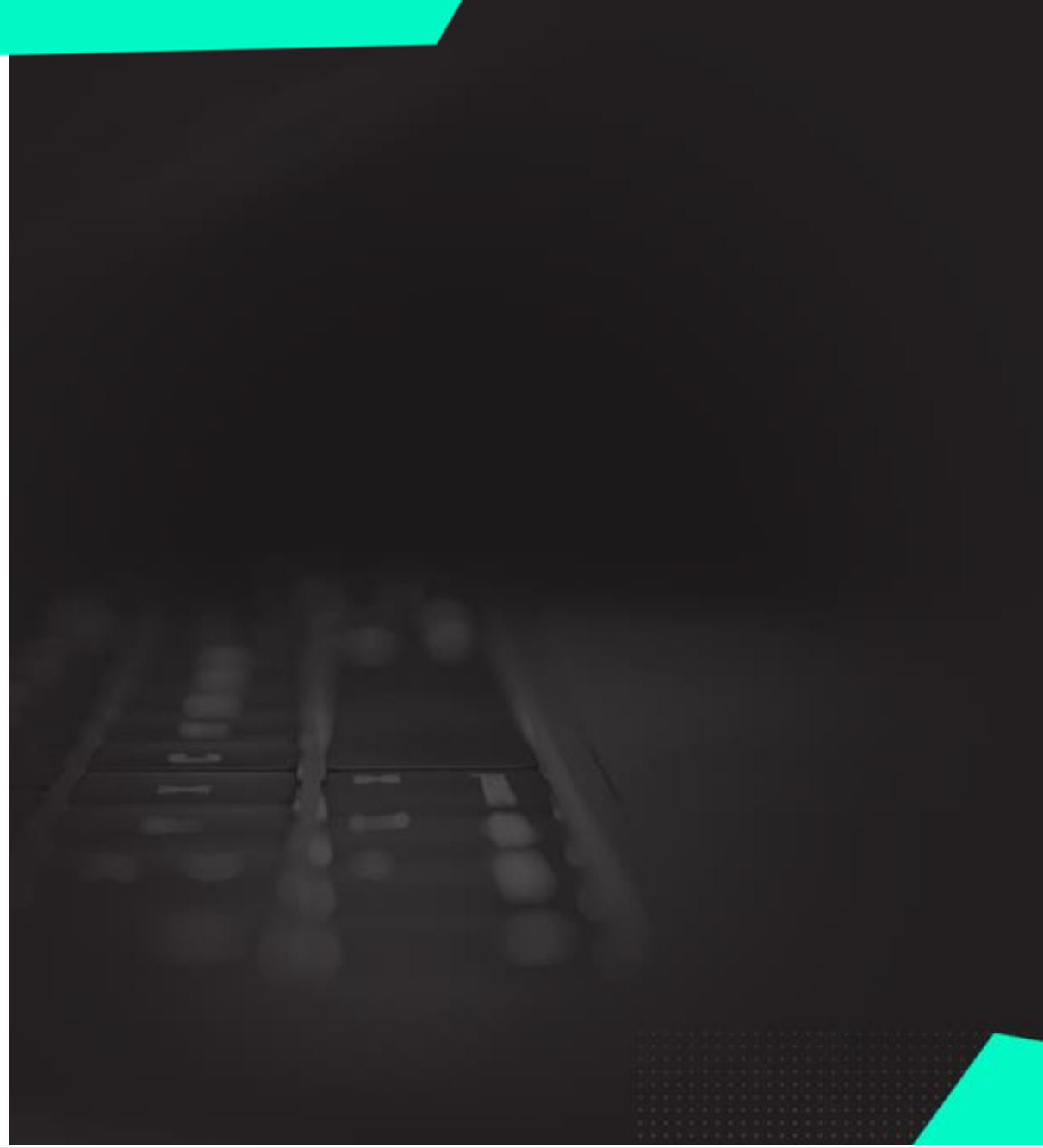
Alinet CZ s.r.o. Pod Hájkem 406/1a, Praha 8, 180 00, CZ

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

Alinet

Reálné útoky v roce 2025?

Skutečné příběhy z forenzního vyšetřování.



Reálné útoky v roce 2025?

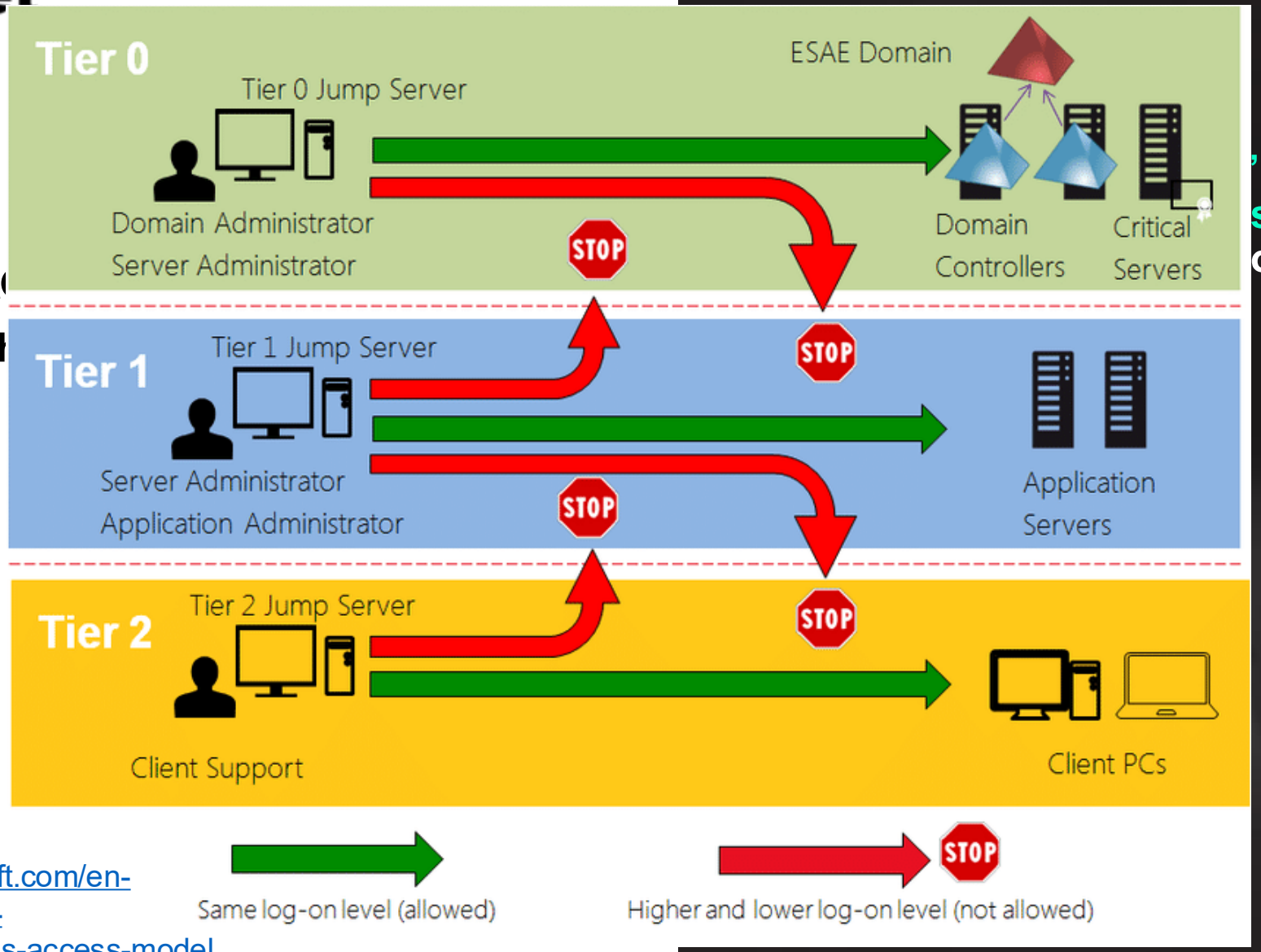
Skutečné příběhy z forenzního vyšetřování.

✓ **Nesegmentovaná síť s zneužití doménového administrátora mělo za důsledek nedostupnost několik měsíců**

Alinet

Reálné úto

Skutečné příběh



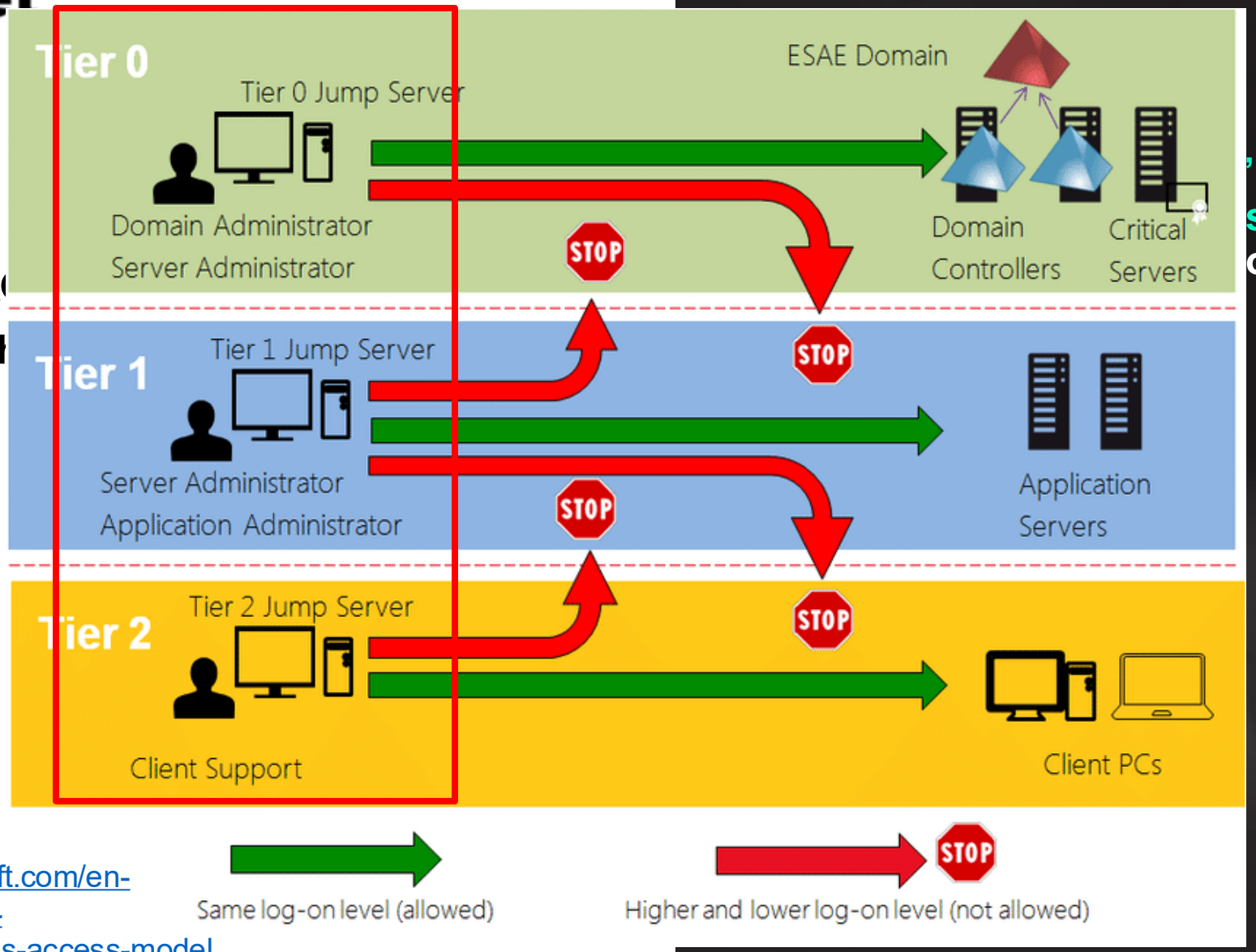
’ s zneužití
strátora mělo za
ost několik měsíců

ZDROJ: https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model

Alinet

Reálné úto

Skutečné příběh



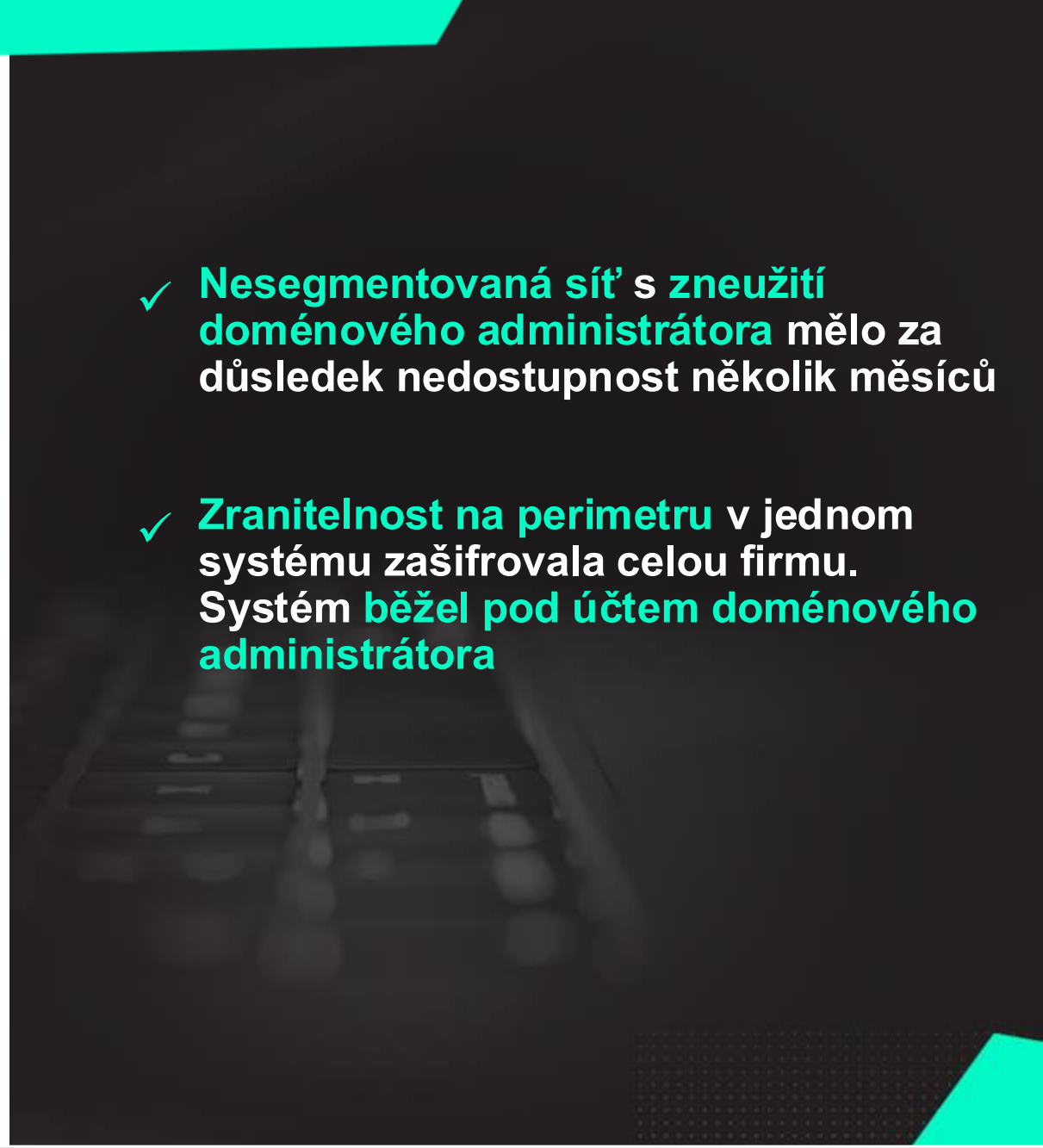
’ s zneužití
strátora mělo za
ost několik měsíců

ZDROJ: https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model

Alinet

Reálné útoky v roce 2025?

Skutečné příběhy z forenzního vyšetřování.



- ✓ **Nesegmentovaná síť** s **zneužití doménového administrátora** mělo za důsledek nedostupnost několik měsíců
- ✓ **Zranitelnost na perimetru** v jednom systému zašifrovala celou firmu. Systém **běžel pod účtem doménového administrátora**

Alinet

Reálné útoky v roce 2025?

✓ **Nesegmentovaná síť s zneužití doménového administrátora mělo za důsledek nedostupnost několik měsíců**

Appendix F: Securing Domain Admins Groups in Active Directory

As is the case with the Enterprise Admins (EA) group, membership in the Domain Admins (DA) group should be required only in build or disaster recovery scenarios. There should be no day-to-day user accounts in the DA group with the exception of the built-in Administrator account for the domain, if it has been secured as described in Appendix D: Securing Built-In Administrator Accounts in Active Directory.

ZDROJ: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-f--securing-domain-admins-groups-in-active-directory

Alinet

Reálné útoky v roce 2025?

✓ **Nesegmentovaná síť s zneužití doménového administrátora mělo za důsledek nedostupnost několik měsíců**

Appendix F: Securing Domain Admins Groups in Active Directory

As is the case with the Enterprise Admins (EA) group, membership in the Domain Admins (DA) group should be required only in build or disaster recovery scenarios. There should be no day-to-day user accounts in the DA group with the exception of the built-in Administrator account for the domain, if it has been secured as described in Appendix D: Securing Built-In Administrator Accounts in Active Directory.

ZDROJ: https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-f--securing-domain-admins-groups-in-active-directory

Alinet

Reálné útoky v roce 2025?

Skutečné příběhy z forenzního vyšetřování.

- ✓ **Nesegmentovaná síť** s **zneužití doménového administrátora** mělo za důsledek nedostupnost několik měsíců
- ✓ **Zranitelnost na perimetru** v jednom systému zašifrovala celou firmu. Systém **běžel pod účtem doménového administrátora**
- ✓ **Neaktualizovaný systém** umožnil přístup komukoliv do interní firemní sítě **bez hesla**

Alinet

Reálné útoky v ro

Skutečné příběhy z forenzní

Microsoft Exchange

Nesegmentovaná síť s zneužití
dministrátora mělo za
stupnost několik měsíců

perimetru v jednom
ovala celou firmu.
od účtem doménového

ný systém umožnil
oliv do interní firemní

Alinet

Reálné útoky v roce 2025?

Skutečné příběhy z forenzního vyšetřování.

- ✓ **Nesegmentovaná síť** s **zneužití doménového administrátora** mělo za důsledek nedostupnost několik měsíců
- ✓ **Zranitelnost na perimetru** v jednom systému zašifrovala celou firmu. Systém **běžel pod účtem doménového administrátora**
- ✓ **Neaktualizovaný systém** umožnil přístup komukoliv do interní firemní sítě **bez hesla**

Alinet

RANSOMWARE?

RANSOMWARE?

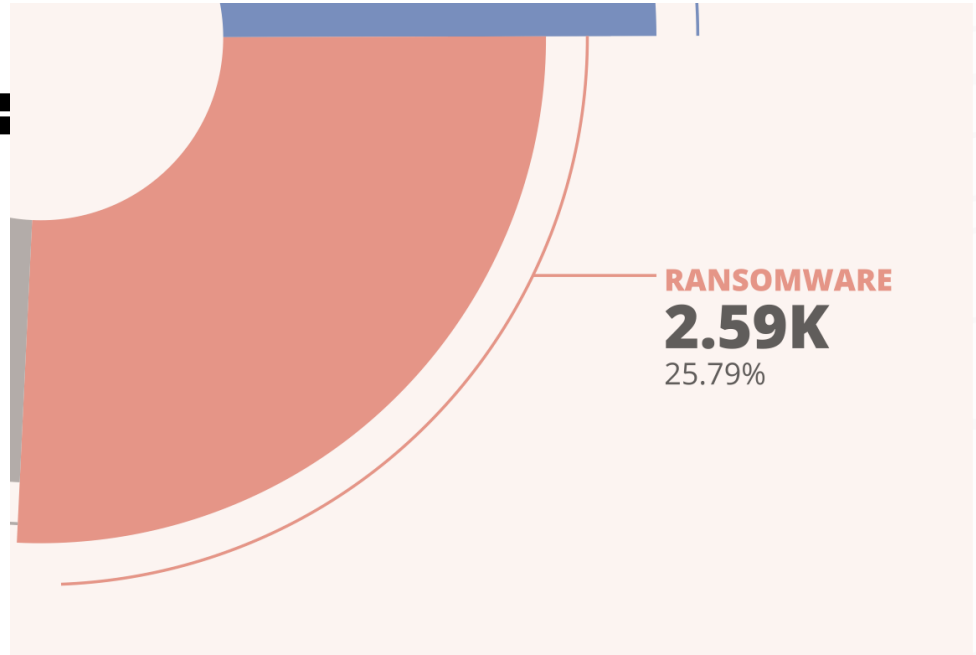
= šance 1 : 4

Zdroj: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf

Alinet

RANSOMWARE?

=



Zdroj: https://www.enisa.europa.eu/sites/default/files/2024-11/2024%20Report%20on%20the%20State%20of%20the%20Cybersecurity%20in%20the%20Union.pdf

Alinet

RANSOMWARE?
Kolik máme času?

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

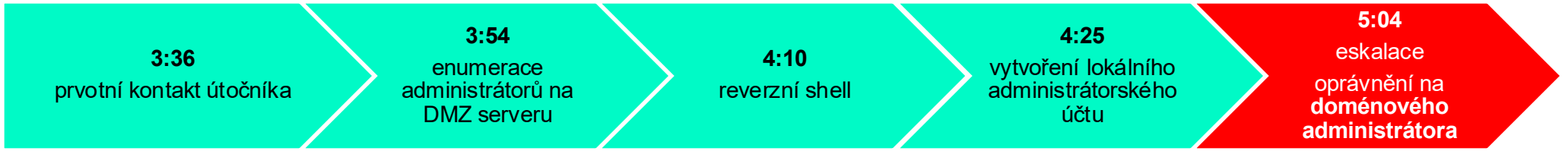
mobil: +420 774 077 108 **e-mail:** info@alinet.cz **web:** www.alinet.cz

Časová osa RANSOMWARE útoku ...

3:36
prvotní kontakt útočníka

Časová osa RANSOMWARE útoku ...

Časová osa RANSOMWARE útoku ...



... ovládnutí sítě trvalo pouhých 88 minut !

Alinet

Časová osa RANSOMWARE útoku ...

... ovládnutí sítě trvalo pouhých 88 minut !

Zpět k zabezpečení privilegovaných účtů …

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

Co jsme udělali …

Alinet

Co jsme udělali

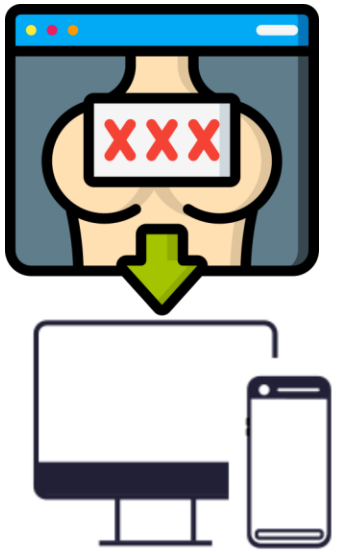
- ✓ **Vzali jsme jednu z TOP PAM na světě**
- ✓ **ODDĚLILI od infrastruktury !**
- ✓ **MAXIMÁLNĚ zahardenovali**
- ✓ **VŠE ENTERPRISTE** (HW, HA, OS, support)
- ✓ **ZAINTEGROVALI service desk** a **Log management**
- ✓ **Dodali naše Know-how z reálných útoků**
- ✓ **VŠE zautomatizovali**
- ✓ **To VŠE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

Alinet

Výstup je APPLIANCE

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

Alinet



DODAVATEL
ADMIN oprávnění

- ✓ **uživatelské jméno**
- ✓ **heslo**

- ✓ **nemáme kontrolu nad …**
- ✓ **… zařízenim**

Firemní VPN server

Interní služby

lokální administrátor

Alinet

DODAVATEL
ADMIN oprávnění

- ✓ **uživatelské jméno**
- ✓ **heslo**

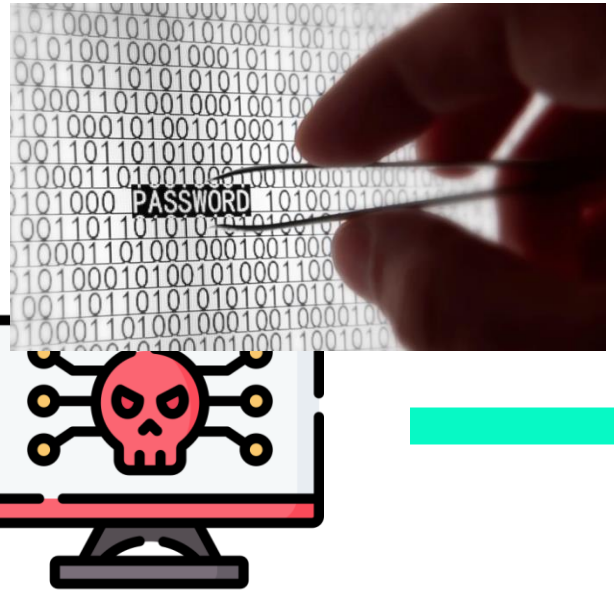
- ✓ **nemáme kontrolu nad …**
- ✓ **… zařízenim**

Firemní VPN server

Interní služby

lokální administrátor

Alinet



DODAVATEL
ADMIN oprávnění

- ✓ uživatelské jméno
- ✓ heslo

- ✓ nemáme kontrolu nad …
- ✓ … zařízenim

VPN

Firemní VPN server

WWW

Interní služby

lokální administrátor

Alinet

Útočník
ADMIN oprávnění

- ✓ uživatelské jméno
- ✓ Heslo
- ✓ ????

Firemní VPN server

Interní služby

lokální administrátor

…88 minut

Alinet

Útočník
ADMIN oprávnění

- ✓ uživatelské jméno
- ✓ Heslo
- ✓ ????

Firemní VPN server

Interní služby

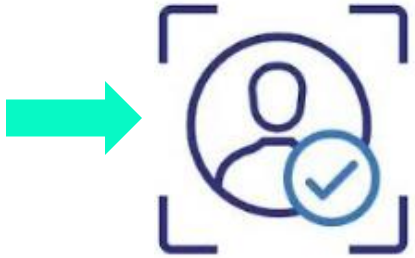
lokální administrátor

…88 minut

Alinet

Jak by to mělo dnes vypadat?

Administrátor nebo dodavatel



Administrátor
nebo dodavatel

PAM appliance

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

Alinet

Administrátor nebo dodavatel

PAM appliance

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

JUMP server

Alinet

Administrátor nebo dodavatel

PAM appliance

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

JUMP server

Interní služby

Alinet

SOC

Administrátor nebo dodavatel

PAM appliance

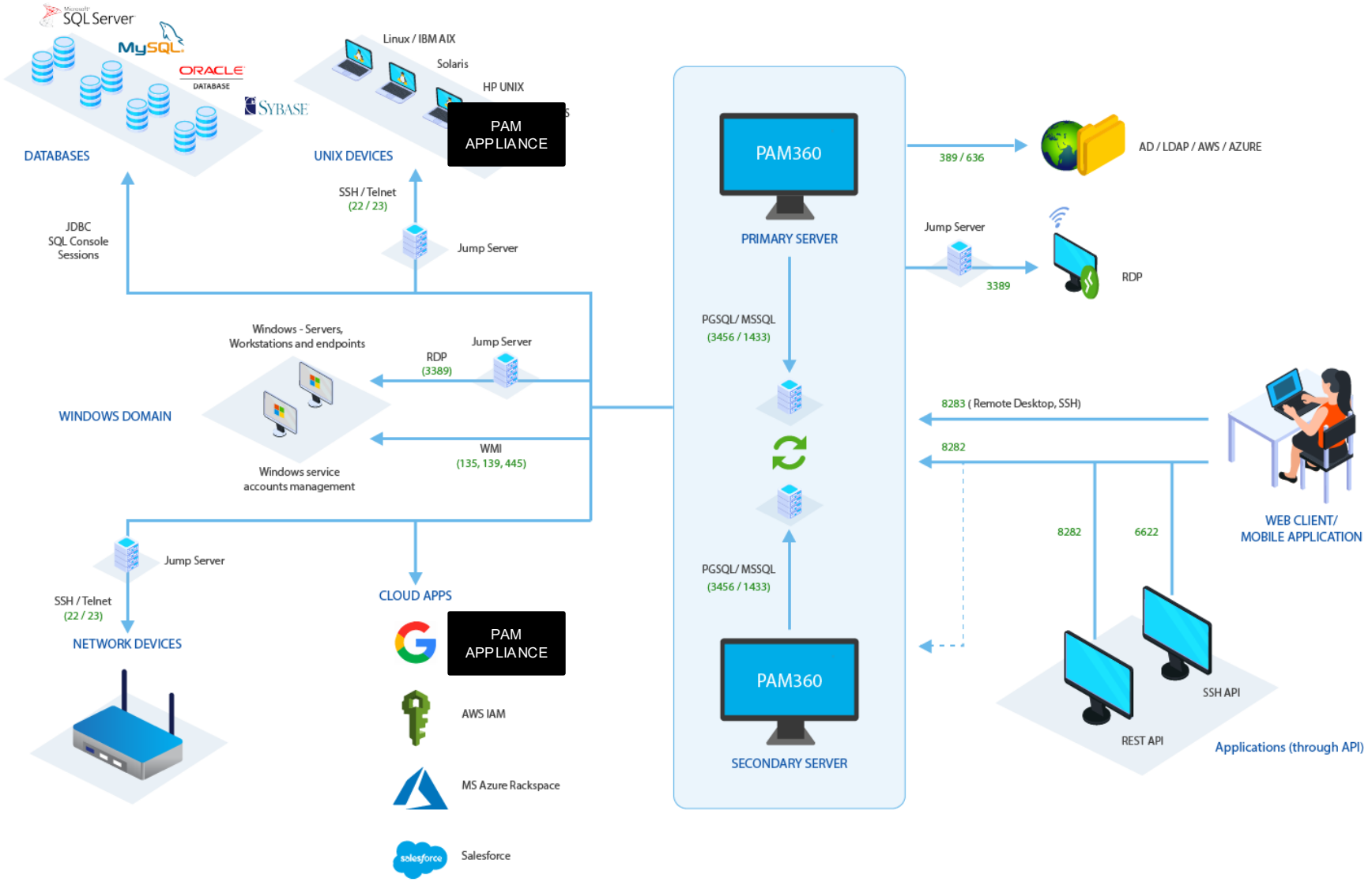
- ✓ MFA ověření
- ✓ Přiřazená role
- ✓ Minimálního oprávnění

JUMP server

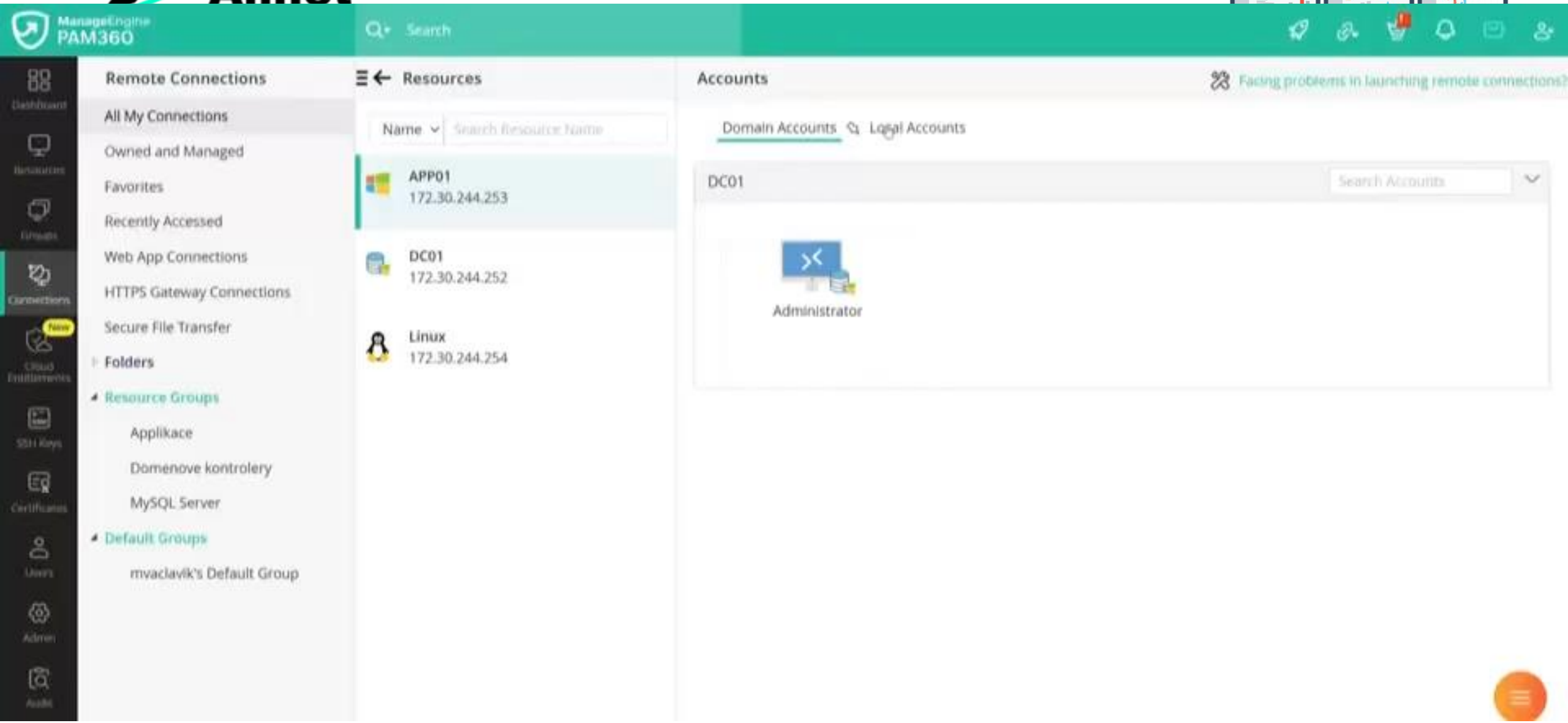
Interní služby

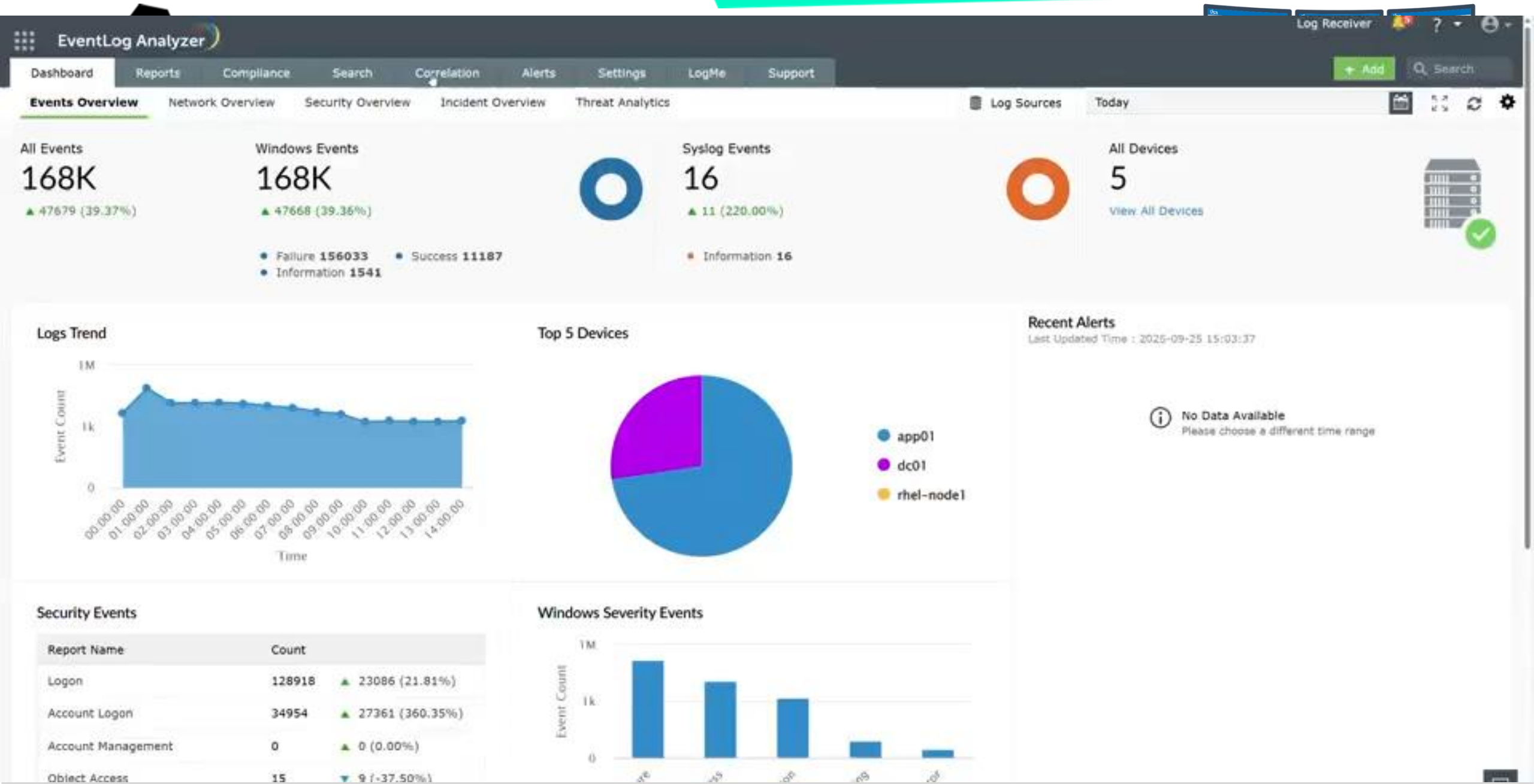
Alinet

PAM360 Architecture diagram



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
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


EventLog Analyzer
Log Receiver
Dashboard
Reports
Compliance
Search
Correlation
Alerts
Settings
LogMe
Support
+ Add
Search
Events Overview
Network Overview
Security Overview
Incident Overview
Threat Analytics
Log Sources
Today
All Events
168K
▲ 47679 (39.37%)
Windows Events
168K
▲ 47668 (39.36%)
Failure 156033
Success 11187
Information 1541
Syslog Events
16
▲ 11 (220.00%)
Information 16
All Devices
5
View All Devices
Logs Trend
1M
1k
0
Event Count
00:00:00
01:00:00
02:00:00
03:00:00
04:00:00
05:00:00
06:00:00
07:00:00
08:00:00
09:00:00
10:00:00
11:00:00
12:00:00
13:00:00
14:00:00
Time
Top 5 Devices
app01
dc01
rhel-node1
Recent Alerts
Last Updated Time : 2025-09-25 15:03:37
No Data Available
Please choose a different time range
Security Events
Report Name
Count
Logon
128918
▲ 23086 (21.81%)
Account Logon
34954
▲ 27361 (360.35%)
Account Management
0
▲ 0 (0.00%)
Object Access
15
▼ 9 (-37.50%)
Windows Severity Events
1M
1k
0
Event Count

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

Cyber Security, **Ransomware Incident Response**

Jakub Alimov

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