

PosAm



Moderné EUS + Bezpečnosť koncových bodov

Ladislav Bogdány, Ľubomír Fačkovec

17.10.2024

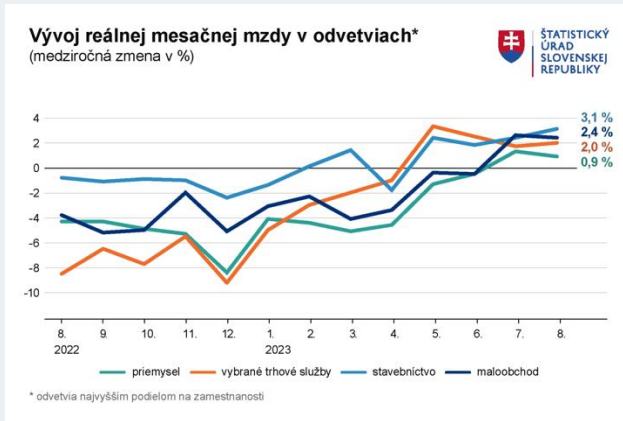
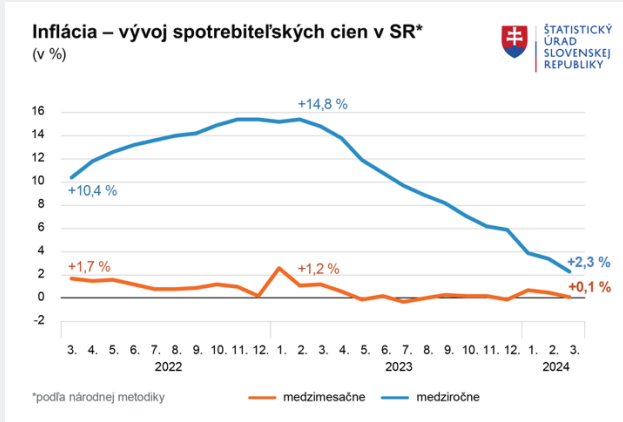


Rozcvička

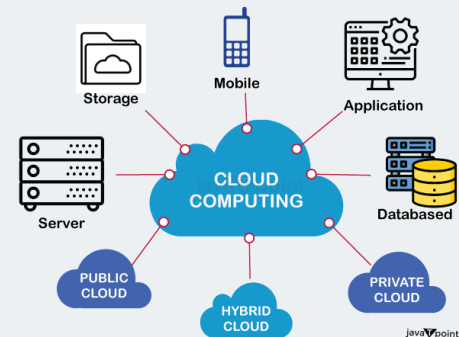
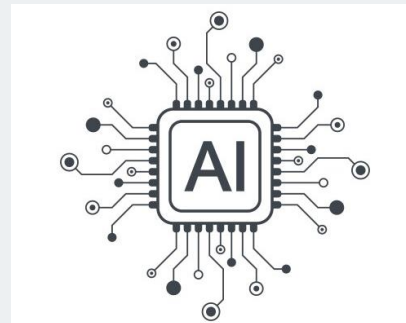
- Kto sa zúčastnil Techdays 2023?
- Kto má licencie M365?
- Kto manažuje PC / Mac z Cloudu?

1. Prečo moderné EUS

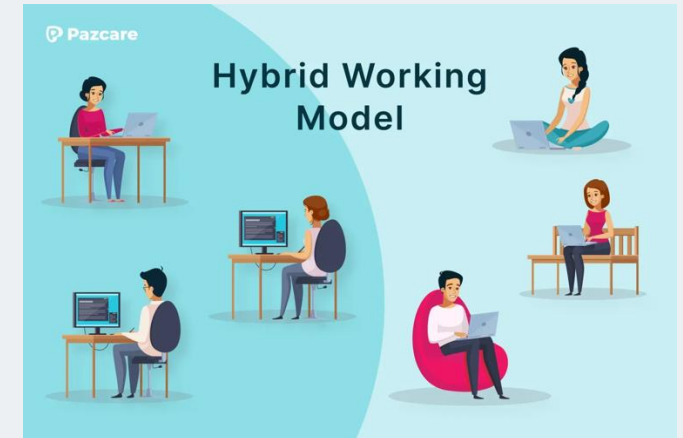
Ekonomické výzvy



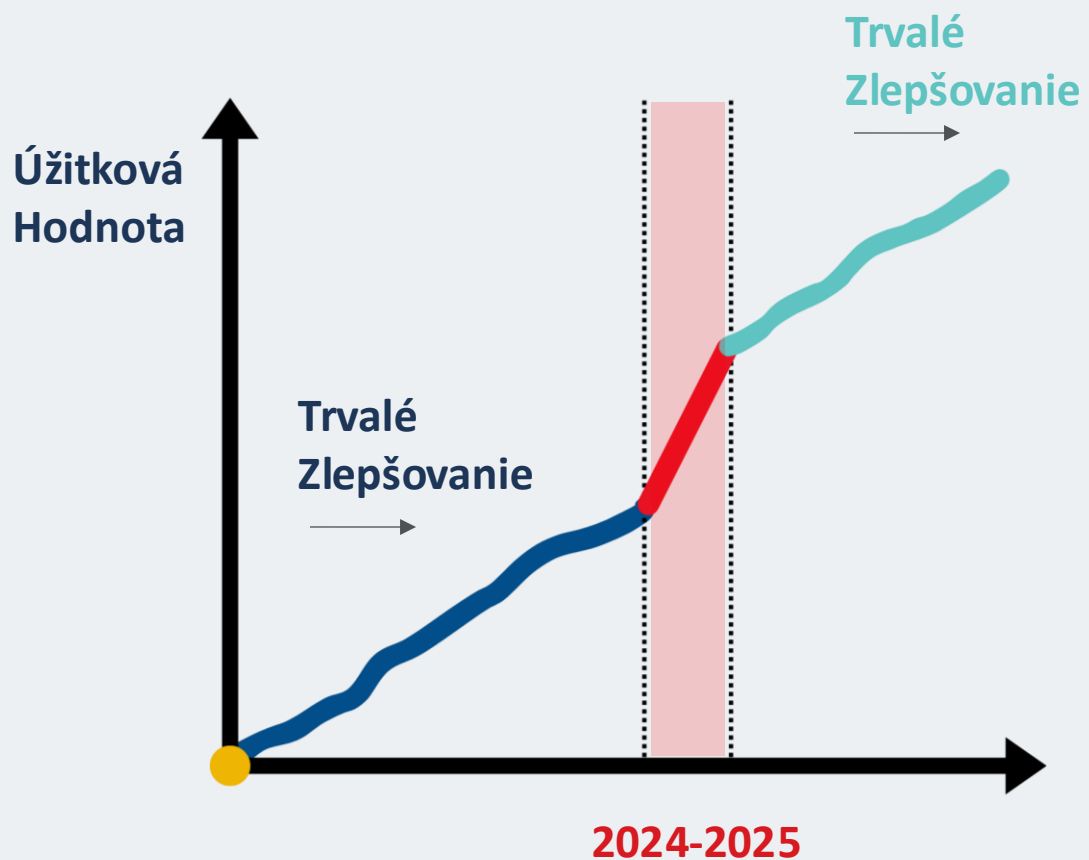
Technologické výzvy



Socio-Environmentálne výzvy



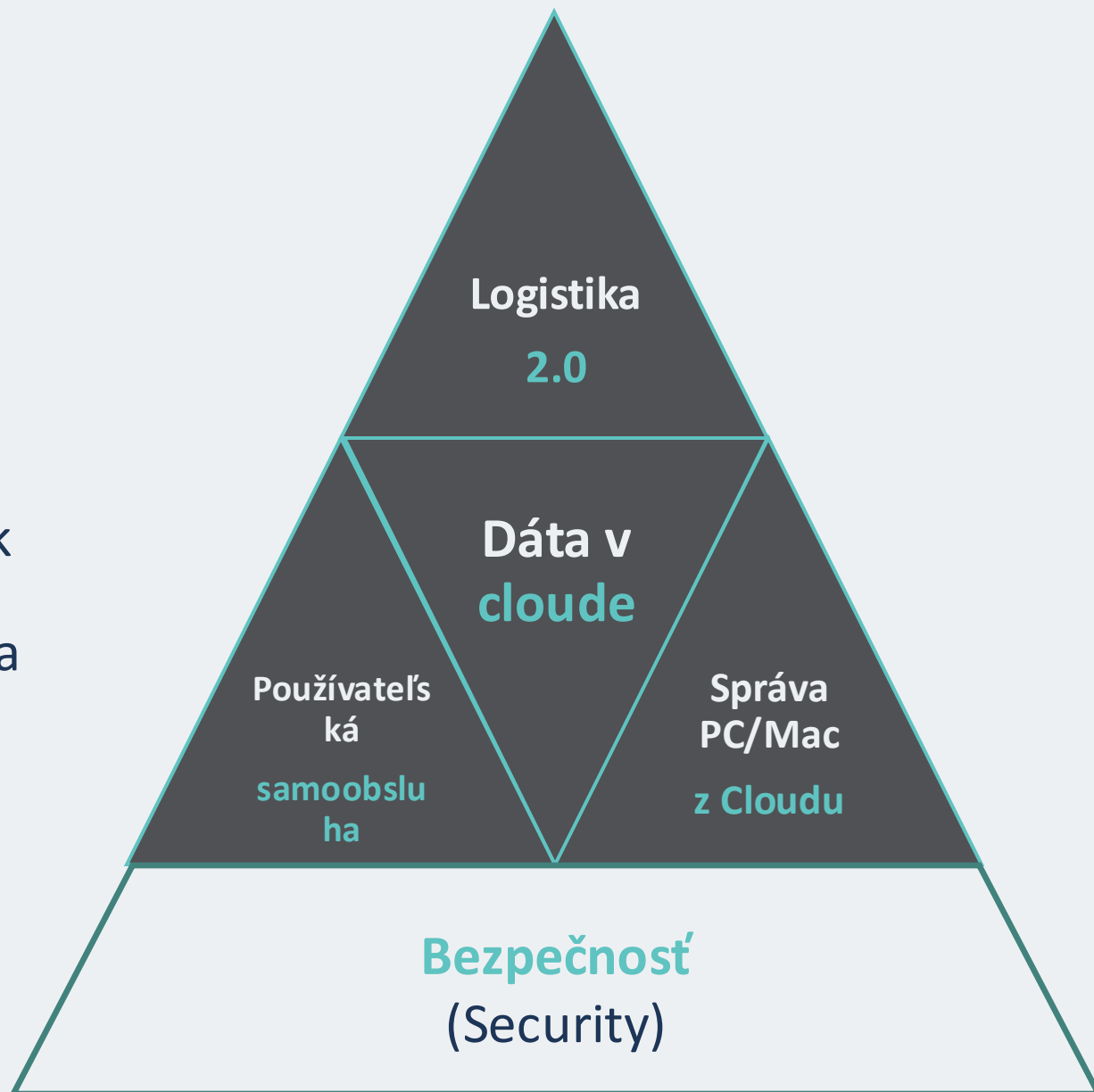
Moderný prístup k End User Services



- Zákazníci očakávajú, že budeme držať krok s výzvami za súčasnej cenovej efektivity
- Absolútna väčšina nákladov je spojená s ľudskou prácou (90%)
- **Náklady vieme znižovať zvyšovaním efektivity**
 - Zvyšovaním produktivity
 - **Zavádzaním INOVÁCIÍ**

Moderné EUS

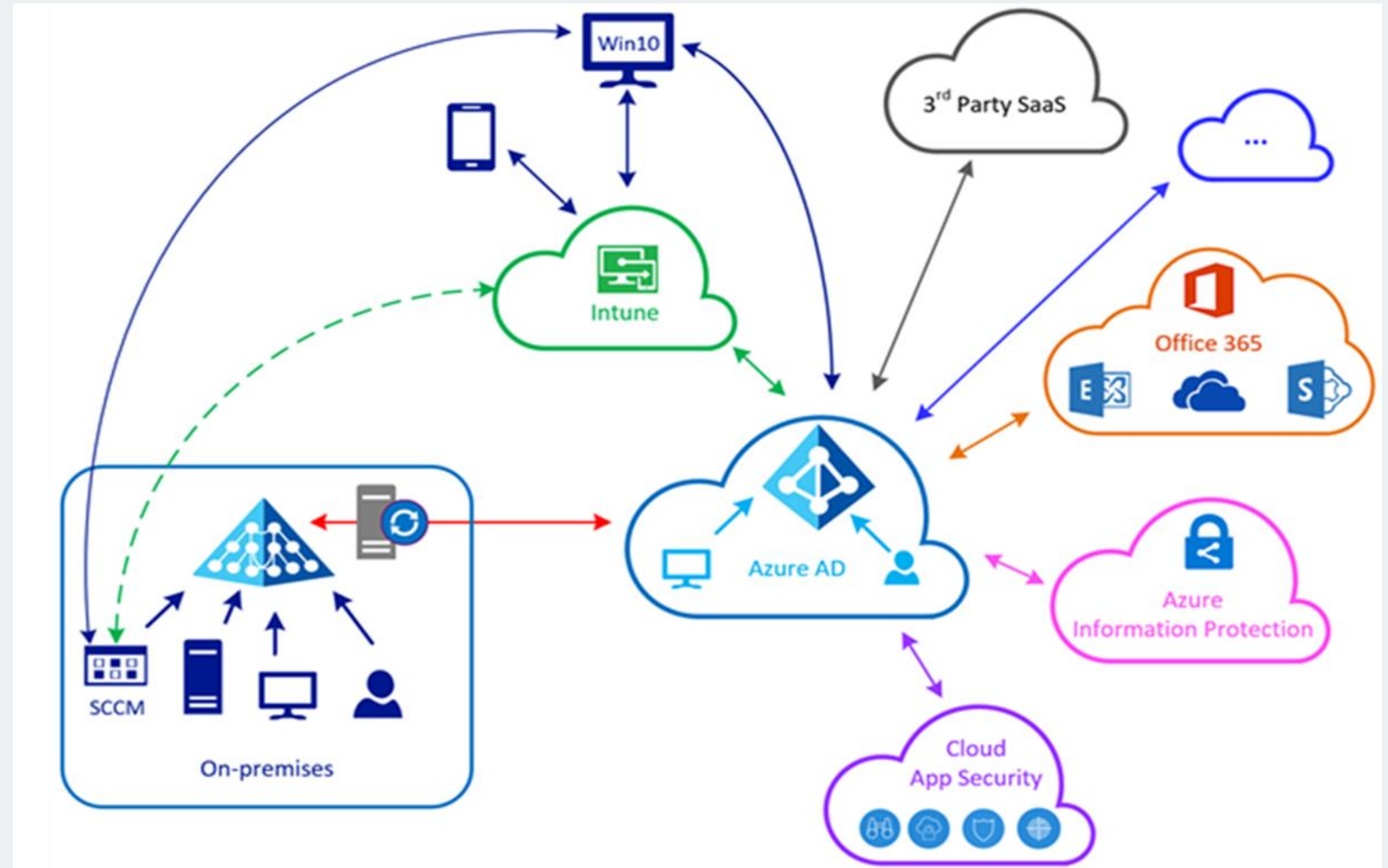
- Synergickým nasadením inovácií EUS dokážeme dosiahnuť maximálny úžitok
- Predpokladaná **úspora** na nákladoch za služby **až 30 %**
- A pridávame **Bezpečnosť**



2. PosAm story

Ako sme to robili predtým a ako to beží teraz

- **Východiskový stav**
- **Stratégia a vízia**
- **"Prvoplánová cesta"**
- **Širšie súvislosti**
- **Vyvolané zmeny**
- **Nová výzva**
- **Výsledok**



Výsledok ako prevádzkujeme PC / Mac

- Prideluje HR oddelenie
- Inštaluje používateľ
- Supportuje Kontaktné centrum

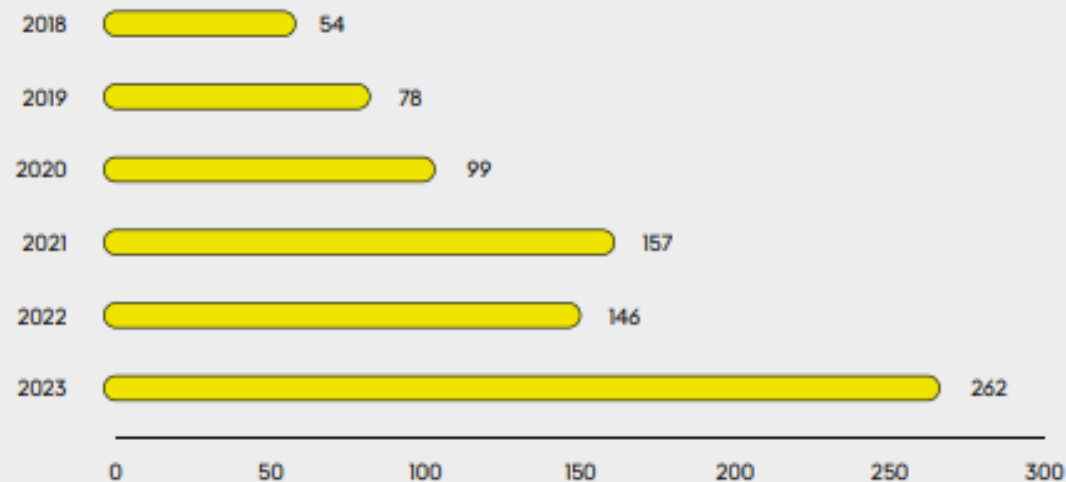
- Cloud konfigurujú a testujú Technici

3. Security

Hlavné hrozby podľa ENISA Threat Landscape 2022-2023

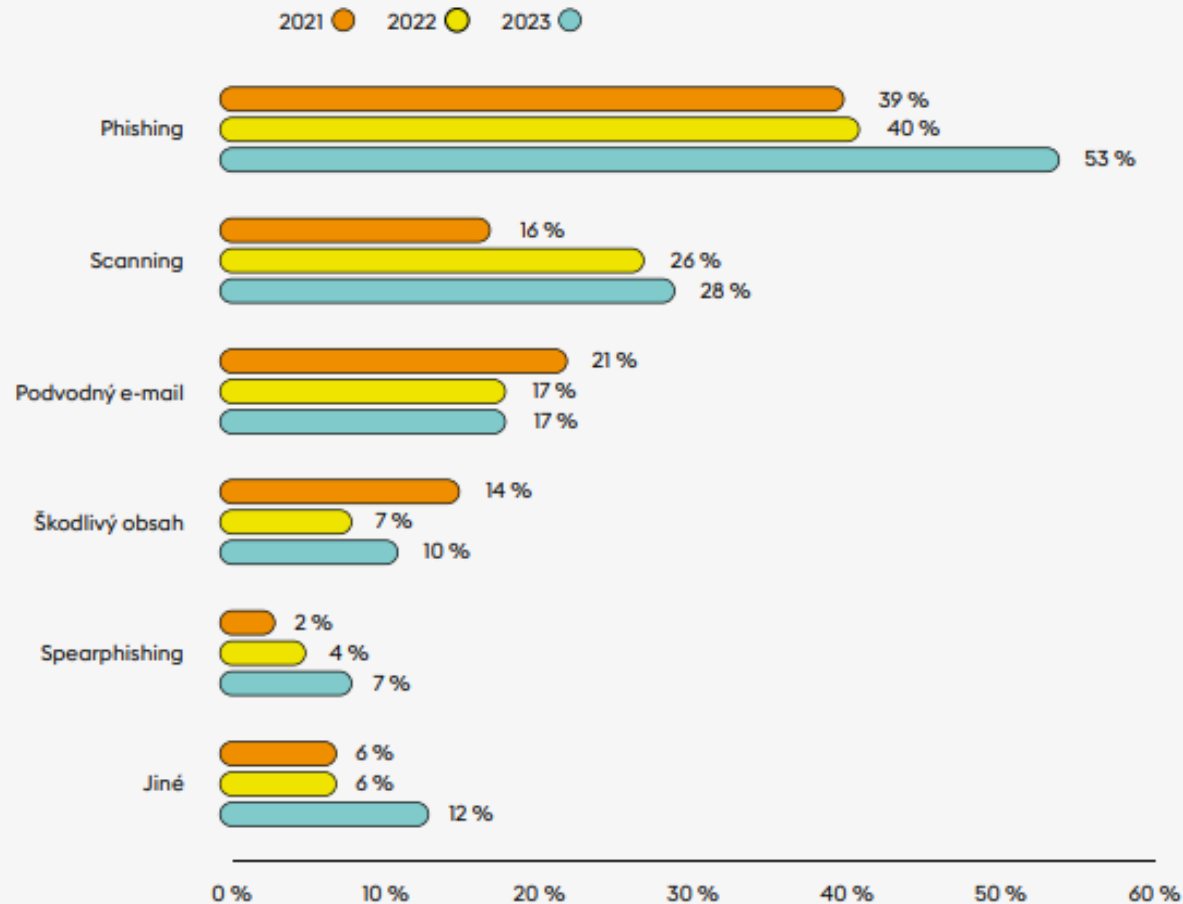


NÚKIB v roce 2023 evidoval celkem 262 kybernetických bezpečnostních incidentů, což je dosud nejvyšší zaregistrovaná hodnota.



Graf 1: Vývoj počtu incidentů evidovaných NÚKIB v letech 2018–2023

Pohledem dotazovaných společností dominuje statistikám kybernetických útoků dlouhodobě phishing, nicméně z letošních dat vyplývá, že se využívání této techniky oproti minulým rokům stupňuje.

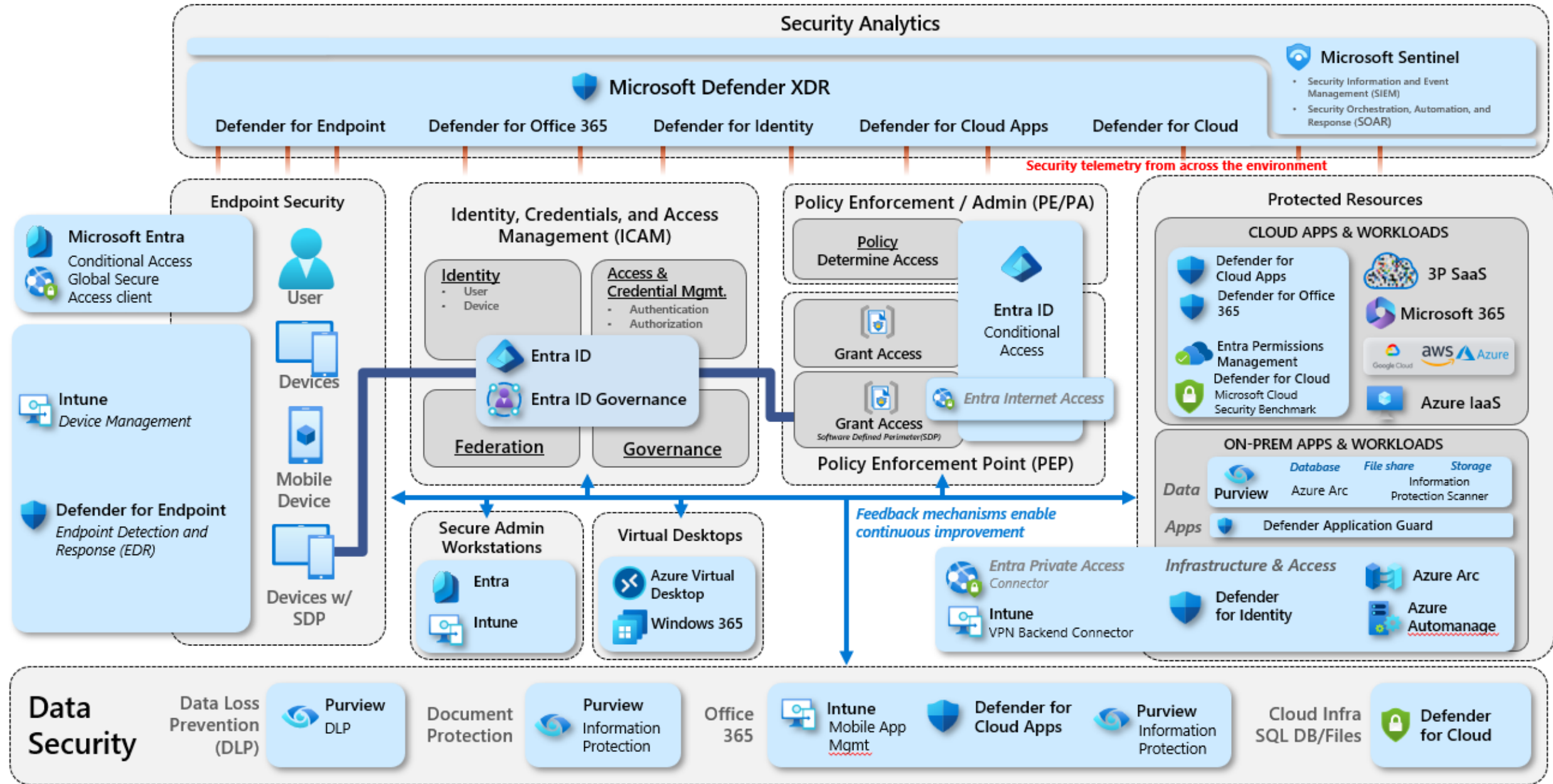


Graf 5 : Kategorie nejčastějších typů kybernetických útoků v letech 2021–2023 (% respondentů)

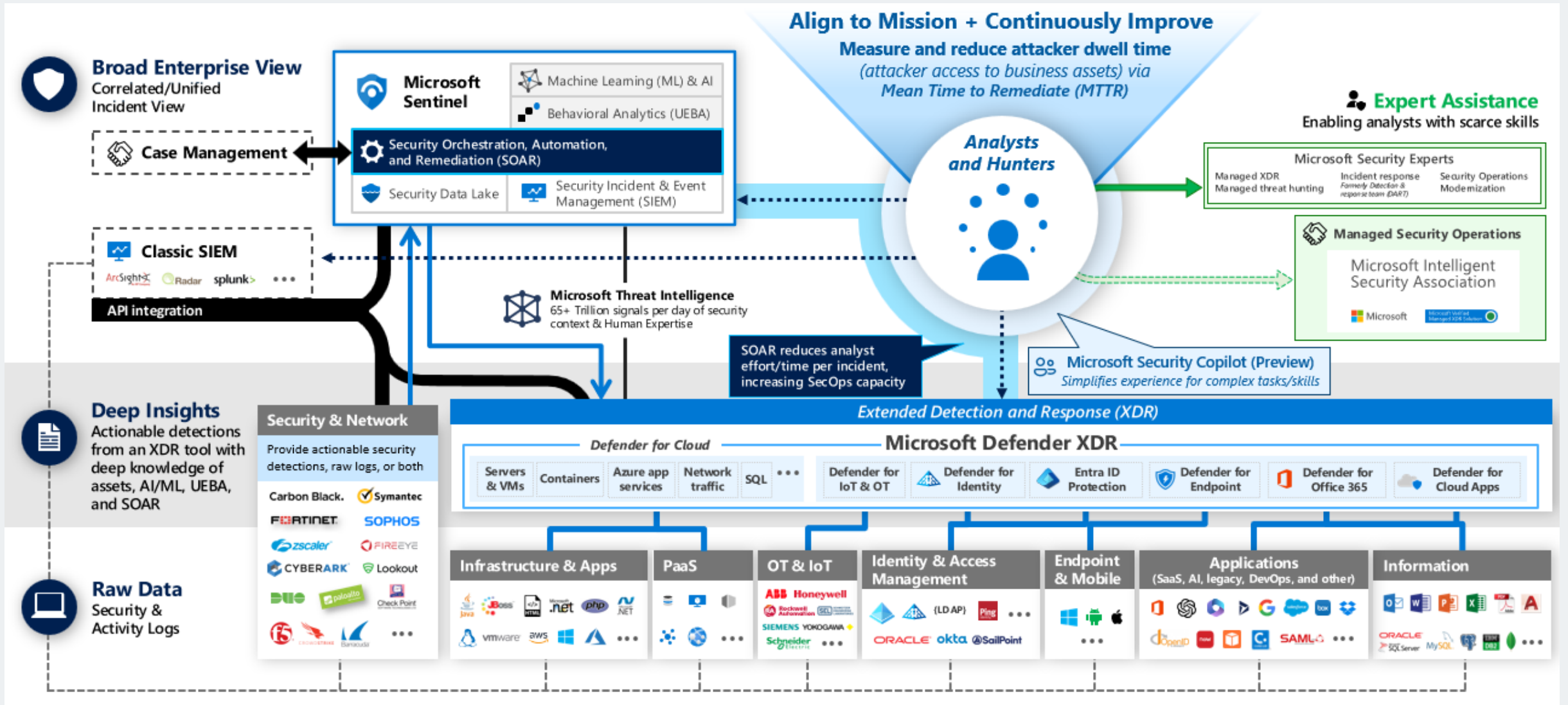
Dôvody

- NIS2 – Novela KB 69/2018 Z. z.
- ISO/IEC 27001:2022
- Konsolidácia a efektívnejšia správa
- Šifrovanie diskov
- Ochrana koncových staníc a XDR
- Vulnerability management
- DLP
- Web filtering
- Integrácia na SIEM - Sentinel

Microsoft Zero Trust (Microsoft Cybersecurity Reference Architectures)



Security Operations



Intune – Endpoint Security a Microsoft Defender

Threat analytics

Copilot Email notification settings Help resources ▼

Threat intel reports are being updated in stages to align with the Microsoft 365 Defender rebrand into [Microsoft Defender XDR](#). ✕



Latest threats

- [Vulnerability Profile: CVE-2024-24919 - Check Point Security Gateways](#) 0 / 0
- [Activity Profile: Twill Typhoon spearphishing campaign abuses MSC files](#) 0 / 0
- [Actor Profile: Pistachio Tempest](#) 0 / 0
- [Vulnerability Profile: CVE-2024-26169](#) 0 / 0

Active Alerts Resolved Alerts 1 more

High-impact threats

- [Activity Profile: OAuth apps used in BEC and phishing](#) 46 / 274
- [Technique Profile: On-premises credential theft \(Threat Overview\)](#) 26 / 300
- [Technique Profile: Malicious use of PowerShell](#) 26 / 97
- [Tool Profile: Impacket](#) 26 / 59

Active Alerts Resolved Alerts 1 more

Highest exposure threats

- [Activity Profile: Twill Typhoon spearphishing campaign abuses MSC files](#) 27
- [Actor Profile: Pistachio Tempest](#) 27
- [Actor Profile: Moonstone Sleet](#) 27
- [Technique Profile: Malicious use of PowerShell](#) 27

High 70-100 Medium 30-69 1 more

431 items Customize columns Filter

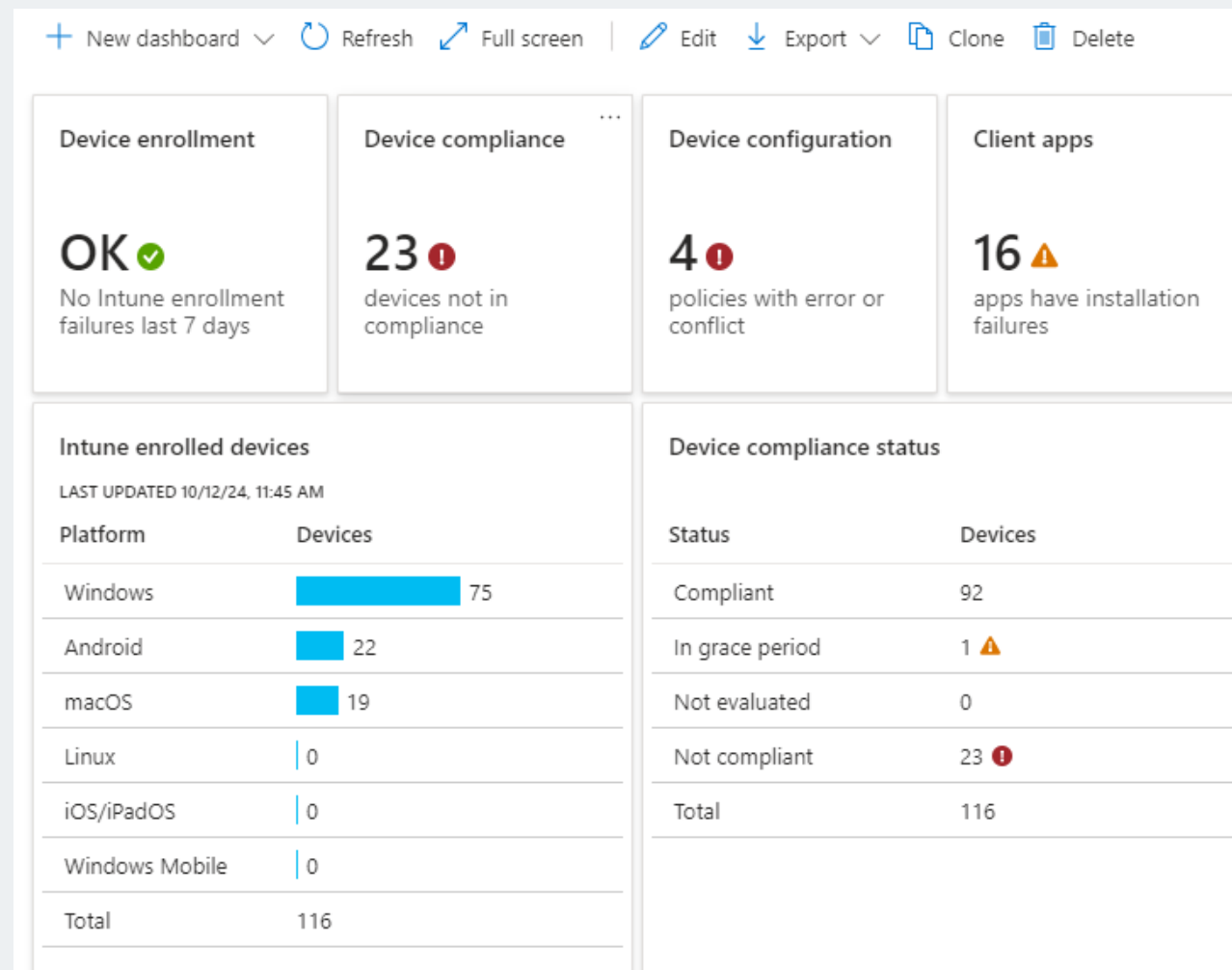
Threat ▼	Alerts ▼	Impacted assets ▼	Threat exposure level ⓘ ▼	Misconfigured devices ⓘ ▼	Vulnerable devices ⓘ ▼	Report type ▼	Published ▼
Vulnerability Profile: CVE-2024...	0 active / 0		0 - Low	Not available	0	Vulnerabilities	Jul 22, 2024 7:26 PM
Activity Profile: Twill Typhoon s...	0 active / 0		27 - Low	20	Not available	Attack campaigns	Jul 12, 2024 8:00 PM
Actor Profile: Pistachio Tempest	0 active / 0		27 - Low	20	Not available	Activity groups	Feb 26, 2021 10:46 AM
Vulnerability Profile: CVE-2024...	0 active / 0		0 - Low	16	0	Vulnerabilities	Jun 21, 2024 8:11 PM

4. Technologie

Podrobné štatistiky/reporty (MS Intune)

Proaktívne zisťovanie a riešenie problémov týkajúcich sa výkonu a spoľahlivosti KZ

- Výkon a spoľahlivosť aplikácií, zariadení a výkonu OS
- Sledovanie súladu, konfigurácie
- Endpoint security - MS Defender
- Detekcia anomálií



Správa aktualizácií OS Windows (MS Intune)

- Windows Update for Business ako súčasť MS Intune
- Podporované systémy Windows 10 a vyššie

Update settings

Microsoft product updates * ⓘ Allow Block

Windows drivers * ⓘ Allow Block

Quality update deferral period (days) * ⓘ ✓

Feature update deferral period (days) * ⓘ ✓

Upgrade Windows 10 devices to Latest Windows 11 release ⓘ Yes No

Set feature update uninstall period (2 - 60 days) * ⓘ ✓

Enable pre-release builds * ⓘ Enable Not Configured

Select pre-release channel ✓

User experience settings

Automatic update behavior ⓘ ✓

Active hours start * ⓘ ✓

Active hours end * ⓘ ✓

Option to pause Windows updates ⓘ Enable Disable

Option to check for Windows updates ⓘ Enable Disable

Change notification update level ⓘ ✓

Use deadline settings ⓘ Allow Not configured

Deadline for feature updates ⓘ ✓

Deadline for quality updates ⓘ ✓

Grace period ⓘ ✓

Auto reboot before deadline ⓘ Yes No

Správa aktualizácií ostatných OS, ovládačov a firmware (Vlastný vývoj)

- Ovládače a firmware
 - Prostredníctvom WUfB
 - Manuálne / Automatické potvrdzovanie
- Ostatné OS
 - iOS/iPadOS
 - MacOS
 - Android FOTA (Zebra, Samsung) – connector na OEM
 - Nastavenia aktualizácie iných prostredníctvom konfiguračného profilu
- Nastavenie BIOS/FW – DELL, HP
 - DCECMI – agent, .cctk nastavenie, heslo v Entra ID
 - HP Connect SaaS to SaaS služba – samostatný portál

4. Ako by sa to mohlo urobiť u Vás

Čím začať

- Analýza infraštruktúry
 - Nastavenia, ktorými je riešená správa koncových zariadení (AD, SCCM, GPO, iné nástroje ..)
 - On-premise komponenty a aplikácie
 - Nastavenie bezpečnosti, sieťových segmentov
- Príprava Azure / Entra prostredia:
 - Rozhodnutie aký level tenanta bude nasadený (Licenčná záležitosť)
 - Vytvorenie a konfigurácia Azure tenanta, resp. úprava aktuálneho stavu
 - Update on-premise komponentov na podporované verzie (odporúča sa aspoň N-1)
- Zvolenie vyhovujúceho spôsobu:
 - Hybridný režim – synchronizácia on-premise AD do Entra ID (v závislosti od aktuálneho stavu)
 - Pure Intune režim – zbavenie sa on-premise komponentov

Roadmapa

- Analýza požiadaviek, prostredí, štandardov a legislatívnych rámcov
- Bezpečnosť
- Režim práce (HomeOffice?)
- Správa dát (Cloud Int./Ext?)
- Samoobsluha / Kiosky



5. Q&A

Ďakujem za pozornosť



Ladislav Bogdány, Ľubomír Fačkovec

PosAm spol. s r.o.

+421 903 440 394, ladislav.bogdany@posam.sk

+421 910 138 922, lubomir.fackovec@posam.sk

PosAm, spol. s r. o., Pribinova 40, 811 09 Bratislava, Slovenská republika

