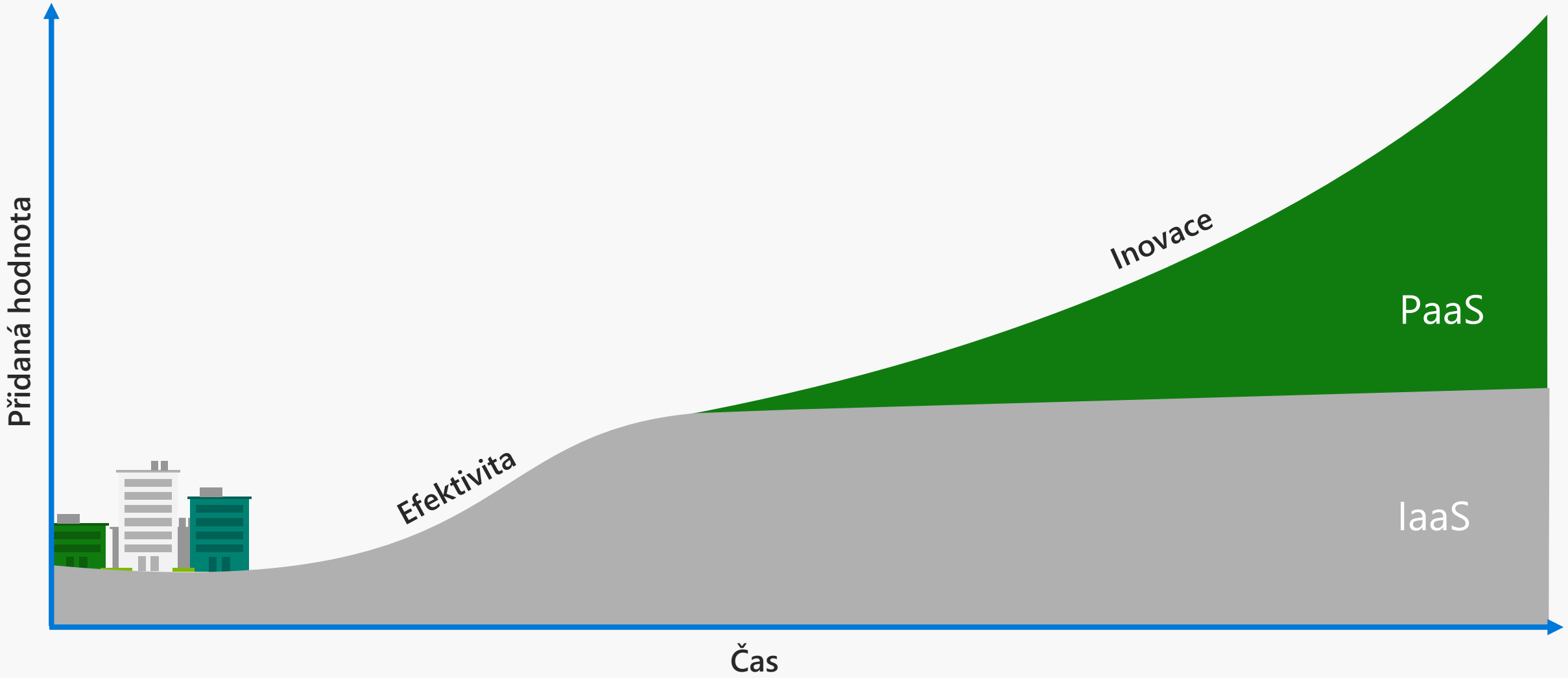
Cloudové inovace a bezpečné služby ve veřejné správě

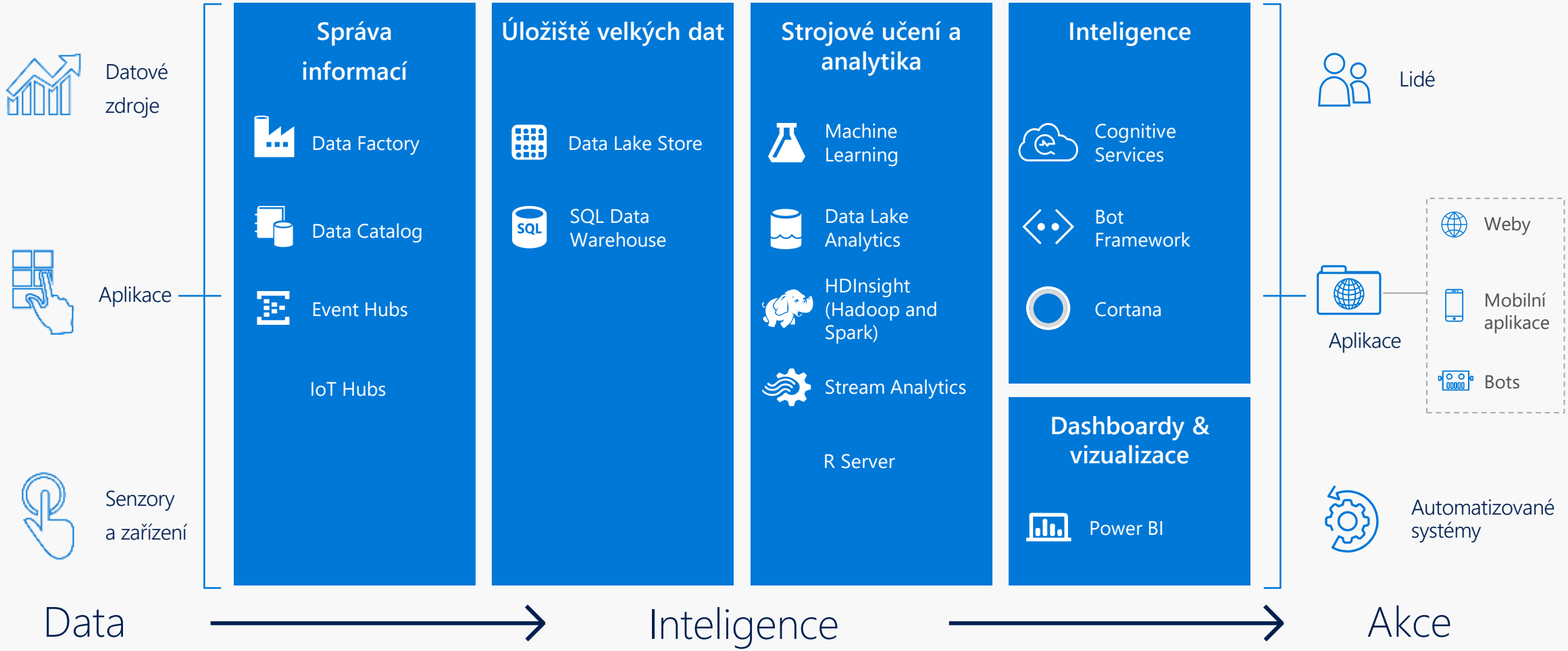
Dalibor Kačmář
Microsoft Česká Republika a Slovensko

LinkedIn: dalibor, Twitter: @kaciho

Od infrastruktury k inovaci



Převeďme data na inteligentní akci



Microsoft

Kognitivní služby

poskytují řešením lidskou stránku

Microsoft Cognitive Services

Obraz

Od obličejů k pocitům – umožní aplikacím pochopit obrázky a video

Řeč

Poslouchá a promlouvá k uživatelům – filtruje hluk, identifikuje řečníka, rozumí obsahu

Jazyk

Zpracovává text a učí se rozpoznat, co uživatel požaduje

Znalosti

Získává bohatou znalost z webu, akademických zdrojů nebo vlastních dat uživatele

Hledání

Prohledávání miliard webových stránek, obrázků, videí a zpráv

Analýza obrázku

Typ obrázku

Clip Art Type	0 Non-clipart
Line Drawing Type	0 Non-Line Drawing
Black & White Image	False

Obsah obrázku

Categories	`[{ “name”: “people_swimming”, “score”: 0.099609375 }]`
Adult Content	False
Adult Score	0.18533889949321747
Faces	`[{ “age”: 27, “gender”: “Male”, “faceRectangle”: {“left”: 472, “top”: 258, “width”: 199, “height”: 199}}]`

Barvy obrázku

Dominant Color Background	White
Dominant Color Foreground	Grey
Dominant Colors	White
Accent Color	

API pro analýzu emocí

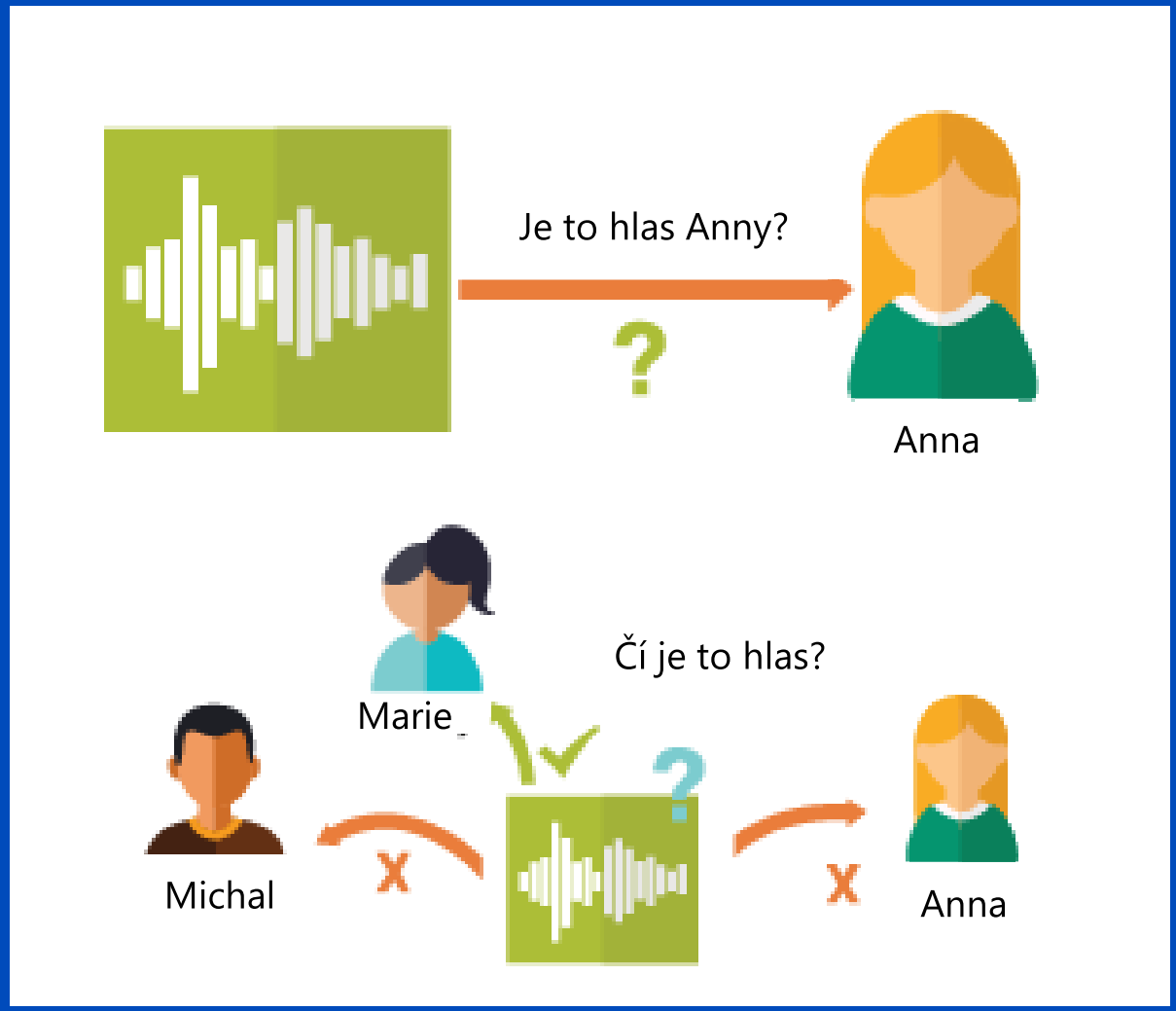
Detekce obličeje

```
"faceRectangle": {"width": 193,
                  "height": 193,
                  "left": 326,
                  "top": 204} …
```

Emoční skóre

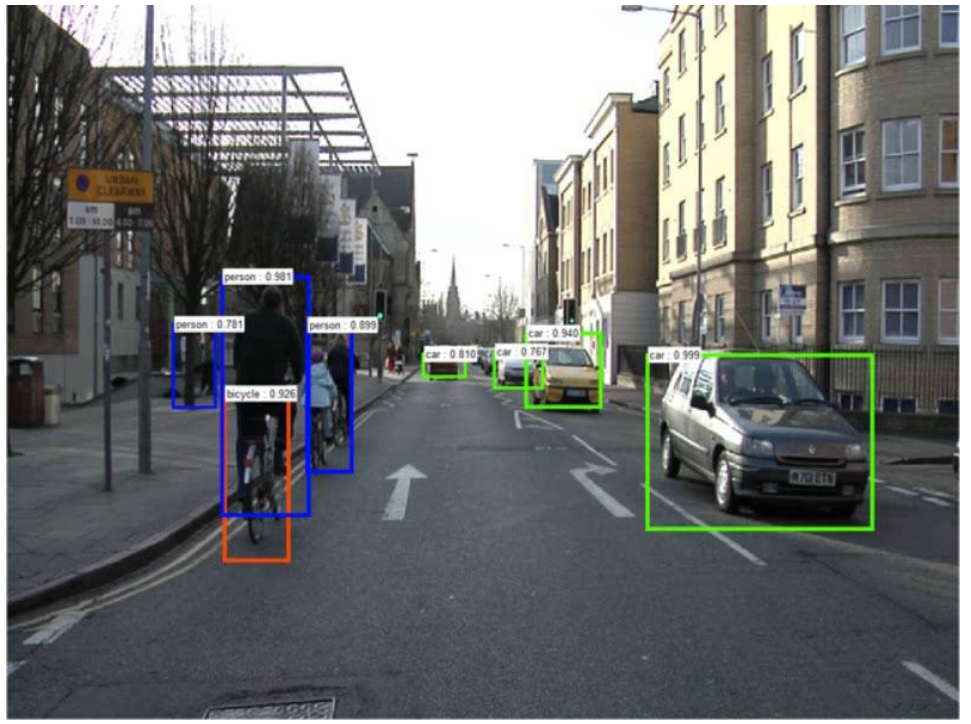
```
“scores": { "anger": 5.182241e-8,
            "contempt": 0.0000242813,
            "disgust": 5.621025e-7,
            "fear": 0.00115027453,
            "happiness": 1.06114619e-8,
            "neutral": 0.003540177,
            "sadness": 9.30888746e-7,
            "surprise": 0.9952837}
```

Rozpoznání mluvící osoby



Cognitive Services
Přidání "chytrosti" vašim aplikacím

Stabilizace obraze



Rozpoznávání objektů v reálném čase

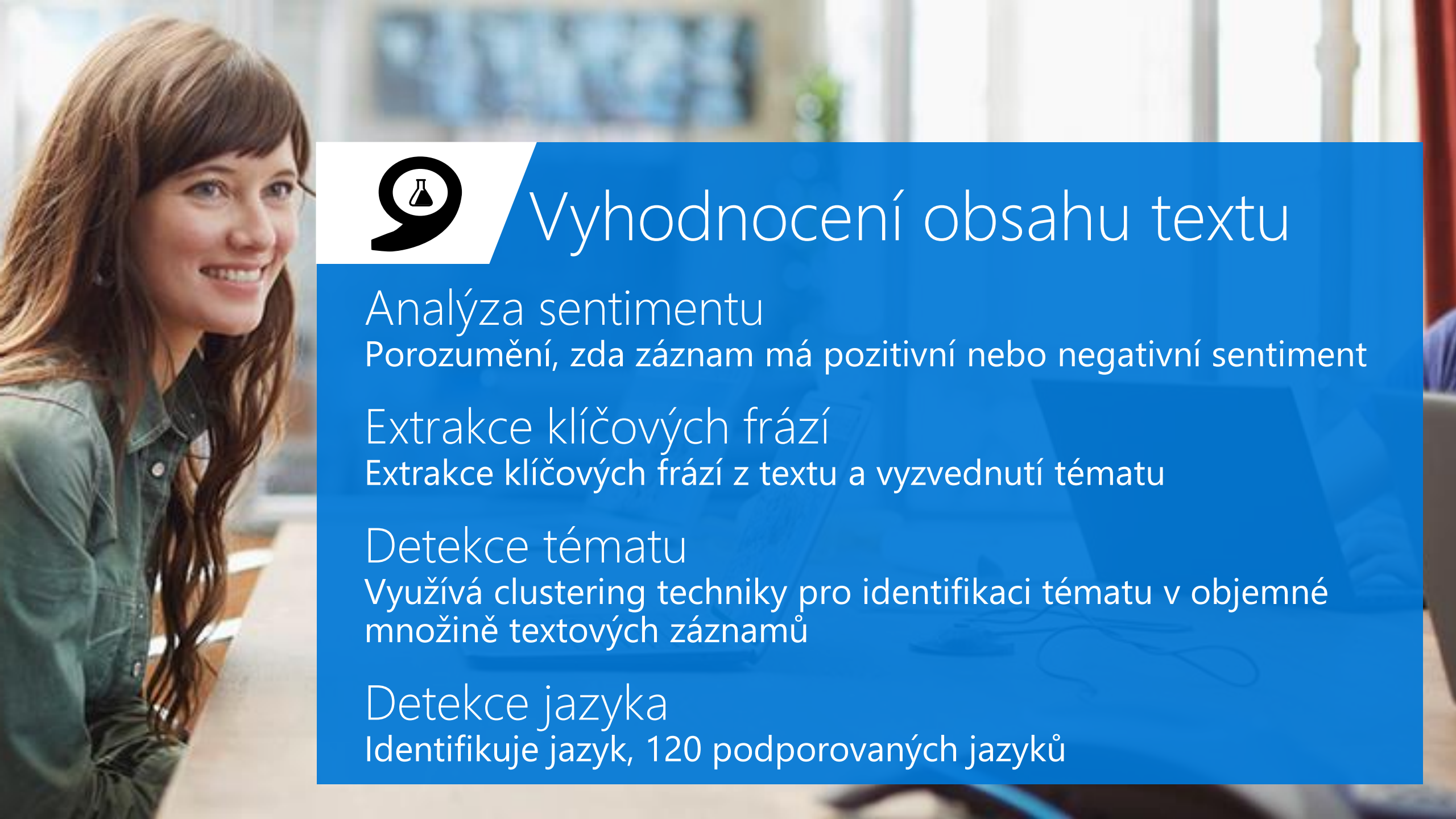
Porozumění jazyku

Rozpoznávání textu

Rozpoznávání obličeje

Analýza obrazu

https://www.microsoft.com/cognitive-services



Vyhodnocení obsahu textu

Analýza sentimentu

Porozumění, zda záznam má pozitivní nebo negativní sentiment

Extrakce klíčových frází

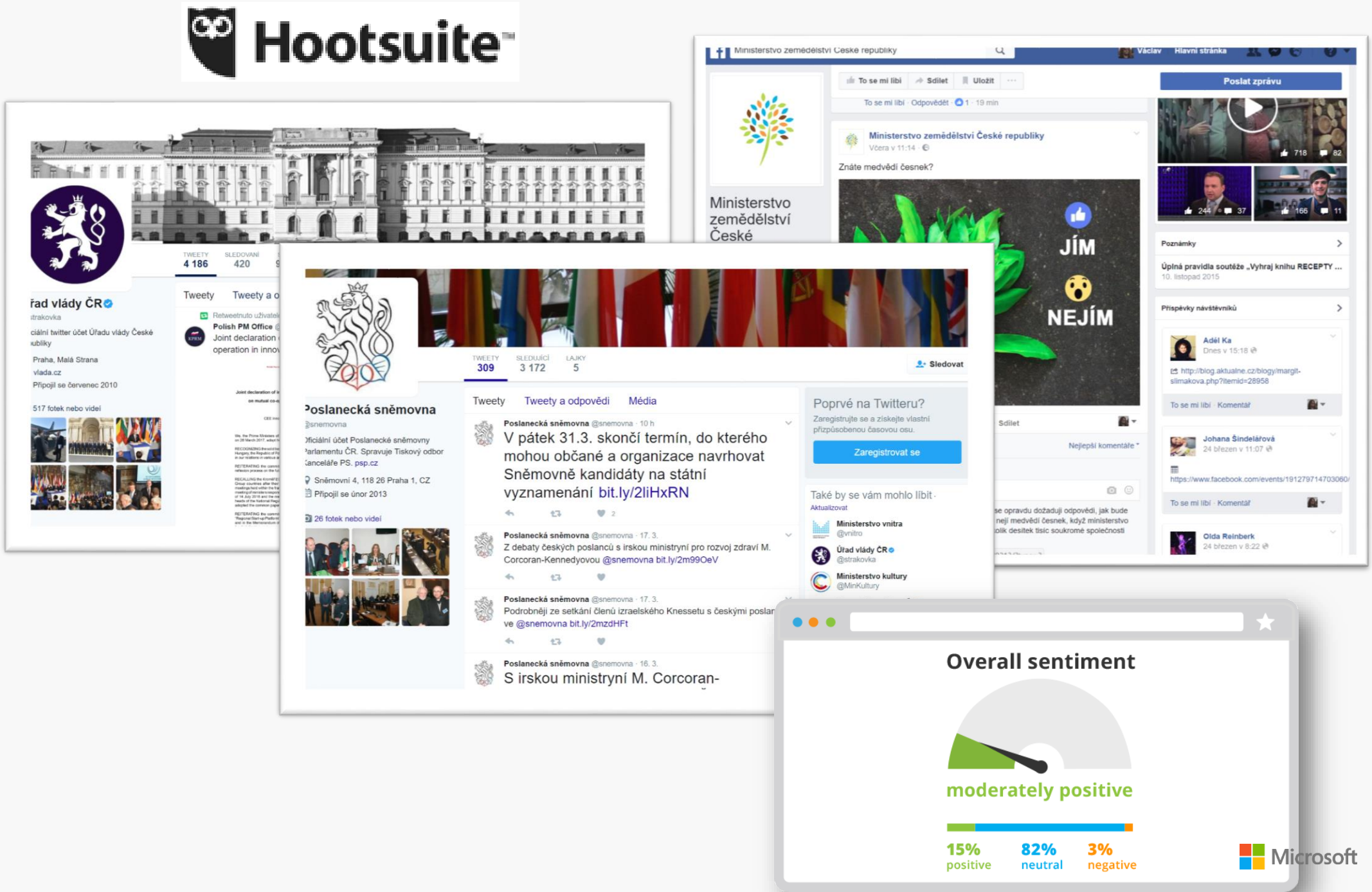
Extrakce klíčových frází z textu a vyzvednutí tématu

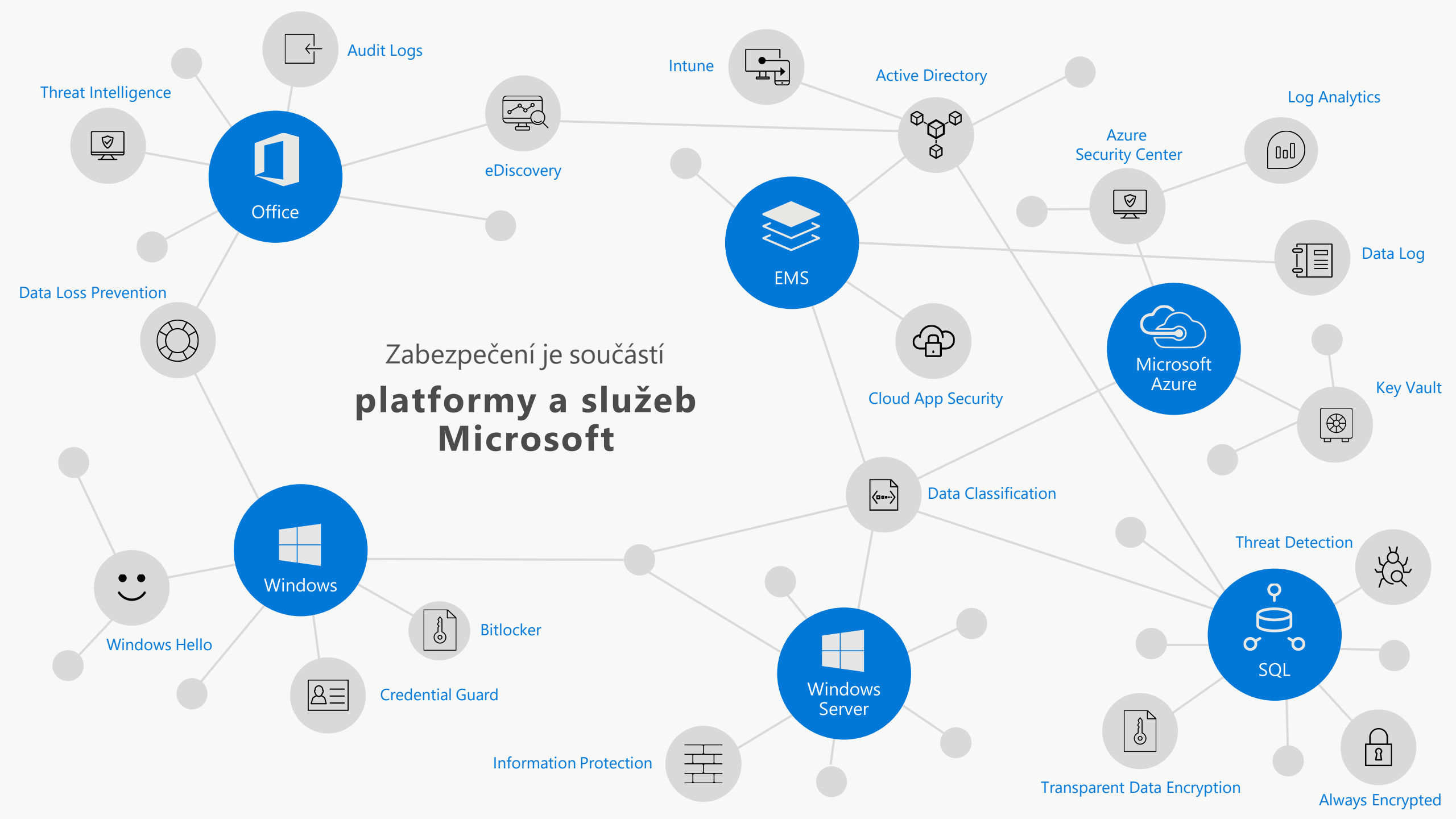
Detekce tématu

Využívá clustering techniky pro identifikaci tématu v objemné množině textových záznamů

Detekce jazyka

Identifikuje jazyk, 120 podporovaných jazyků


Hootsuite
Ministerstvo zemědělství České republiky
To se mi líbí
Sdílet
Uložit
Poslat zprávu
Ministerstvo zemědělství České republiky
Včera v 11:14
Znáte medvědí česnek?
JÍM
NEJÍM
Poznámky
Úplná pravidla soutěže „Vyhraj knihu RECEPTY ...
10. listopad 2015
Příspěvky návštěvníků
Adél Ka
Dnes v 15:18
Johana Šindelářová
24 březen v 11:07
Olda Reinberk
24 březen v 8:22
Úřad vlády ČR
TWEETY 4 186
SLEDOVANÍ 420
Tweety
Tweety a o
Retweetnuto uživatel
Polish PM Office
Joint declaration
operation in innov
Praha, Malá Strana
vlada.cz
Připojil se červenec 2010
517 fotek nebo videí
Poslanecká sněmovna
TWEETY 309
SLEDUJÍCÍ 3 172
LAJKY 5
Sledovat
Tweety
Tweety a odpovědi
Média
Poslanecká sněmovna @snemovna · 10 h
V pátek 31.3. skončí termín, do kterého mohou občané a organizace navrhovat Sněmovně kandidáty na státní vyznamenání bit.ly/2liHxRN
Poslanecká sněmovna @snemovna · 17. 3.
Z debaty českých poslanců s irskou ministryní pro rozvoj zdraví M. Corcoran-Kennedyovou @snemovna bit.ly/2m99OeV
Poslanecká sněmovna @snemovna · 17. 3.
Podrobněji ze setkání členů izraelského Knessetu s českými poslan
ve @snemovna bit.ly/2mzdHFt
Poslanecká sněmovna @snemovna · 16. 3.
S irskou ministryní M. Corcoran-
Sněmovní 4, 118 26 Praha 1, CZ
Připojil se únor 2013
26 fotek nebo videí
Poprvé na Twitteru?
Zaregistrujte se a získejte vlastní přizpůsobenou časovou osu.
Zaregistrovat se
Také by se vám mohlo líbit
Aktualizovat
Ministerstvo vnitra
@vnitro
Úřad vlády ČR
@strakovka
Ministerstvo kultury
@MinKultury
Overall sentiment
moderately positive
15% positive
82% neutral
3% negative
Microsoft


Audit Logs
Threat Intelligence
Office
eDiscovery
Intune
Active Directory
Log Analytics
Azure
Security Center
EMS
Data Log
Data Loss Prevention
Cloud App Security
Microsoft
Azure
Key Vault
Zabezpečení je součástí
platformy a služeb
Microsoft
Data Classification
Threat Detection
Windows
Windows Hello
Bitlocker
Credential Guard
Windows
Server
SQL
Information Protection
Transparent Data Encryption
Always Encrypted

Široké portfolio certifikací a mezinárodních standardů

Certifikace a pokladová dokumentace nyní přístupné na Microsoft Trust Center www.microsoft.com/trust

GLOBÁLNÍ

- ISO 27001
- ISO 27018
- ISO 27017
- ISO 22301
- ISO 9001
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3
- CSA STAR Self-Assessment
- CSA STAR Certification
- CSA STAR Attestation

US GOV

- Moderate JAB P-ATO
- High JAB P-ATO
- DoD DISA SRG Level 2
- DoD DISA SRG Level 4
- DoD DISA SRG Level 5
- SP 800-171
- FIPS 140-2
- Section 508 VPAT
- ITAR
- CJIS
- IRS 1075

PRŮMYSLOVÉ

- PCI DSS Level 1
- CDSA
- MPAA
- FACT UK
- Shared Assessments
- FISC Japan
- HIPAA / HITECH Act
- HITRUST
- GxP 21 CFR Part 11
- MARS-E
- IG Toolkit UK
- FERPA
- GLBA
- FFIEC

REGIONÁLNÍ

- Argentina PDPA
- EU Model Clauses
- UK G-Cloud
- China DJCP
- China GB 18030
- China TRUCS
- Singapore MTCS
- Australia IRAP/CCSL
- New Zealand GCIO
- Japan My Number Act
- ENISA IAF
- Japan CS Mark Gold
- Spain ENS
- Spain DPA
- India MeitY
- Canada Privacy Laws
- Privacy Shield
- Germany IT Grundschutz workbook

Zabezpečení díky analytice dat

Ochrana pro naše zákazníky,

pro naše cloudové služby,

i pro ostatní spotřebitele

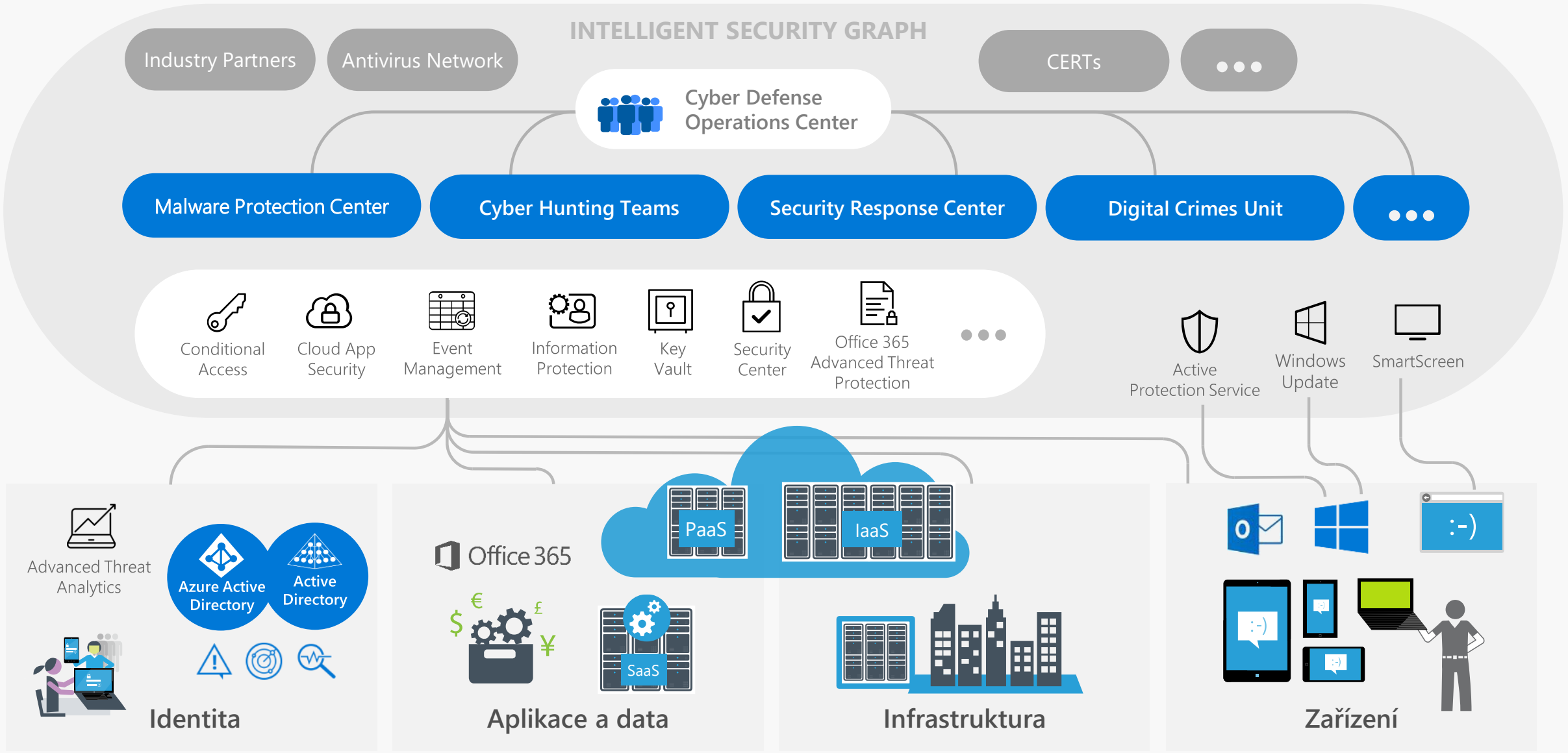
Koordinace proti kybernetickým hrozbám

Microsoft Cyber Defense Operations Center

Microsoft Secure Blog: naše CDOC doporučené postupy

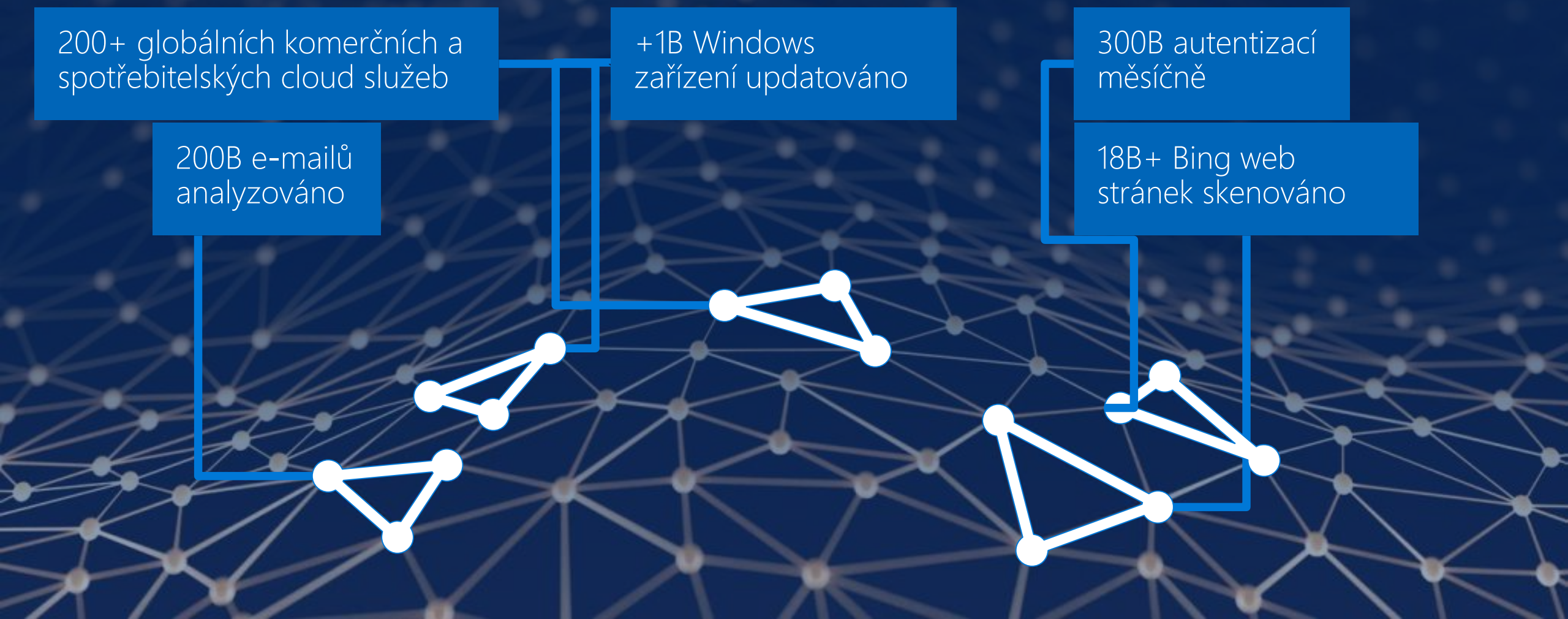
- Digital Crimes Unit
- Microsoft Security Response Center
- Microsoft Threat Intelligence Center
- Office 365
- Microsoft Azure
- Windows & Devices Group

Bezpečnostní technologie a organizační opatření



NAŠE JEDINEČNÁ INTELIGENCE

Microsoft Intelligent Security Graph

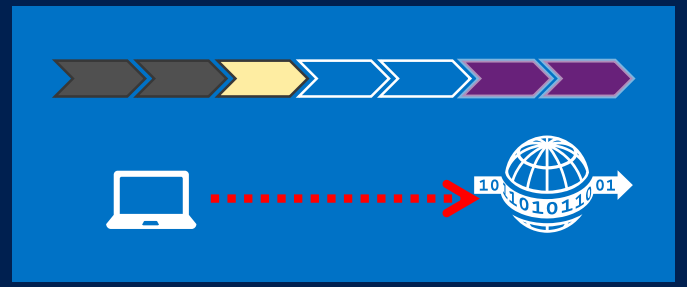


Využíváme Threat Intelligence

Detekce & Ochrana …

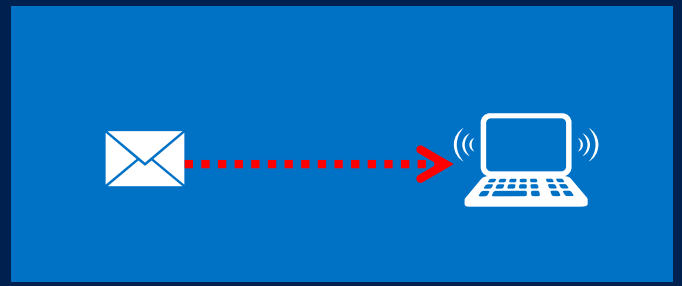
…On Premises

s Windows 10, Defender Advanced Threat Protection (ATP), Advanced Threat Analytics (ATA)



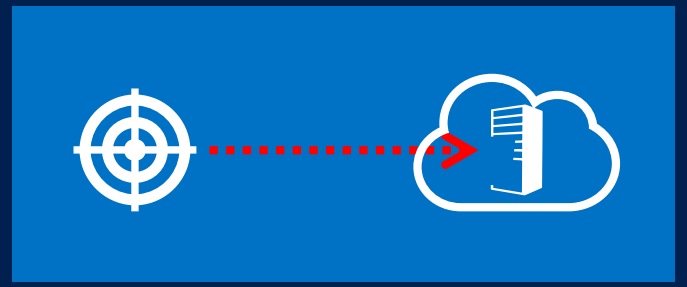
…použitím SaaS (O365)

s Advanced Threat Protection (ATP), Cloud App Security, Azure Active Directory

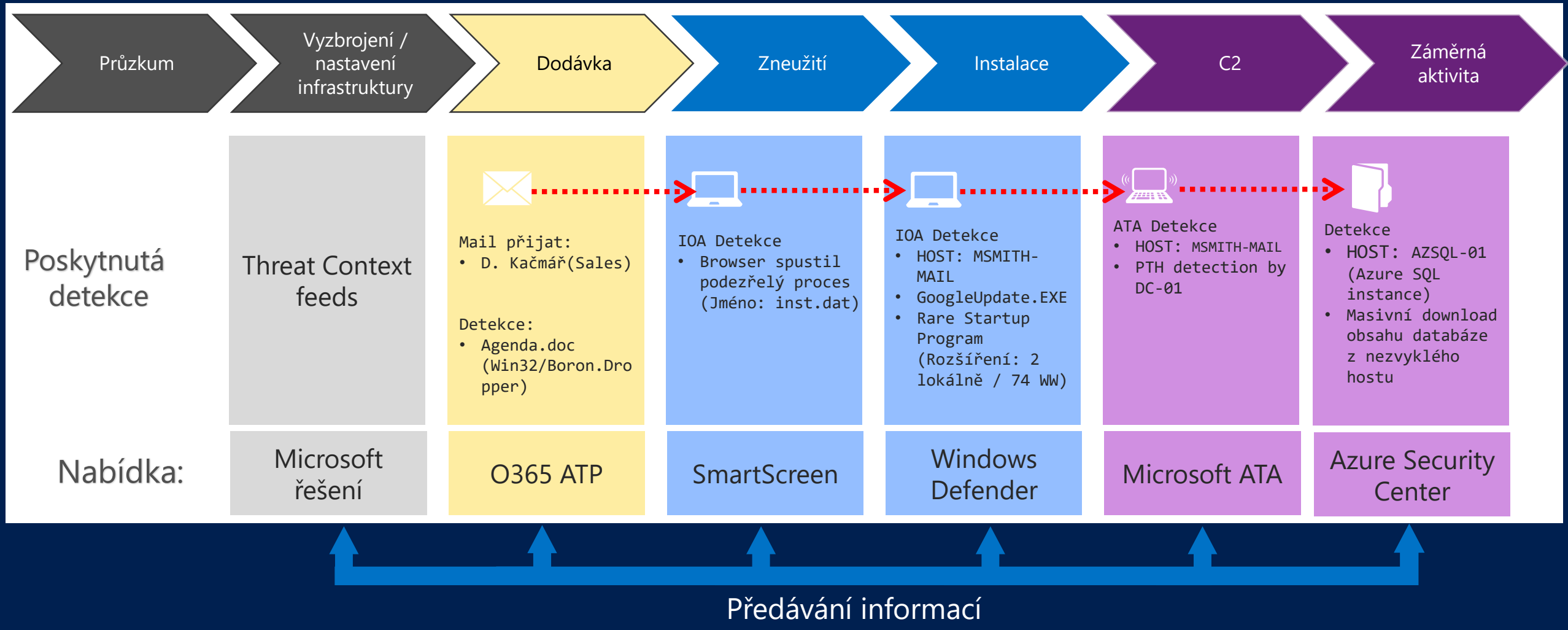


…v IaaS a PaaS

s Azure Security Center



Úplná detekce napříč firemním prostředím



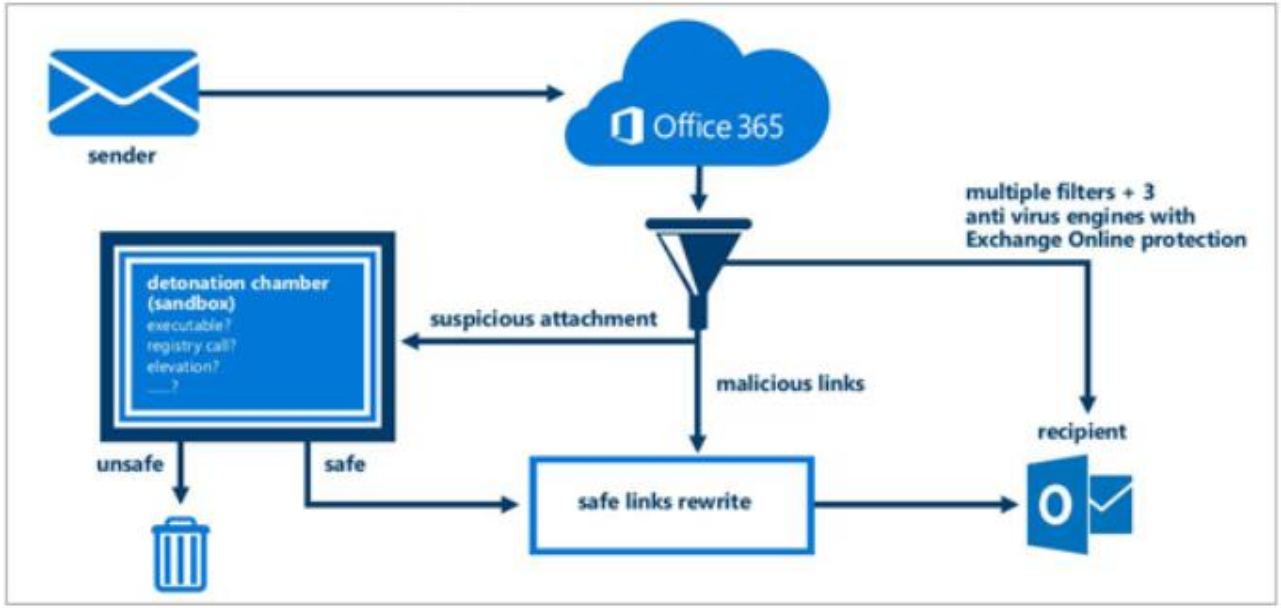
Exchange Online Advanced Threat Protection

Safe Attachments

- Sandboxing příloh a test jejich chování
- Ochrana i před 0-day útoky

Safe Links

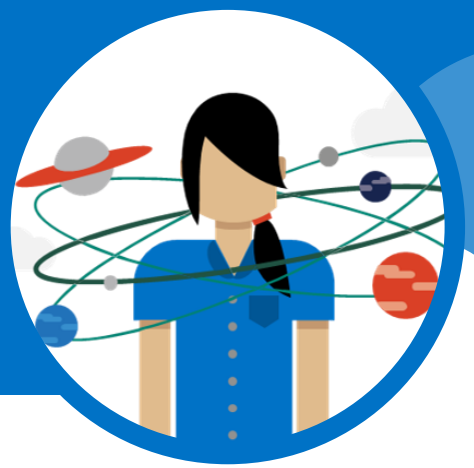
- Aktivuje URL přes dočasný proxy server
- Reputační databáze > 1 mil. URL linků



Azure Security Center umožňuje předcházet, detekovat a reagovat na hrozby

Získání znalosti a kontroly

Bezpečnost cloud rychlostí



Integrace řešení partnerů

Detekce kybernetických útoků

Azure Security Center

CHRÁNIT, DETEKOVAT & REAGOVAT

Porozumění bezpečnostní reality

Viditelnost napříč všemi Azure subskripcemi – aplikace bezpečnostních politik a monitorování souladu

Dostupnost bezpečnosti cloud rychlostí

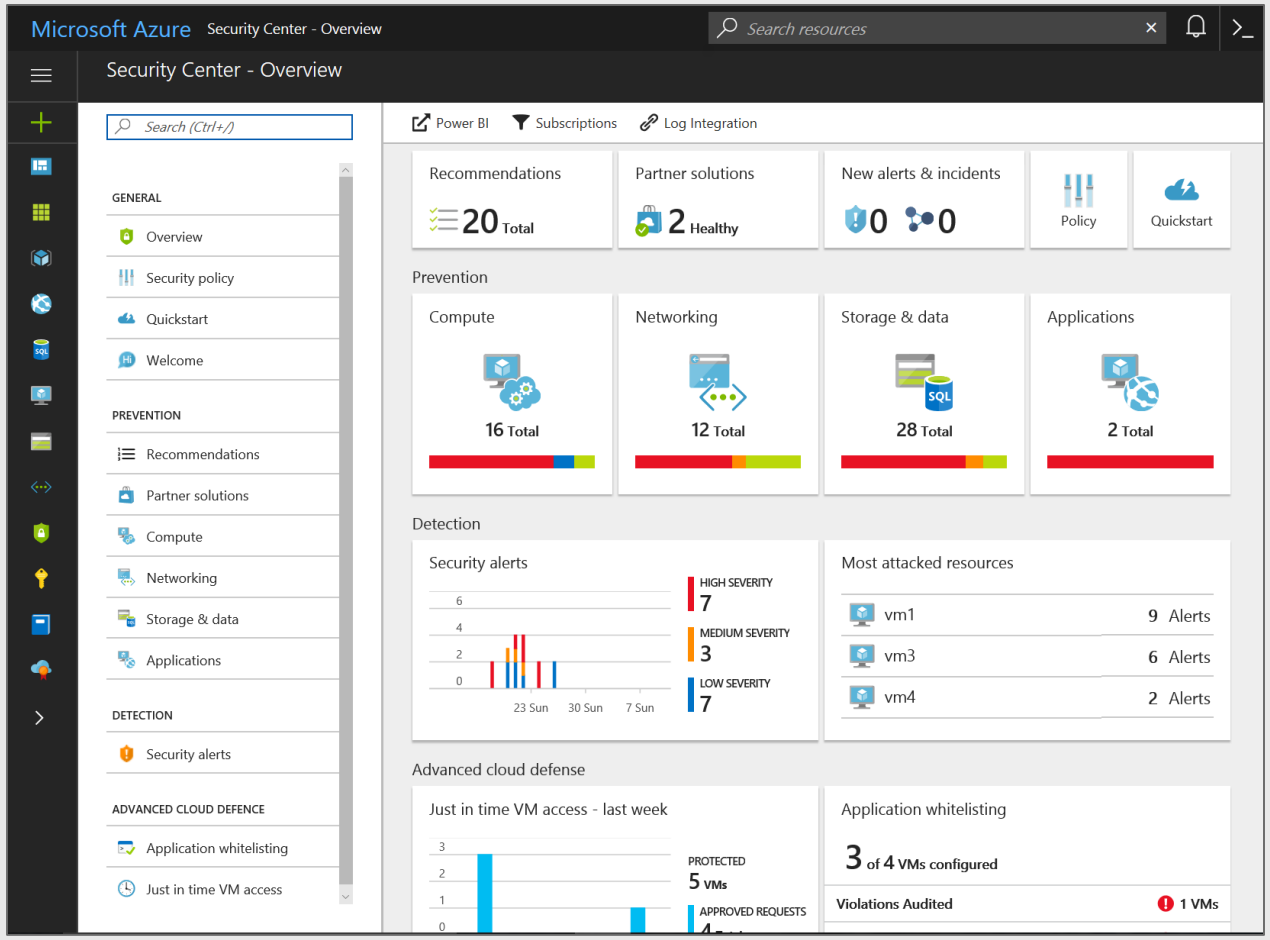
Snadné nalezení a oprava zranitelností – náprava pomocí zabudovaných bezpečnostních postupů a integrovaných partnerských řešení

Brzká detekce útoků

Detekuje útoky pomocí advanced security analytics a Microsoft global threat intelligence

Rychlá reakce pro minimalizaci dopadů

Získejte informace o akcích útočníka (mapováno napříč kill chain), cíle a taktiky



Ochrana hybridních řešení (cloudu)

Azure Security Center

Bezpečnost jsou součást cloudu - Azure

Sledování všech zdrojů a průběžné ověření bezpečnosti (antimalware, system updates, šifrování, konfigurace VPNs)

Akční bezpečnostní doporučení

Bezpečnostní politiky pro IT governance

Integrovaná správa a monitoring partnerských bezpečnostních řešení

Detekce ohrožení pomocí pokročilé analytiky

+

OMS Security

Bezpečnost postavená s Log analytikou

Sběr dat z libovolného zdroje (Azure nebo AWS, Windows Server/Linux, VMware/OpenStack)

Pohled na status bezpečnosti (antimalware, system updates)

Korelace detekovaných škodlivých aktivit a rychlé vyhledání řešení

Integrace provozní a bezpečností správy

Detekce ohrožení pomocí pokročilé analytiky

Pokročilé schopnosti detekce

Threat intelligence

Sleduje známé „škodlivé hráče“

Příklady
- Síťový provoz na škodlivé IP adresy
- Spouštění škodlivých kódů

Analýza chování

Sleduje známé vzory a škodlivé chování

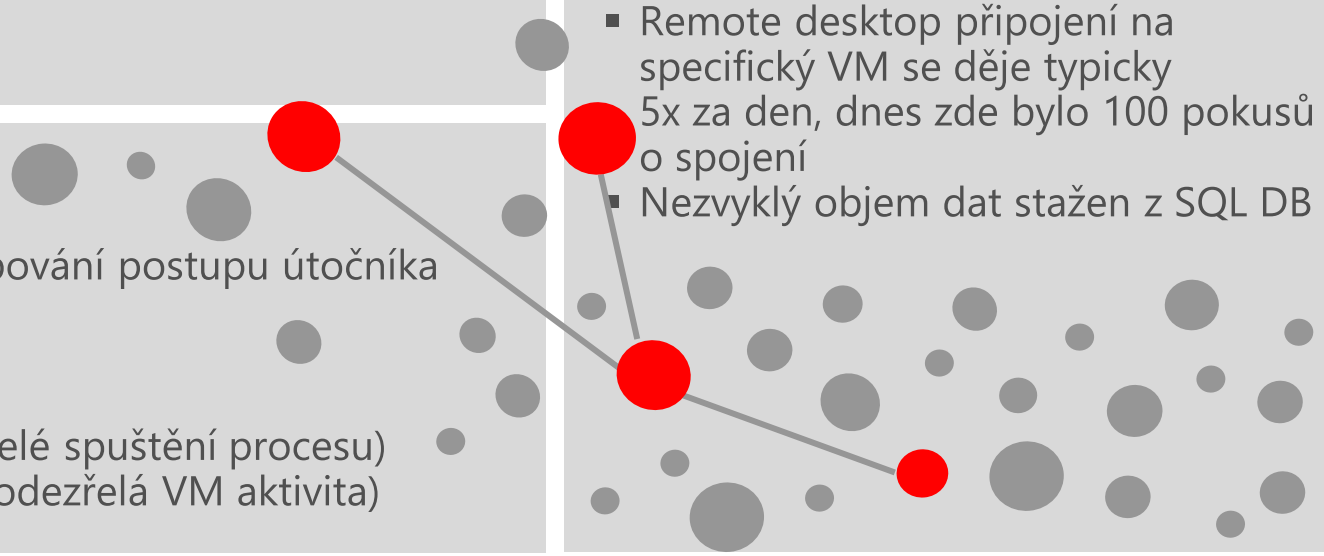
Příklady
- Proces spuštěný škodlivým způsobem
- Vzory SQL injection

Detekce anomálií

Využívá statistické profily pro budování historické baselinky

Upozorňuje na odchylky, které odpovídají potenciálnímu směru útoku

Příklad
- Remote desktop připojení na specifický VM se děje typicky 5x za den, dnes zde bylo 100 pokusů o spojení
- Nezvyklý objem dat stažen z SQL DB

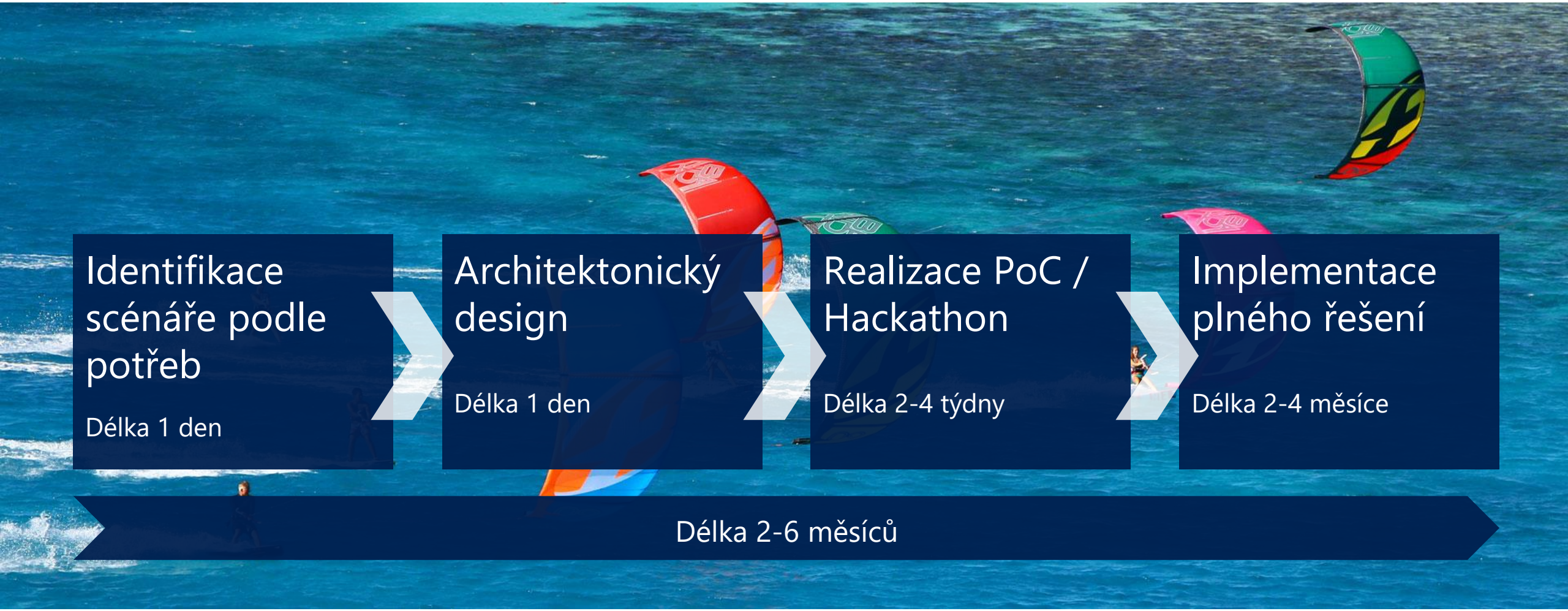


Fúze

Kombinuje events a alerty z celého „kill chain“ pro mapování postupu útočníka

Příklady
- SQL injections (WAF + Azure SQL Logs)
- Malicious process (Crash dump… a později … podezřelé spuštění procesu)
- Breach detection (Brute force pokus … a později … podezřelá VM aktivita)

Začněte v malém, buďte agilní, nasazujte rychle …



… s vysokou bezpečností

Microsoft