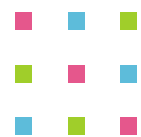


GDPR a poskytovatelé cloudových služeb

Jiří Černý, Ředitel pro právní záležitosti ČR/SK
Vlastimil Tesař, Partner Technology Strategist
Microsoft s.r.o.



Vymezení role poskytovatele Cloudu

- **Prevádzkovateľ:** osoba, nebo orgán veřejné moci, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů

(zákazník poskytovatele cloudové služby)

- **Sprostredkovateľ:** osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce

(poskytovatel cloudové služby)

- **Dotknutá osoba:** fyzická osoba, která je identifikovaná , resp. identifikovatelná s použitím osobních údajů































(zákazník nebo zaměstnanec Prevádzkovateľa)

- **GDPR mimo Cloud** – MS nemá roli **sprostredkovateľa**

Sdílená zodpovědnost za bezpečnost v cloudu

Shared responsibilities

Microsoft understands how different cloud service models affect the ways that responsibilities are shared between CSPs and customers.

Responsibility	On-Prem	IaaS	PaaS	SaaS
Data classification & accountability				
Client & end-point protection				
Identity & access management				
Application level controls				
Network controls				
Host infrastructure				
Physical security				
	 Cloud Customer	 Cloud Provider		

Q: Jak se staví Microsoft k použití SW při zpracování on-premise

A: MS nemá roli zpracovatele

Viz Product Terms quotation:

19. Zpracování osobních údajů

V rámci svojí role zpracovatele a dílčího zpracovatele osobních údajů v souvislosti s produktem nebo poskytováním odborných služeb společnost Microsoft přijímá závazky v souladu s obecnými podmínkami nařízení Evropské unie o ochraně osobních údajů v příloze 4 [podmínek služeb online](#) vůči všem zákazníkům s účinností ke dni 25. května 2018.

Online Services Terms (OST) – Podmínky pro služby online

- **Podmínky ochrany osobních údajů a zabezpečení – od str. 7**
 - Závazek užití dat pouze pro poskytování služeb (ne pro reklamní nebo jiné komerční účely)
 - Závazek neposkytnutí dat třetím stranám kromě vyjmenovaných situací a procesů
 - Oznámení incidentu zákazníkovi; poskytnutí podrobných informací o incidentu
 - Použití dodavatelů (pouze za účelem poskytování služeb, odpovědnost Microsoftu)
 - Umístění pro uchování dat a jurisdikce smlouvy – EU; zpracování dat – možné WW
 - Ochrana osobních údajů – vrácení / smazání dat, pracovníci, subdodavatelé
 - Vyjmenovaná bezpečnostní opatření (v členění ISO 27001) a certifikace (závazek pokračovat)
- Příloha 3: **Standardní smluvní doložky dle Rozhodnutí Komise 2010/87/EU**
- Příloha 4: **Obecné nařízení GDPR Evropské unie – platí pro všechny zákazníky**
 - Splnění povinností zpracovatele dle článků 28, 32 a 33 plus některé další závazky

OST: <http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46>

SLA: <http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=37>



Jak může zpracování v cloudu pomoci?

- Některé funkce spojené s **výkonem práv subjektů** dat (čl. 12 až 20)
 - Nalezení osobních údajů, přístup, omezení, protokolární výmaz, přenositelnost
- Reflektovat **smluvní požadavky na zpracovatele** (čl. 28)
- Pořizování **záznamů o činnostech zpracování** (čl. 30 bod 2.)
- **Zabezpečení** technických a organizačních **opatření** (čl. 32)
- Implementace **pseudonymizace a šifrování** dat (čl. 25, 32)
- Pomoc při šetření a ohlašování **bezpečnostních incidentů** (čl. 33, 34)
- **Modelové posouzení vlivu** na ochranu os. údajů – DPIA (čl. 35)
- **Kodexy chování** zpracovatelů a **certifikace** služeb (čl. 40 až 43)

Kde najdeme Security & Privacy controls

OST – Podmínky pro služby Online – seznam bezp. opatření:

- OST str. 12 – 14: seznam bezp. opatření ve struktuře ISO 27001:2013
- OST str. 14: závazek pokračovat s průmyslovými certifikacemi

Trust Center:

www.microsoft.com/trust

Podklady - členění podle:

- Rolí – Risk / Compliance / Security / BDM
- Principů – Security / Transparency / Privacy...
- Cloud. služeb – Azure, O365, D365...
- Odtud „More reports....“:

Service Trust Platform

<https://servicetrust.microsoft.com/> (vyžaduje user credentials)

také aka.ms/STP

Repository podkladů k certifikacím:

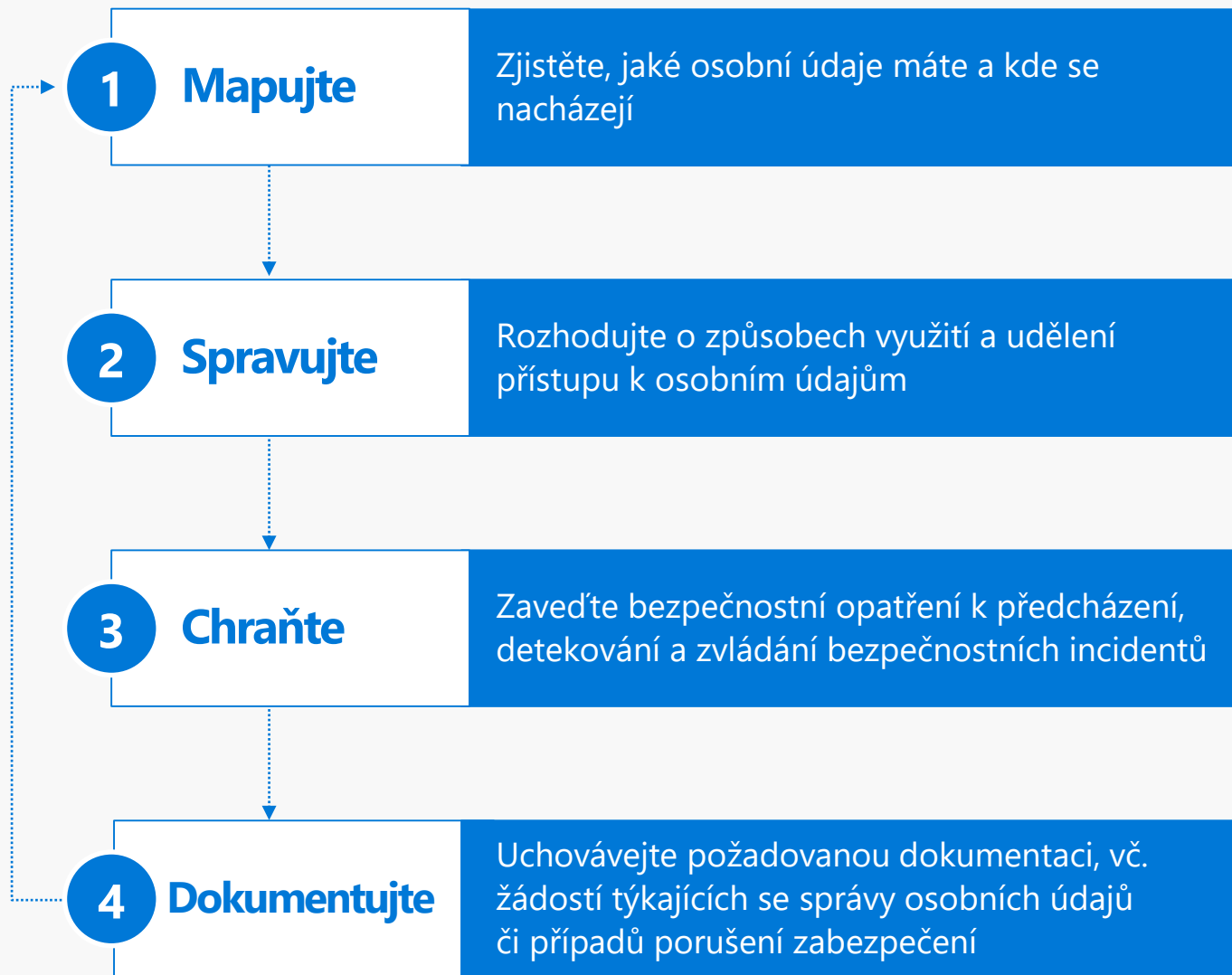
- Compliance Reports (ISO 27k a SOC reports)
- Trust documents (security whitepapers)

O365 Service Assurance

<https://protection.office.com>

The screenshot displays the 'Audited controls' page in the Office 365 Security & Compliance center. The left sidebar contains navigation links: Home, Alerts, Permissions, Security policies, Data management, Search & investigation, Reports, and Service assurance. The main content area shows the 'Audited control details' for ISO 27001:2013. It includes a search bar and a list of controls. The first section is 'A.5.1 Office 365 - Management Direction for information Security - 2 controls', which includes 'A.5.1.1 Policies for information security' and 'A.5.1.2 Review of information security policies'. The second section is 'A.6.1 Organization of Office 365 Information Security - Internal Organization - 5 controls', followed by 'A.6.2 Office 365 - Mobile devices and teleworking - 2 controls', 'A.7.1 Human resource security - Prior to employment - 2 controls', and 'A.7.2 Human resource security - During employment - 3 controls'.

Jak uchopit GDPR



1 Mapujte:

Zjistěte, jaké osobní údaje máte, kde se nacházejí, kdo/co k nim má přístup

Co všechno hledat:

Jakékoli atributy, které mohou vést k identifikaci subjektu údajů

- Jméno
- Emailová adresa
- Příspěvky na sociálních sítích
- Fyzické, fyziologické nebo genetické informace
- Info o zdravotním stavu
- Lokalizační údaje
- Bankovní údaje
- IP adresa
- Cookies
- Kulturní atributy

Inventarizace:

Identifikujte místa uchování osobních údajů, možné přístupy k nim, mapy toků dat

- Emaily
- Dokumenty
- Databáze
- Přenosná média
- Metadata
- Logy - záznamy
- Backupy

Příklady řešení

Microsoft Azure

Microsoft Azure Data Catalog

Enterprise Mobility + Security (EMS)

Microsoft Cloud App Security

Dynamics 365

Audit Data & User Activity
Reporting & Analytics

Office & Office 365

Data Loss Prevention
Advanced Data Governance
Office 365 eDiscovery

SQL Server and Azure SQL Database

SQL Query Language

Windows & Windows Server

Windows Search, Windows PowerShell

2 Spravujte:

Účely a scénáře využití údajů, správa souhlasů, pravidla přístupu k údajům

Správa dat:

Vymezení zásad, rolí a odpovědnosti při zpracování a užití osobních údajů

- Souhlas / právní titul
- Životní cyklus:
- V úložišti
- Při zpracování
- Backup
- Archivace
- Recovery
- Doba expirace
- Likvidace

Kategorizace dat:

Organizace a štitkování dat pro zajištění správného použití

- Druhy osobních údajů
- Citlivost
- Kontext / užití
- Vlastnictví dat
- Zaměstnanci
- Administrátoři
- Uživatelé

Příklady řešení

Microsoft Azure

Azure Active Directory
Rights Management Services
Azure Role-Based Access Control (RBAC)

Enterprise Mobility + Security (EMS)

Azure Information Protection

Dynamics 365

Security Concepts

Office & Office 365

Advanced Data Governance
Journaling (Exchange Online)

Windows & Windows Server

Microsoft Data Classification Toolkit

3 Chraňte:

Zavedte bezpečnostní opatření k předcházení, detekování a zvládání bezpečnostních incidentů

Prevence proti hrozbám:

Zabezpečení dat

- Fyzická ochrana datového centra
- Síťová bezpečnost
- Zabezpečení úložiště
- Počítačová bezpečnost
- Správa identit
- Řízení přístupu
- Šifrování
- Zmírňování rizik

Detekce a zvládání bezpečnostních incidentů:

- Monitorování systému (*System monitoring*)
- Identifikace bezpečnostní incidentů
- Zjišťování dopadů
- Plán pro zvládání incidentů
- Zotavení po incidentu (*Disaster recovery*)
- Metodika ohlašování dozor. orgánu
- Metodika oznamování subjektům dat

Příklady řešení

Microsoft Azure

Azure Key Vault, Azure Security Center
Azure Storage Service Encryption

Enterprise Mobility + Security (EMS)

Azure Active Directory Premium
Microsoft Intune

Office & Office 365

Advanced Threat Protection
Threat Intelligence

SQL Server and Azure SQL Database

Transparent data encryption
Always Encrypted

Windows & Windows Server

Windows Defender Advanced Threat Protection
Windows Hello
Device Guard / Credential Guard

4 Dokumentujte:

Uchovávejte požadovanou dokumentaci, vč. žádostí týkajících se správy osobních údajů či případů porušení zabezpečení

Provozní záznamy

Organizace musí zaznamenávat:

- Logy změn údajů
- Účel zpracování údajů
- Zpracování různých kategorií osob. údajů
- Přístupová oprávnění třetích stran k datům
- Organiz. a technická bezpečnostní opatření
- Doby uchovávání vs. prokazatelné smazání osobních údajů

Dokumentace

Zajistit dokumentaci:

- Dokumentaci zpracování osobních údajů, včetně cloud. „zpracovatele“
- Ohlašování a oznamování případů porušení zabezpečení
- Model správy dat
- Vyřizování žádostí subjektů dat
- Revizní zprávy o souladu
- Archivaci logů

Příklady řešení

Microsoft Trust Center
Service Trust Portal

Microsoft Azure
Azure Auditing & Logging
Microsoft Azure Monitor

Enterprise Mobility + Security (EMS)
Azure Information Protection

Dynamics 365
Reporting & Analytics

Office & Office 365
Service Assurance
Office 365 Audit Logs
Customer Lockbox

Windows & Windows Server
Windows Defender Advanced Threat Protection

Beginning your General Data Protection Regulation (GDPR) journey

Whitepaper 31 stran
Metodika 4 kroků + nástroje
i v češtině

www.aka.ms/GDPRwhitepaperCZ

Příprava na obecné nařízení o ochraně osobních údajů (GDPR)

Dosáhněte rychleji souladu s nařízením
GDPR pomocí služby Microsoft Cloud





Modelové analýzy rizik a scénáře pro DPIA

- GDPR prezentace a zdroje v CZ: www.aka.ms/jaknaGDPR
k dispozici modelové analýzy rizik pro zákazníky (v češtině):
 - Analýza rizik: **Zdravotnická dokumentace v cloudu Azure** (ICZ a.s.)
 - Znalecký posudek ústavu CETAG: adekvátní úroveň zabezpečení dle GDPR
 - Analýza rizik: **Spisová služba Gordic GINIS v cloudu Azure** (RAC s.r.o.)
 - **Formát DPIA pro zpracování osobních údajů v Office 365** (ICZ a.s.)
 - Osobní údaje v Exchange Online
 - Citlivé osobní údaje v SharePoint Online
 - Telemedicína / citlivé osobní údaje přes a upload přes Skype for Business
- Soulad s požadavky GDPR ověřen právní kanceláří Pierstone s.r.o.

S.ICZ a.s.

Na hřebenech II 1718/10
140 00 Praha 4

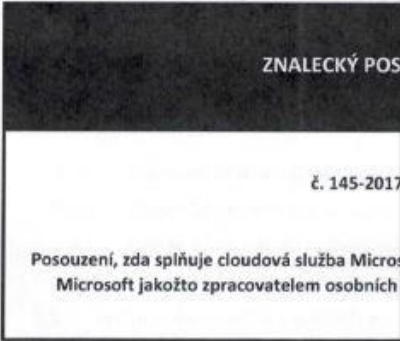
Na posouzení právních aspektů sp
PIERSTONE s.r.o., advok
Na Příkopě 9
110 00 Praha 1

Analýza rizik a
zdravotn

Studie zpracovaná n

Dokument:	MICR01451-STUDIE
Zakázka:	MICR.01451
Zpracoval:	Ondřej Steiner a kol
Datum:	16.12.2016

PIERSTONE s.r.o.
IČ: 27451925
Na Příkopě 9
110 00 Praha 1
www.pierstone.com



Objednatel: MICROSOFT s.r.o.
IČ: 47123737
Vyskočilova 1561/4a
140 00 Praha 4

Zhotovitel: Ústav kvalifikovaný pro zna
Cetag, s.r.o.
IČ: 27451925
Na Poříčí 1070/19
110 00 Praha 1

Účel posudku: Právní úkony objednatele

V Praze, dne 15. dubna 2017

Znalecký posudek se vydává písemně ve třech
předávají objednateli a jedno vyhotovení se ukládá
ústavu. Posudek má celkem -42- stran, z toho -46-

Analýza rizik provozu spisové služby
v Microsoft Azure
v1.1 (Final)
Dokument ze dne 23.12.2016

S.ICZ a.s.

Na hřebenech II 1718/10
140 00 Praha 4

Na posouzení právních aspektů spolupracovala
PIERSTONE s.r.o., advokátní kancelář
Na Příkopě 9
110 00 Praha 1

Modelová DPIA a analýza rizik pro zpracování
osobních údajů v Microsoft Office 365

Studie zpracovaná na základě poptávky Microsoft s.r.o.

Dokument:	MICR01817-STUDIE-110.docx		
Zakázka:	MICR.01817	Verze:	1.1
Zpracoval:	Kolektiv autorů S.ICZ	Stav:	finální
Datum:	10.4.2017	Počet stran:	137

Široké portfolio certifikací a mezinárodních standardů

Certifikace a podklady: Microsoft Trust Center www.microsoft.com/trust; Repository: www.aka.ms/STP

GLOBAL



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

INDUSTRY



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

REGIONAL



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

Shrnutí



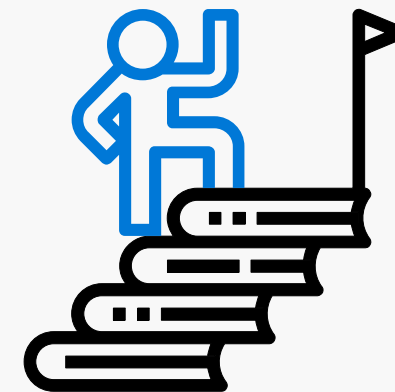
Zjednodušení cesty k souladu

Využijte ověřená řešení v cloudu s využitím delegace odpovědností na zpracovatele



Posouzení rizik a realizace opatření

Využijte služby a nástroje pro pokrytí rizik a pružné zavedení adekvátních bezpečnostních opatření



Využití expertních znalostí

Unikátní kompetence partnerské sítě spol. Microsoft v oblasti řízení rizik, procesů, a právního poradenství

Zdroje k GDPR:

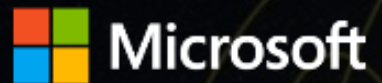
Microsoft Corp hlavní stránka:
microsoft.com/GDPR

Prezentace a zdroje v češtině:
aka.ms/jaknaGDPR

Microsoft Trust Center
microsoft.com/trust

Service Trust Platform – podklady k certifikacím,
auditní zprávy: aka.ms/STP
(vyžaduje log-in, NDA level)





VYUŽITÍ CLOUDOVÝCH SLUŽEB MICROSOFT A UKÁZKY ŘEŠENÍ

This presentation is intended to provide an overview of GDPR and is not a definitive statement of the law.

Proboha, co s tím??? A proč?



§



Cesta, jak se stát a zůstat **GDPR compliant**



**OPERATIVA
OCHRANA
AKTUALIZACE**

DATA - APLIKACE – TECHONLOGIE – ZABEZPEČENÍ

**PROCESY
ŠKOLENÍ**



**ROZDÍLOVÁ
ANALÝZA**

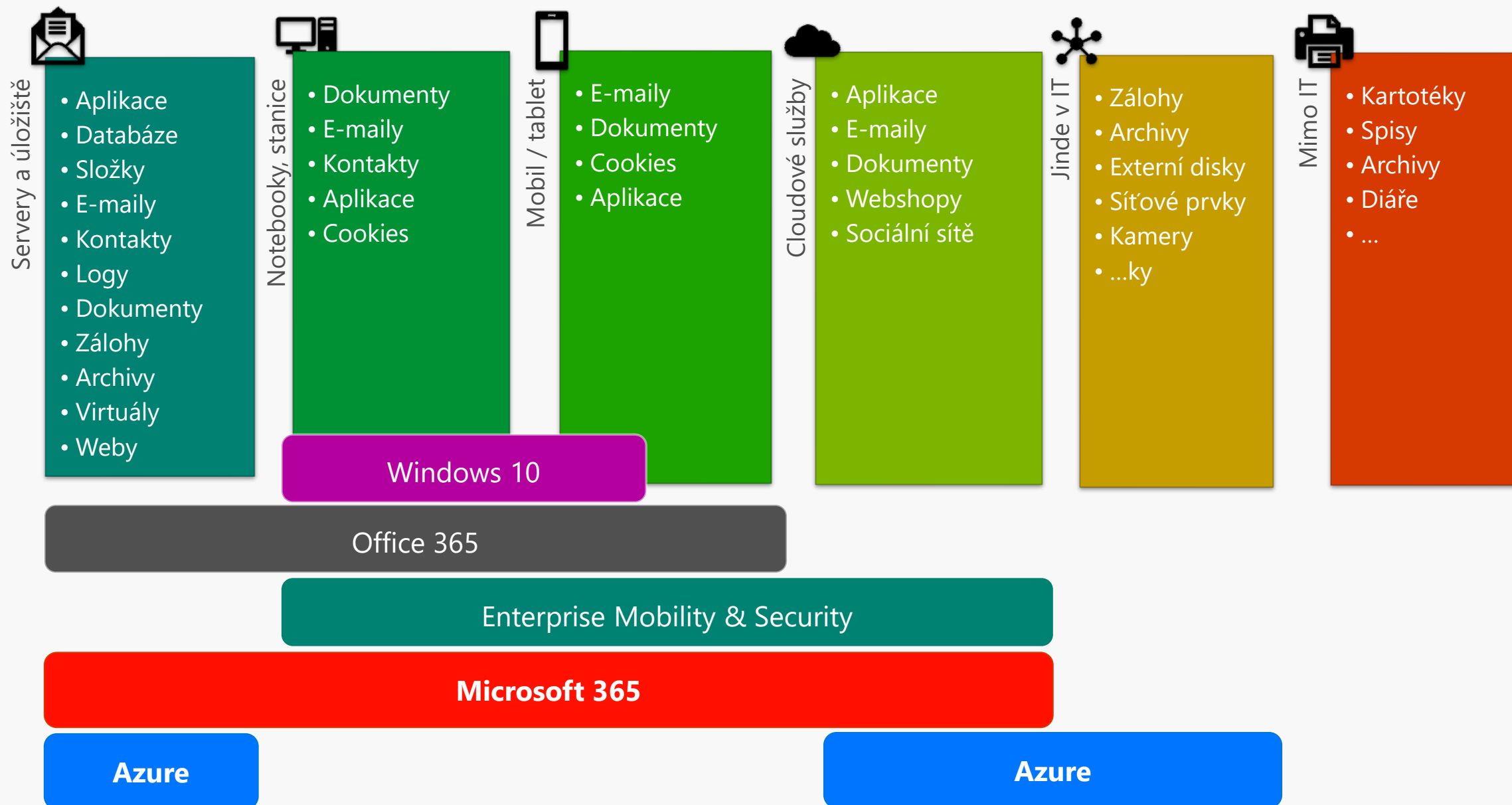


**POSOUZENÍ VLIVU
DPIA**



25. květnem 2018 to nekončí. Naopak začíná.
Ujistěte se, že máte pokryty všechny potřebné
procesy,
aby vás v budoucnu nic nepřekvapilo.

Kde všude leží data s osobními údaji?



Využití podle služeb



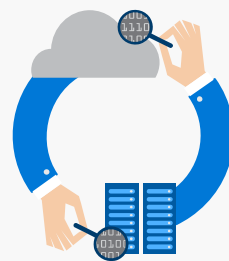
Office 365 pro GDPR

Maximální využití technického, bezpečnostního i organizačního zajištění všech cloudových služeb

- Multifaktorová autentizace, ochrana před kybernetickými útoky, přístup řízený zákazníkem, šifrování dat, smluvní závazky a SLA....

Ochrana informací s osobními daty

- **Zabezpečení dokumentů a e-mailů** – možnost zneplatnění a omezení přístupu bez ohledu na jejich umístění, omezení odeslání, nastavení politik a analýza jejich dodržování
- **Vyhledání** dokumentů, e-mailů, kontaktů s osobními údaji a informací na stánkách napříč systémem Office 365 pomocí funkce eDiscovery pověřenými osobami
- **Minimalizace výskytu** stejných dokumentů s osobními údaji jejich jednoduchým sdílením a ne kopírováním pomocí e-mailových příloh – propojení s aplikacemi Office
- Možnosti **vytvoření agend** spojených se zajištěním výkonu práv subjektů – workflow, záznamy žádostí a jejich vyřízení



EMS - příběhy

Zajištění zařízení, ze kterého se přistupuje k osobním údajům

- Zabezpečení stanic a mobilních zařízení proti neoprávněnému přístupu – pravidla, šifrování, správa
- Vymazání obsahu zařízení v případě odcizení nebo ztráty

Zajištění bezpečného ověření oprávněného uživatele

- Snížení možnosti zneužití přístupu nebo sdílení hesla pomocí multifaktorové autentizaci pro přístup k firemním aplikacím
- Analýza hrozeb v lokální síti, spojená se zneužitím přístupů

Omezení přístupu k dokumentům s osobními údaji bez ohledu na jejich umístění

- Ochrana šifrováním a omezením přístupu k dokumentům s osobními údaji
- Možnost zneplatnění dokumentů s osobními údaji bez ohledu na jejich umístění

Monitorování potencionálních rizik spojených s cloudovými službami



Windows 10 - příběhy

Zabezpečení zařízení proti napadení a odcizení dat

- **Proaktivní ochrana** proti Ransomware a dalšímu škodlivému kódu pomocí Device Guard a Applocker.
- **Integrovaný antivirový systém** Windows Defender Antivirus chrání i proti malware, který ještě nebyl nikde použit

Zabezpečené informace při odcizení nebo ztrátě

- **Firemní a informace osobní data** na zařízeních a uložiscích zabezpečená pomocí technologie Windows Information Protection a Azure Information protection
- **Šifrování obsahu pevného disku** technologií Bitlocker chrání zařízení v případě ztráty nebo odcizení
- **Odolnost proti** útokům zneužívající **zcizení hesla** z paměti zařízení pomocí funkce Credential Guard
- **Zabezpečená identita oprávněného uživatele**
Vestavěná podpora vícefaktorového ověření uživatele Windows Hello for Business.



Microsoft 365 - příběhy

Kombinace Windows, Office 365 a EMS

- **Ochrana koncových zařízení** před odcizením informací
- **Zajištění před neoprávněným přístupem** k zařízení a aplikacím s osobními údaji
- **Ochrana před hroby útoků** a odcizení dat v síti
- **Ochrana dokumentů a e-mailů** s osobními informacemi šifrováním
- Aplikace **Office pro bezpečnou** a efektivní **produktivitu**
- **Certifikované** cloudové **prostředí** pro e-maily a dokumenty
- **Licenční zajištění** Windows a Office 365 jako služby
- **Stále aktuální** prostředí z pozice bezpečnosti i funkcí



Azure příběhy

Management & Security

Předcházení bezpečnostních incidentů

- **Integrace systémů do jednoho globálního pohledu** ze všech komponent on-prem i cloudu – sítě, servery, identity, SIEM
- Doporučení pro **zabezpečení monitorované infrastruktury** napříč platformami – Windows, Linux, OpenStack, Vmware...
- Zabezpečení **proti zásahu administrátora**

Rychlost reakce na incident

- **Notifikace o incidentech** (SMS, e-mail, push, dashboard, mobilní aplikace)
- **Zpětné dohledání** incidentů po dobu až 24 měsíců s neomezeným prostředky – storage, výkon, analýzy...
- **Vyhledání událostí** nebo incidentů spojených s konkrétním uživatelem nebo systémem

Využití podle rozsahu zpracování



Běžné zpracování Bez rizika (bez DPIA)

Využití technického, bezpečnostního i organizačního zajištění cloudových služeb MS

- Zabezpečení infrastruktura, multifaktorová autentizace, ochrana před kybernetickými útoky, šifrování dat, smluvní závazky a SLA...
- **Migrace do Office 365, infrastruktura do Azure Iaas**

Ochrana informací s osobními daty

- **Zabezpečení dokumentů a e-mailů** – možnost zneplatnění a omezení přístupu bez ohledu na jejich umístění, omezení odeslání, nastavení politik a analýza jejich dodržování
- **Vyhledání** dokumentů, e-mailů, kontaktů s osobními údaji a informací na webech napříč systémem Office 365 pomocí funkce eDiscovery pověřenými osobami
- **Minimalizace výskytu** stejných dokumentů s osobními údaji jejich jednoduchým sdílením a ne kopírováním pomocí e-mailových příloh – propojení s aplikacemi Office
- **Využití vlastností Office 365 E3**



Rizikové zpracování Citlivé, hromadné... (potřebné DPIA)

Vše ze základního scénáře

Nejvyšší úroveň zabezpečení infrastruktury, aplikací, uživatelů i zařízení

- Předcházení bezpečnostních incidentů a včasná reakce na incident
- Zajištění zařízení, ze kterého se přistupuje k osobním údajům proti krádeži, neoprávněnému uživateli i útokům
- Monitorování potencionálních rizik spojených s cloudovými službami

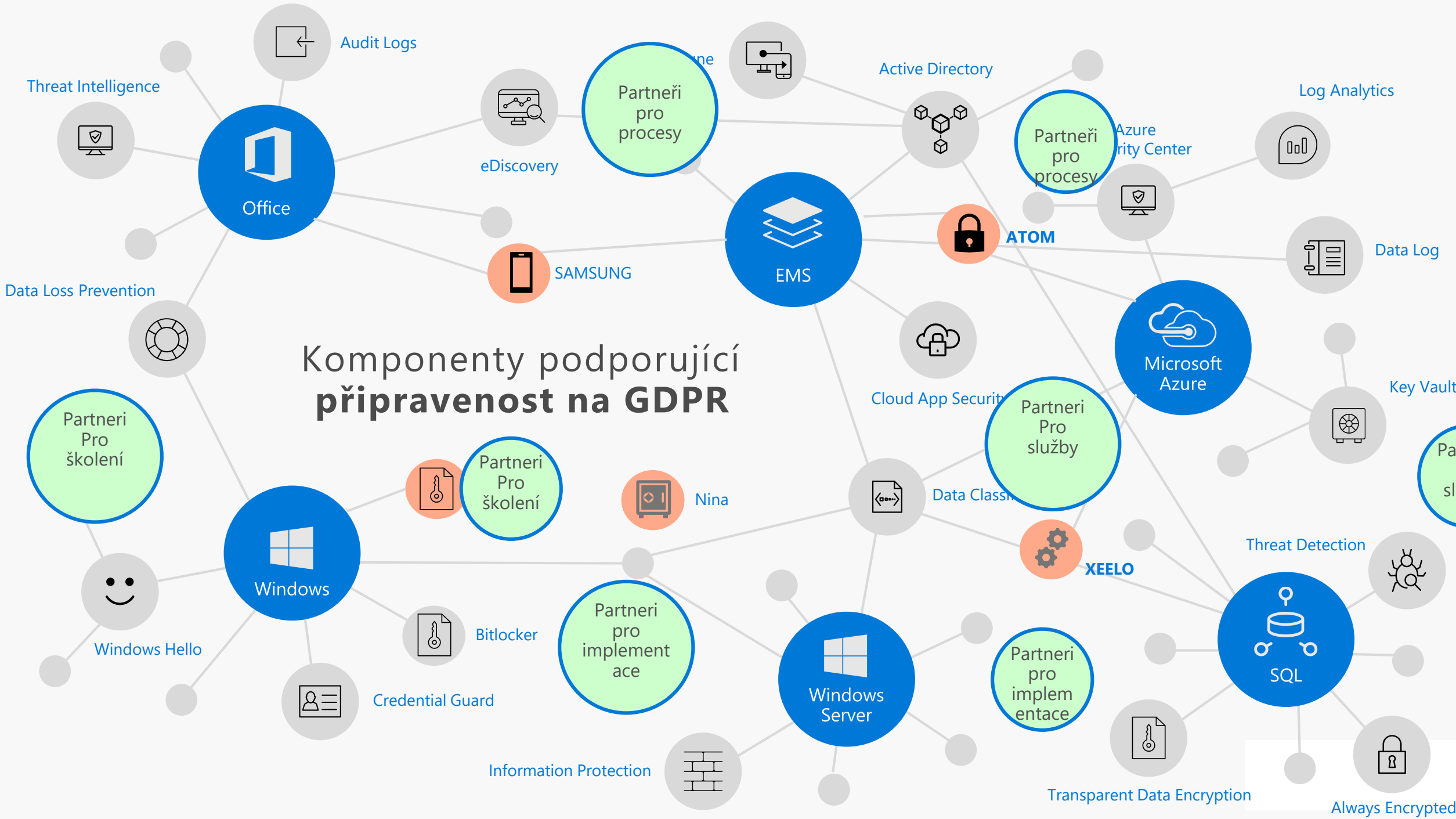
Funkce Azure OMS, O365 E5, Win 10, EMS, M365 E5

Vytvoření nových aplikací a agend splňujících GDPR

- Vytváření aplikací pro podporu GDPR, které nahradí nevyhovující aplikace
- Centralizace agend a osobních informací do centrálního systému
- Partnerská řešení pro podporu GDPR
- **Nové aplikace v Azure PaaS, Dynamics 365**
- **Partnerské aplikace pro GDPR (KPCS Atom, Xeelo...)**

Partnerská řešení pro GDPR

využívající Microsoft Cloud



XEELO

Don't complain. Just comply

XEELO GDPR SOLUTION

Cesta, jak se stát a zůstat **GDPR compliant**



**OPERATIVA
OCHRANA
AKTUALIZACE**

**PROCESY
ŠKOLENÍ**



**ROZDÍLOVÁ
ANALÝZA**



**POSOUZENÍ VLIVU
DPIA**



Podpora **DPIA**



Podpora **žádosti subjektu údajů**



Co je sbaleno v Xeelo GDPR

99

GDPR
ČLÁNKŮ



38

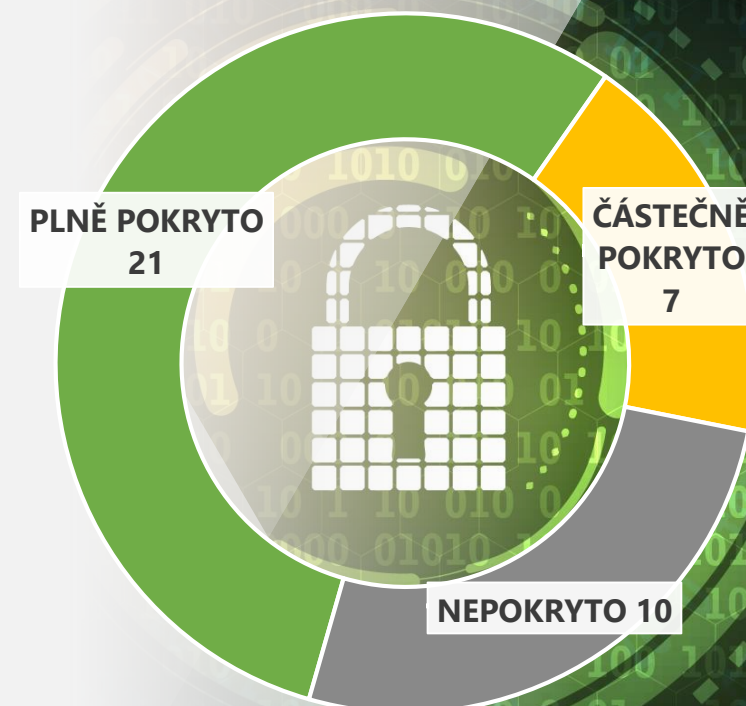
RELEVANTNÍCH
PRO FIRMY



28

POKRÝVÁ
XELO GDPR
Ostatní je organizace

ZBYTEK JE např. nominace DPO, závazná podniková pravidla, odpovědnost za škodu, konzultace s dozorovým úřadem apod.



Posouzení vlivu na OOÚ

- Audit
- SA Otázka
- SA Dotazník
- Nedostatky
- Řízení rizik

Mapování dat

- Organizace
- Datový zdroj
- Datová tabulka
- Datová položka

Kmenová data

- Dodavatel
- Zákazník
- Osoba
- Segment
- Asset
- Person (Help - E/I)

Operativní

- Dokument
- Trénink
- Incident
- Požadavek na změnu
- Externí žádost

Moje data

- Můj dotazník
- Můj dokument
- Můj trénink
- Článek
- Často kladené dotazy

Super hlavní data

- Správce
- Typ dat
- Typ zabezpečení
- Typ právního souhlasu
- Typ zákonného rámce

Co vás čeká **po 25. květnu 2018**



EXTERNÍ ŽÁDOSTI

Když někdo požádá o detekci dat...



ZÁKONNÝ RÁMEC & PRÁVNÍ SOUHLAS

Abyste měli souhlas se zpracováním dat...



ŘÍZENÍ INCIDENTŮ

Když k něčemu přece jen dojde...



ZMĚNOVÉ POŽADAVKY

Když bude potřeba změnit IT systémy...



ŠKOLENÍ A EVIDENCE ÚČASTNÍKŮ

Pro prokázání proběhlých školení...



DISTRIBUCE INTERNÍCH SMĚRNIC

Pro prokázání, že informujete zaměstnance...



ZÁZNAMY O ZPRACOVÁNÍ

Když se rozhodnete změnit to, jak fungujete...



MIGRACE DAT DO ZEMÍ MIMO EU

Když moje data opouští EU...



ŘÍZENÍ RIZIK

Abyste mohli řídit a vyhodnocovat rizika...



FAQ & SMĚRNICE

Když potřebujete přesné znění...

Co vás čeká **po 25. květnu 2018 s XEELe**



ZÍSKÁTE PŘEHLED NAD SYSTÉMY V CELÉ FIRMĚ

Důvod zmapovat vaše systémy a data



OPATŘÍTE SI PODKLADY A ZMÍRNÍTE SANKCE

Budete moci říct, že jste udělali maximum



ZÍSKÁTE MOŽNOST CENTRALIZOVAT VAŠE DATA

Budete mít jedno místo pravdy a zbavíte se duplicitního zadávání



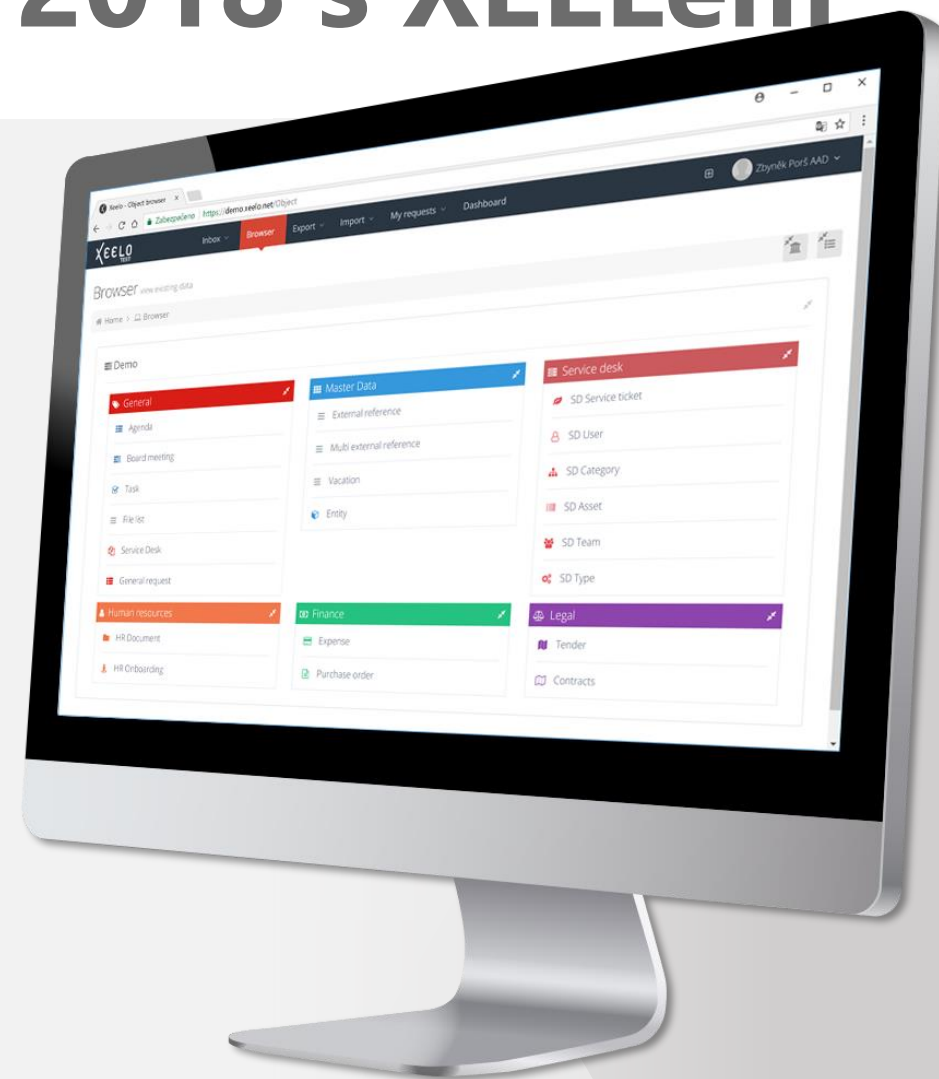
DOSTANETE VÍCE PROCESŮ POD KONTROLU

Využijte to jako příležitost digitalizovat vaši firmu



VYBUDUJTE SI JEDNOTNOU VRSTVU NA ŘÍZENÍ WORKFLOW

Dejte vašim zaměstnancům jednotné prostředí pro jejich dennodenní úkoly



Vystoupejte na **nejvyšší horu**

Vyřešte všechny procesy a zůstaňte GDPR compliant

25. květnem 2018 to nekončí. Naopak začíná.
Ujistěte se, že máte pokryty všechny potřebné procesy,
aby vás v budoucnu nic nepřekvapilo.





www.xeelo.com/gdpr



Advanced Threat & Operation Monitoring

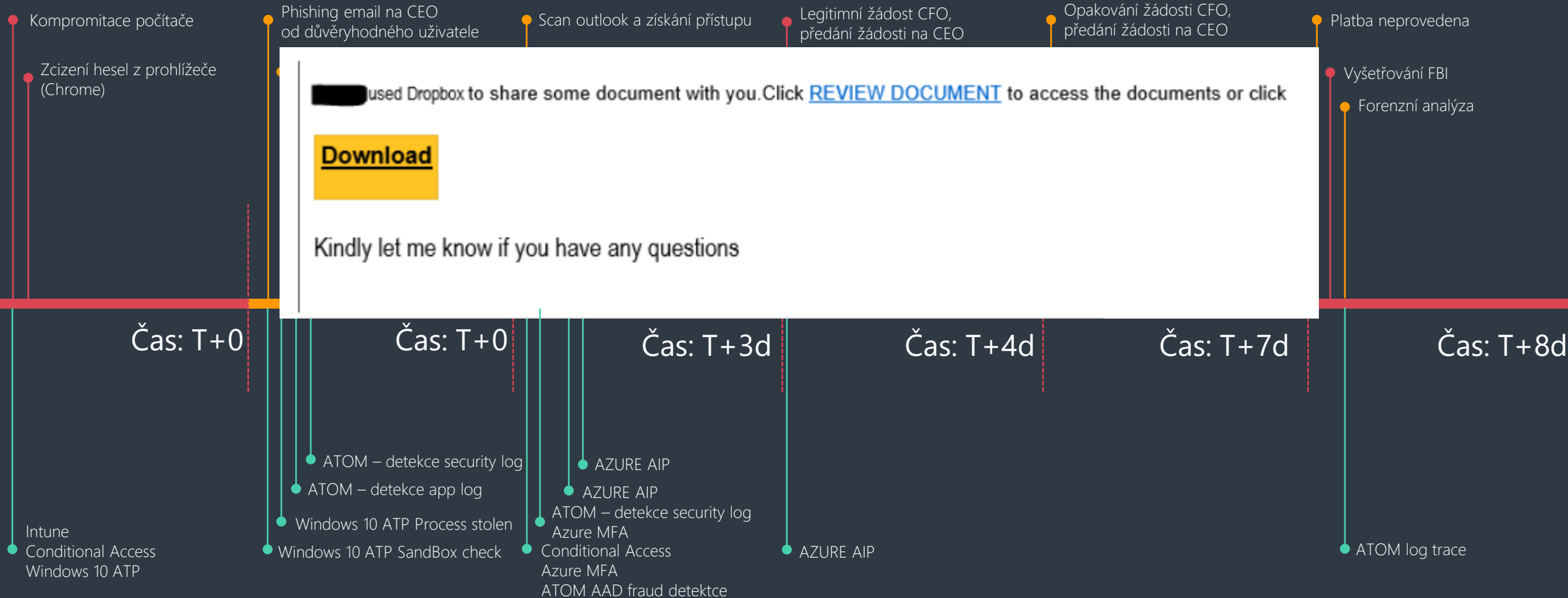
Svět se již změnil



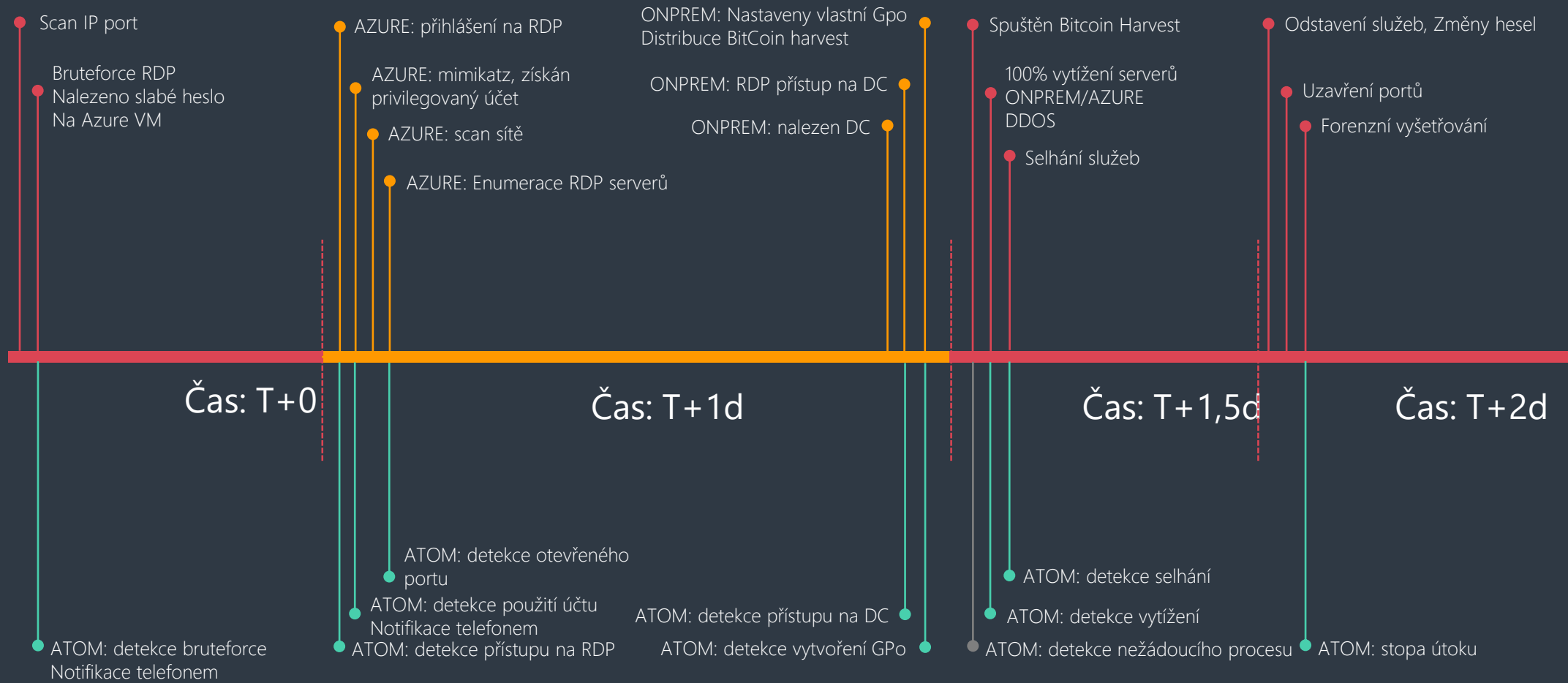
§



Skutečné příběhy... dějství první



Skutečné příběhy... dějství druhé



ATOM, KPCS a GDPR Article 32 section 1 lit b. GDPR

Integrita

- Kontrola změn služeb
- Kontrola změn souborů
- Kontrola síťového provozu
- Kontrola přihlášení ke koncovému bodu

Dostupnost

- Network monitoring
- Performance monitoring
- Event management
- Health check lite

Odolnost

- Porovnání s baseline
- Vyhodnocení best practice
- Service Map a vazby služeb, procesů a systémů

Důvěrnost

- Kontrola skupin AD
- Kontrola lokálních skupin
- Kontrola chování uživatele
- Integrace s ATA a SIEM
- Kontrola DNS dotazů

Pre
Assessment

Personal Data
Assessment

Risk Analysis
& Measures

Mandatory Measures

GDPR EFFECTIVE
25.5.2018

Continuous Data Privacy Management

Measures Implementation

ATOM



Vybudováno na Microsoft Azure
Flexibilní, škálovatelné, bez geografického omezení, řada bezpečnostních certifikací



Nepotřebuje žádné investice
Model pay-as-you go, základní verze zdarma, rychlé nasazení



Zaměřte se na důležité
Expertní znalost konzultantů obsažena v produktu, upozornění na problémy ohrožující bezpečný a bezproblémový chod



Bezpečnost, podpora GDPR
Využití pro GDPR, bezpečnostní audit a bezproblémový provoz IT, mobilní klient



Detailní reporty
Každý týden report na váš e-mail, dle zvolené varianty bezpečnostní doporučení



Žádná omezení, žádné limity
Jakýkoliv server, jakýkoliv cloud, Windows, Linux, síťové prvky

Azure OMS – základ ATOM



AD Assessment

3
Servers Assessed
in last 21 days

0
High Priority Recommendations

3
Low Priority Recommendations

104
Passed checks

Alert Management

576
Active critical alerts in the last...

0
Active warning alerts in the la...



Antimalware Assessment

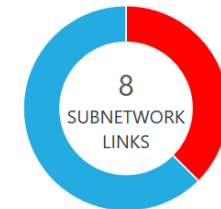


Active Threats
0

Remediated Threats
0

Insufficient Protection
2

Network Performance Monitor



Unhealthy Subnetwork Li...
3

Healthy Subnetwork Links
5

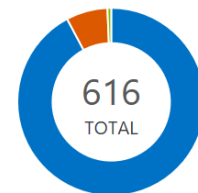
Service Map

7
Machines reporting
(Last 30 min)

8
All-time machines reporting

8 **0**

Office 365



AzureActiveDirectory
568

Exchange
44

OneDrive
4

DNS Analytics (Preview)

0
Malicious Activity
(Last 24 hours)

3
DNS Servers

SQL Assessment

1
Servers Assessed
in last 21 days

1
High Priority Recommendations

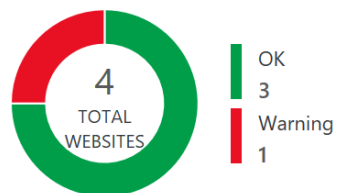
2
Low Priority Recommendations

34
Passed checks

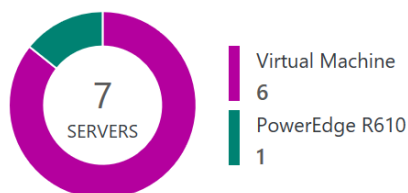
Vlastní doplněná řešení ATOM



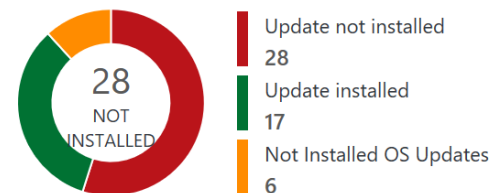
Web Probe



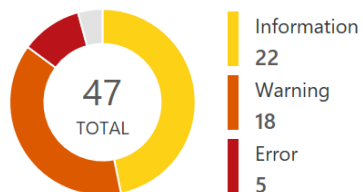
Windows Hardware and Software Inventory



Windows Update Management



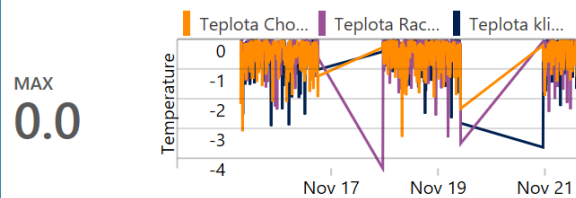
Advanced Threat Analytics



Logon Activity Web Service

8.5k
Types of data

Environment Probe - Sample Data

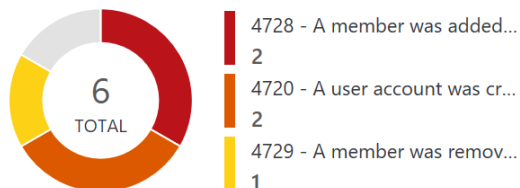


Logon to Remote Desktop Service

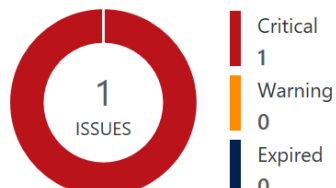
82.6k
Failed Logon

42
Success Logon

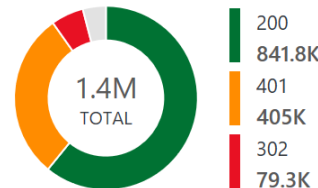
Change in privileged groups



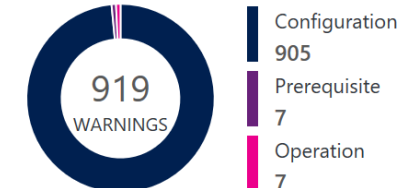
Local Certificates Status



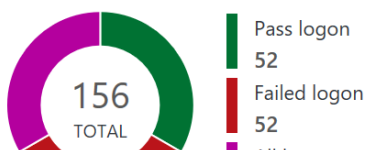
IIS Status



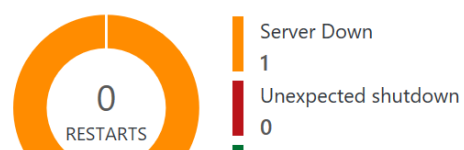
Best Practice Analyzer



Monitoring Access Project Honolulu



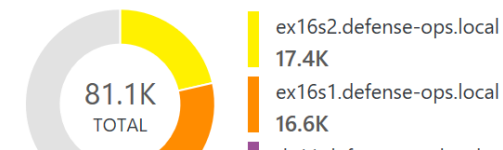
Operating system HealthCheck Lite



Local Users and Groups Assessment



Task Scheduler Status



Každé řešení má detail



Change in privileged groups

[More info](#) →

Information Part

Active Directory contains a few critical security groups – Privileged Groups. These are built-in groups in Active Directory that have been granted various levels of permissions in the both domain and forest, starting with full administrative permissions (Enterprise Admins, Domain Admins, Administrators, Schema Admins) to more limited, but still significant, permissions (Account Operators, Server Operators, DNSAdmins). Changes to these groups may affect proper Active Directory functionality and security.

Prerequisite

Please make sure to enable appropriate auditing policy using Default Domain Controllers GPO.

USER MANAGEMENT

Who Changed User Accounts



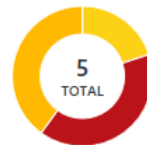
DEFENSE-OPS\dan
7

MODIFIED BY	MODIFIED OBJECT	CHANGES
dan	WKSAdmin	2
dan	wksadmin	2
dan	Organization Managem...	2
dan	josef.stasa	1

[See all...](#)

ALL CHANGES IN SECURITY GROUPS

All changes in Security Groups

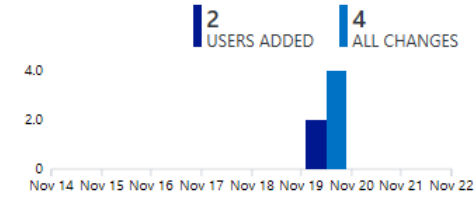


None 1
Domain Admins 2
Organization Management 2

MODIFIED GROUP	ADDED MEMBERS
None	1
Domain Admins	2
Organization Management	2

[See all...](#)

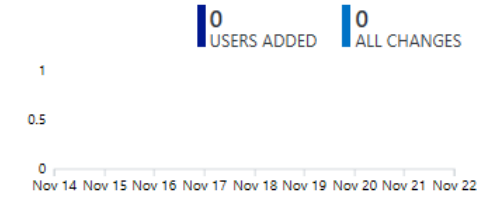
DOMAIN ADMINS MEMBERSHIP



MODIFIED BY	CHANGES
DEFENSE-OPS\dan	2

[See all...](#)

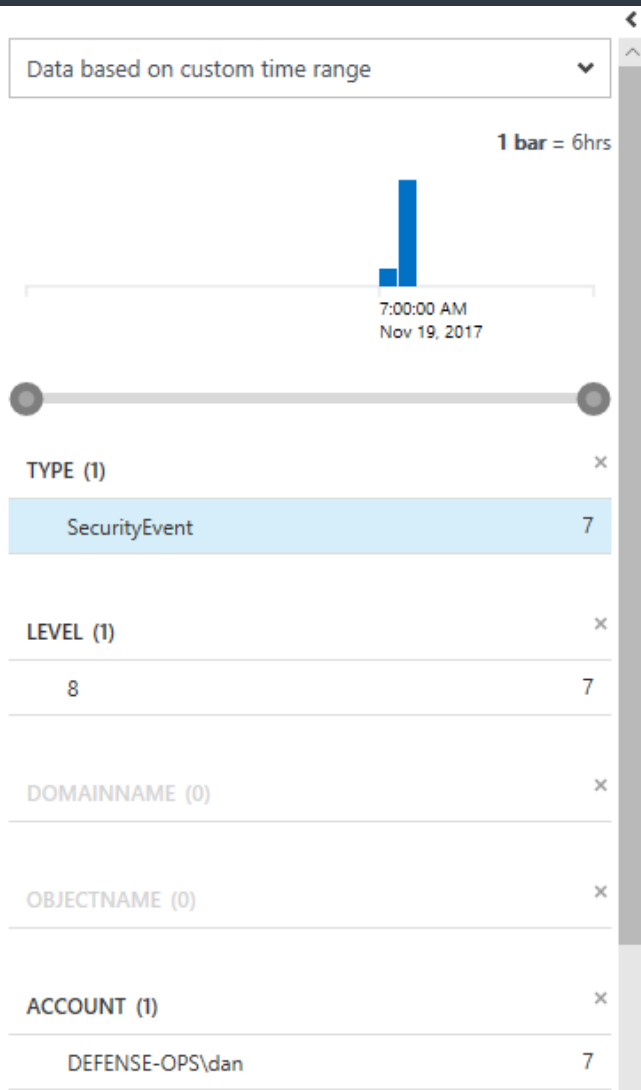
ENTERPRISE ADMINS MEMBERSHIP



MODIFIED BY	CHANGES
-------------	---------

[See all...](#)

Nebo úplný detail – audit trail



Show legacy language converter

```
SecurityEvent  
| where (EventID == "4755" or EventID == "4756" or EventID == "4720" or EventID == "4722" or EventID == "4725" or EventID == "4726" or EventID == "4730")  
| where Account == "DEFENSE-OPS\dan"
```

7 Results [List](#) [Table](#) [Computer Security](#)

11/19/2017 3:38:43.767 PM | SecurityEvent

... TimeGenerated : 11/19/2017 3:38:43.767 PM
... Account : DEFENSE-OPS\dan
... Computer : WEB1.defense-ops.local
... Level : 8
... Activity : 4720 - A user account was created.

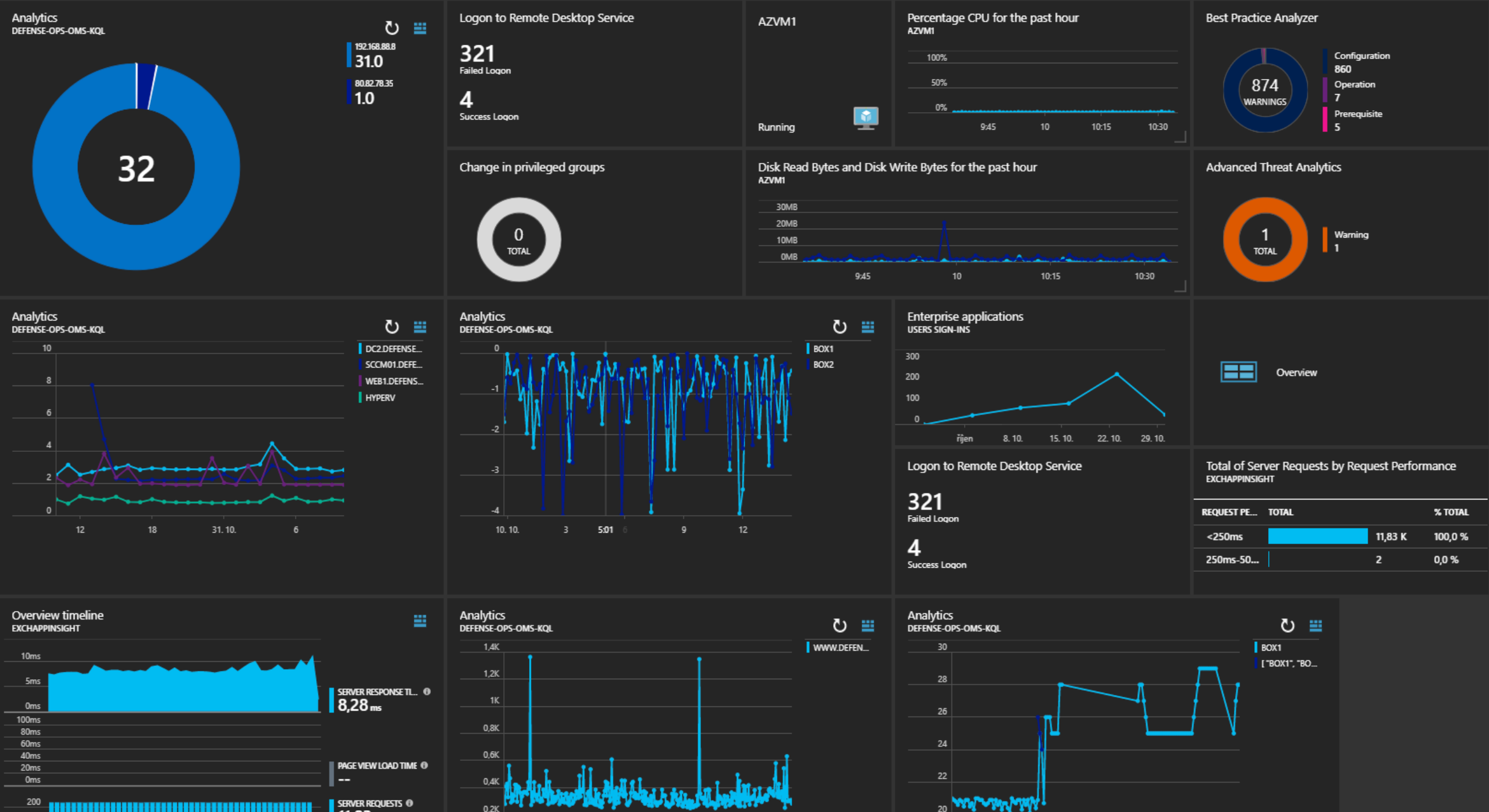
[+] show more

11/19/2017 3:38:43.823 PM | SecurityEvent

... TimeGenerated : 11/19/2017 3:38:43.823 PM
... Account : DEFENSE-OPS\dan
... Computer : WEB1.defense-ops.local
... Level : 8
... Activity : 4722 - A user account was enabled.

[+] show more

11/19/2017 3:43:09.657 PM | SecurityEvent



Ale nemusím být odborník ATOM report



1 OVERVIEW

This document represents the actual state of your environment as collected, processed and cleansed from False Positives. It shows how your environment fares from different perspectives.

The **severity** grade is based on our own experience, also a reference of Microsoft, reflecting typical Impact and Probability ratings. However, risks are perceived differently in each organization, therefore we recommend analyzing the results further with your organization priorities and needs on mind.

This report is intended for a general overview and even though it is represented by sum of issues (issue / asset), considering its configuration or actual state.

Your current rating is 1/4 and you reached 24% from the maximum points.



Figure 1: Environment Rating

In this report, following servers, roles and applications were examined in your environment.

DESCRIPTION	VALUE
Total Count of Servers	7
Total Count of AD Domain Controllers	2
Total Count of SQL Servers	1

Hodnocení
prostředí jako
celku



2 MANAGEMENT SUMMARY

This is the most significant part of the report, which offers insight to the state of your environment and points out the most serious problems. For more details, check out the ATOM portal, where you can find more information, including mitigation tips, for the discovered issues. "Last report issues" section shows how the environment is trending, so you can compare the values and see, which direction it is trending. New checks are added continuously to extend the reach into your environment.

Carefully look through this section and when you need more details, the "Click here" link will lead you to the ATOM portal to the right Intelligence Pack, where you can find them.

	NUMBER OF ISSUES	LAST REPORT ISSUES	NUMBER OF SUCCESS TESTS	MORE INFORMATION
Active Directory Assessment				
Security and Compliance	0	0	26	Click here
Availability and Business Continuity	0	0	141	Click here
Performance and scalability	0	0	32	Click here
Upgrade Migration and Deployment	0	0	9	Click here
Operations and Monitoring	0	0	4	Click here
SQL Assessment				
Security and Compliance	0	0	5	Click here

Klikni pro detail
– konzole ATOM



Bezpečnost je výzva

- Nedostatek zdrojů – technických / lidských
- Spousty (nebo žádné) nástrojů na monitoring
- Je nutné být v souladu s GDPR ve 2018

ATOM: získává data pro reportování potenciálních průniků

Správa systémů příliš komplexní

- Je nesnadné porozumět diagnostickým informacím z nástrojů.
- Nebo je informací moc
- Hybridní multi OS prostředí

ATOM: reporty obsahují znalosti „jak na to“ u podstatných problémů jak bezpečnost, tak operations

Nechcete investovat / již monitorujete

- Model Pay-as-you go.
- Není nutná implementace, bez investic.
- Propojení stávajících systémů

ATOM: připraven za 15min, report po prvním týdnu. Propojení SCOM, Zabbix a další



Nemáte čas na
analýzu

Chybí Vám
znalosti

Prostředí je
příliš složité

Každý týden report ve vašem e-mailu

- Obsahuje to nejdůležitější, včetně doporučení nápravy
- Zaměříte se na ty nejdůležitější problémy v prostředí
- Sledujte změny, mějte dokumentaci prostředí aktuální
- Nemusíte být expertem na všechny systémy, abyste zajistili jejich efektivní chod
- Volitelně – s nápravou pomůžeme, garantované SLA (v EU) pro kritické a bezpečnostní problémy

Dělejte správná rozhodnutí ve správný čas



Složitě věci, snadno pochopitelné





www.ATOM.ms | atom@atom.ms



Zdroje k GDPR:

Microsoft Corp hlavní stránka:
microsoft.com/GDPR

Prezentace a zdroje v češtině:
aka.ms/jaknaGDPR

Microsoft Trust Center
microsoft.com/trust

Service Trust Platform – podklady k certifikacím,
auditní zprávy: aka.ms/STP
(vyžaduje log-in, NDA level)





Děkuje Vám za pozornost

Jiří Černý

jjiric@microsoft.com

Vlastimil Tesař

vlastimil.tesar@microsoft.com