Microsoft

GDPR Akademie – 2. část

Zajištění bezpečnosti provozu vašich aplikací s osobními daty a partnerská řešení pro podporu GDPR

Martin Hruška, Vlastimil Tesař, Tomáš Králik, Ondřej Výšek, Zbynek Pors, Martin Imrich

Vymezení pojmů, Microsoft & GDPR

Vlastimil Tesař

Agenda

- Vymezení základních pojmů, Microsoft a GDPR
- Přehled řešení Microsoft pro zabezpečení infrastruktury a aplikací
- Bezpečnostní a provozní monitoring
- Zabezpečení cloudových služeb a uživatelských přístupů
- Zabezpečení uživatelských přístupů
- Partnerská řešení pro podpodru GDPR
  - Zabezpečení infrastruktury pomocí služby Advanced Threat Operations Management
  - Zabezpečení pomocí DLP systému na koncových stanicích
  - Aplikace pro řízení požadavků a agend GDPR

Hlavní principy General Data Protection Regulation

- Obecné „nařízení“ o ochraně osobních údajů (přímo aplikovatelné v ČR)
- Transparentnosti při zpracování a používání osobních údajů
- Nově definovaná práva fyzických osob („subjektů údajů“)
- Omezení zpracovávání osobních údajů pouze na stanovené a opodstatněné účely
- Omezení ukládání osobních údajů pouze na dobu nezbytnou pro daný účel
- Zajištění ochrany osobních údajů pomocí náležitých postupů zabezpečení

- Týká se všech organizací v EU nebo pracujících s osobními údaji rezidentů EU
- Účinnost od 25.5.2018
- Sankce až €20m nebo 4% celosvět. obratu společnosti (ve veřejné správě bude „cap“)

Organizační a technická opatření

- Osobní údaje by měly být zpracovávány způsobem, který zaručí náležitou bezpečnost a důvěrnost těchto údajů, mimo jiné za účelem zabránění neoprávněnému přístupu k osobním údajům a k zařízení používanému k jejich zpracování nebo jejich neoprávněnému použití.
- Není-li porušení zabezpečení osobních údajů řešeno náležitě a včas, může to fyzickým osobám způsobit fyzickou, hmotnou či nehmotnou újmu, jako je ztráta kontroly nad jejich osobními údaji nebo omezení jejich práv, diskriminace, krádež nebo zneužití identity, finanční ztráta…
- Mělo by být zjištěno, zda byla zavedena veškerá vhodná technická a organizační opatření, aby se okamžitě stanovilo, zda došlo k porušení zabezpečení osobních údajů, a aby byly dozorový úřad a subjekt údajů neprodleně informovány.
- Jakmile se tedy správce o porušení zabezpečení osobních údajů dozví, měl by je bez zbytečného odkladu, a je-li to možné, do 72 hodin poté, co se o něm dozvěděl, ohlásit příslušnému dozorovému úřadu, ledaže může v souladu se zásadou odpovědnosti doložit, že je nepravděpodobné, že by dané porušení zabezpečení osobních údajů mělo za následek riziko pro práva a svobody fyzických osob.
- Při vytváření podrobných pravidel týkajících se formátu a postupů ohlašování případů porušení zabezpečení osobních údajů by měly být náležitě zohledněny okolnosti porušení, včetně otázky, zda byly osobní údaje chráněny vhodnými technickými opatřeními, jež pravděpodobnost zneužití totožnosti a jiných forem zneužívání účinně omezují…

Vymezení rolí v GDPR ve vztahu k Microsoftu

- Správce / Prevádzkovateľ : osoba, nebo orgán veřejné moci, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů *(firemní zákazník, Vy)*

- Zpracovatel / Sprostredkovateľ : osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce
  (v případě cloudové služby Microsoft ve smluvním vztahu se zákazníkem)

- Subjekt osobních údajů / Dotknutá osoba : fyzická osoba, která je identifikovaná , resp. identifikovatelná s použitím osobních údajů *(fyzický zákazník, zaměstnanec, občan)*

- GDPR pro Microsoft mimo Cloud – poskytuje technologie, ale nemá roli Zpracovatele
- Role zpracovatele vůči správci musí být smluvně podložená (viz dále)

Sdílená odpovědnost Správce - Zpracovatel

Řízení rizik na straně Správce

Kategorizace údajů a stanovení politik ochrany

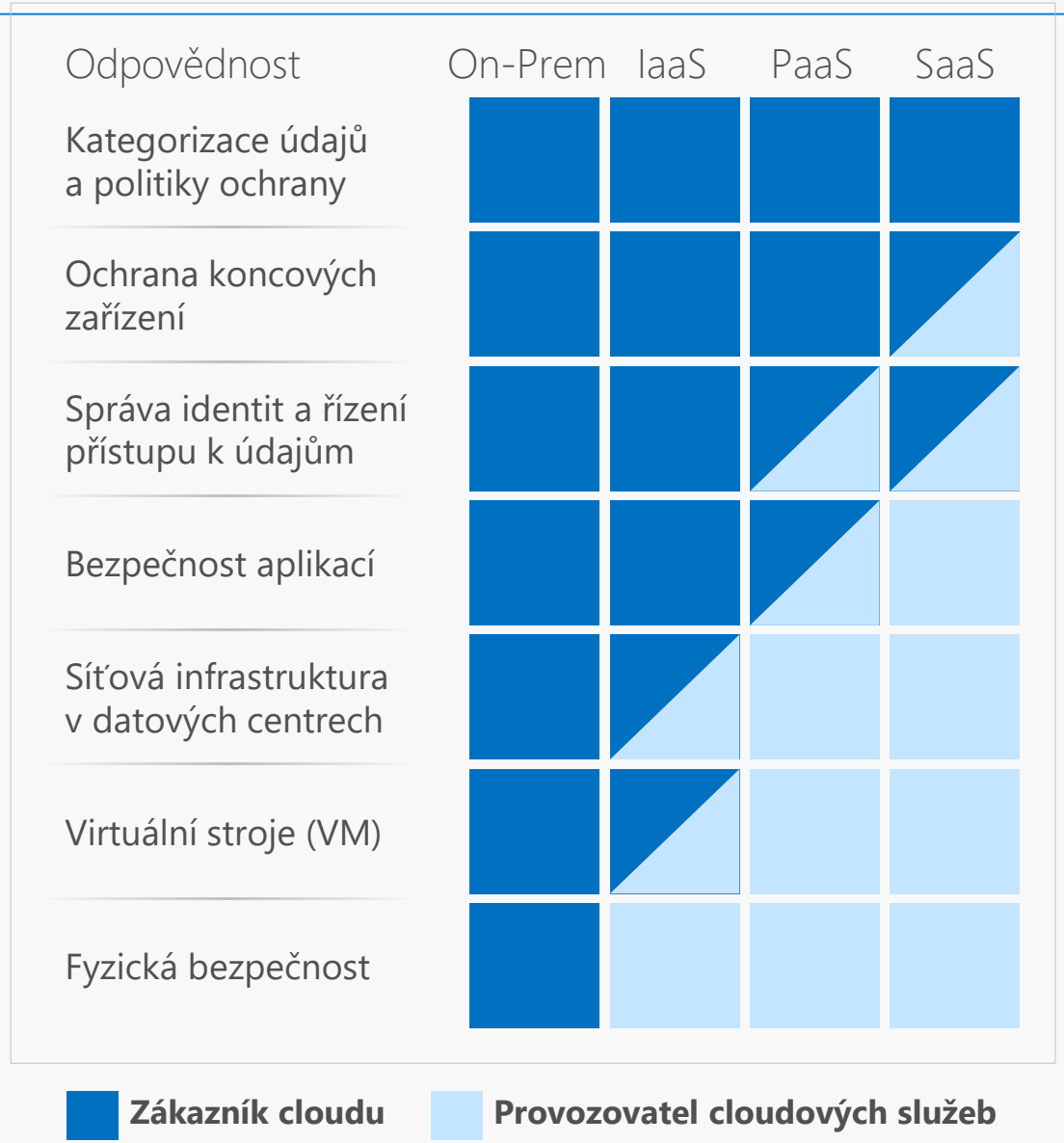
Sdílené řízení rizik

Správa identit a řízení přístupu k údajům

Řízení rizik na straně Zpracovatele

Fyzická bezpečnost a infrastruktura datových center

[Shared responsibility](#) – Microsoft whitepaper



Smluvní záruky Microsoft = zpracovatel

Požadavek	Řešení
Smluvní podmínky dle čl. 28	**OST - „Podmínky pro služby online“** od září 2017 má standardně přílohu č. 4 – řeší explicitně soulad s články 28, 32 a 33 GDPR. Obsahuje „Podmínky ochrany osobních údajů a zabezpečení“ (str. 8 a dále)
Zabezpečení zpracování – čl. 32	OST kap. „Zabezpečení“ str. 13 a dále - bezp. opatření, certifikace a auditní zprávy Dále Příloha 4 GDPR Odkazy na Trust Center www.microsoft.com/trust Celé auditní zprávy a dokumenty jsou na Service Trust Platform (www.aka.ms/STP)
Místo uložení dat	OST – odst. „Umístění pro uchování neaktivních zákaznických dat“
Místo zpracování dat	Může nastat v jistých případech i mimo EU. Řešení – GDPR čl. 46 Standardní smluvní doložky o ochraně údajů přijaté EC (viz potvrzení EC a vyjádření ÚOOÚ). Zahrnuty jako příloha č. 3 OST. Podrobnosti viz www.microsoft.com/trust, oblast Privacy, „Where your data is located“, „Who can access your data“
Použití a zpřístupnění zákaznických dat	OST – Příloha 4 GDPR, OST – str. 7, Použití zákaznických dat, Zveřejnění (zpřístupnění) zákaznických dat

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

Přehled řešení Microsoft pro zabezpečení infrastruktury a aplikací

Vlastimil Tesař

GDPR + Cloud

Maximální využití technického, bezpečnostního i organizačního zajištění všech cloudových služeb

- Ověření uživatelů i správců- Multifaktorová **autentizace**
- **Ochrana** před kybernetickými útoky
- **Šifrování** dat
- **Organizační opatření** v cloudových službách pro přístup k systémům i datům
- Přístup **řízený zákazníkem –** Customer Lock Box
- Zajištěné **logování a audity –** viz dále

Snížení nákladů na zavedení souladu s GDPR

- Na **zmapování stávajícího stavu** (rozdílové analýzy, DPIA)
- Na **technická i organizační opatření** pro zajištění provozu a zabezpečení osobních informací a systémů
- **Na vlastní výkon práv subjektů**
- Na případnou **finanční sankci** v případě úniku dat
- Na **ztrátu zákazníků** spojenou se ztrátou důvěry a reputace
- Maximální využití primárních vlastností Office 365 pro produktivitu uživatelů a nejen kvůli zabezpečení a GDPR

Bezpečnost pro každého nejen kvůli GDPR

1. Zašifrujte si svůj notebook pomocí BitLockeru

- Pokud je nepravděpodobné riziko zneužití, nemusíte informovat regulátora, ani subjekty údajů.

2. Nastavte si šifrování a PIN pro mobilní telefon

- Pokud je nepravděpodobné riziko zneužití, nemusíte informovat regulátora, ani subjekty údajů.

3. Přesuňte svůj e-mail do Office 365

- Ochrana proti spamu a malwaru , vyhledávání osobních informace napříč Office 365 díky eDiscovery. Smluvní závazky Office 365 pro GDPR.

4. Ukládejte dokumenty na OneDrive for Business v Office 365

- Bezpečné sdílení dokumentů uvnitř i mimo firmu, automatické ukládání z aplikací Office, omezení kopií dokumentů v přílohách a hlavně automatická záloha. Smluvní závazky Office 365 pro GDPR.

5. Chraňte citlivé dokumenty pomocí Information protection

- Dokumenty jsou šifrované, otevřou je pouze ověření uživatelé, dokument je možné zneplatnit v případě neaktuálnosti osobních informací a eliminovat riziko úniku informací.

6. Udržujte své zařízení aktualizované

- Pouze aktualizované systémy mohou být bezpečné a Microsoft pravidelně vydává bezpečnostní aktualizace, které zamezují napadnutí počítače s Win10 novými typy útoků. Vždy n nainstalované nejnovější vlastnosti aplikací Office.

Microsoft Azure

Infrastruktura & Aplikace

Využití pro stávající aplikace

- Aplikace využívající **nedostatečně** technicky a organizačně **zajištěnou infrastrukturu**
- Přenesení části požadavků k naplnění **zavedení vhodných technických a organizačních opatření** na zajištění ochrany práv subjektu údajů na zpracovatele

Využití pro nové a redesignované aplikace

- **Minimalizace vstupních investic** do HW vybavení pro vývoj a provoz nových aplikací, splňujících požadavky GDPR
- **Okamžitá dostupnost** prostředků a prostředí pro vývoj nových aplikací, splňujících požadavky GDPR
- **Bezpečné prostředí provozu** aplikací, splňujících požadavky GDPR

Agendy GDPR

- **Vývoj a provoz aplikací** spojených se zajištěním **výkonu práv subjektů**
- Platforma pro **procesy zpracování –** Dynamics 365, Office 365…

Microsoft Azure

Správa a zabezpečení

Předcházení bezpečnostním incidentům
Azure Security Center

- 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

Detekce a zvládání incidentů – Security as a Service

- 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 události, incidentu, spojených s konktrétním uživatelem, procesem atp v daném čase

Integrace s EMS, Office 365, Azure

Zabezpečení stanic
Windows 10

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*
- **Zabezpečená identita oprávněného uživatele** Vestavěná podpora vícefaktorového ověření uživatele Windows Hello for Business.

Zabezpečené informací při odcizení nebo ztrátě

- **Firemní a informace osobní data** na zařízeních a uložištích 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**

Zabezpečení EMS

Enterprise Mobility & Security

Zajištění zařízení, které 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 potecionálních rizik spojených s cloudovými službami

Bezpečnostní a provozní monitoring

Ondřej Výšek

Microsoft Operations Management Suite

Ondrej Vysek
Chief Sales Officer, Microsoft
MVP
KPCS CZ

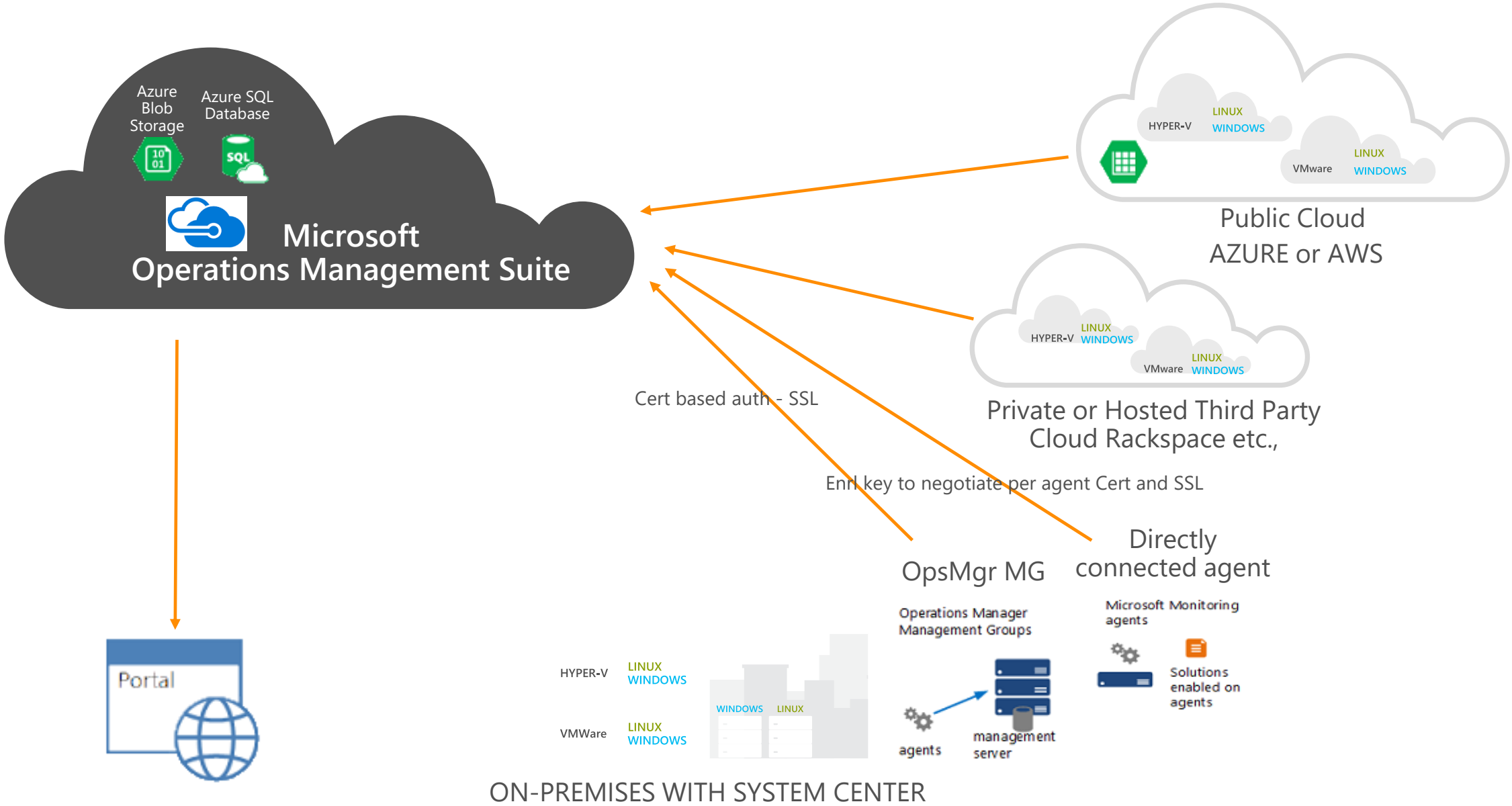
Where to start?

Gain full visibility to react quickly and proactively prevent issues

- Transform machine data
- Gain immediate insight
- Resolve incident faster

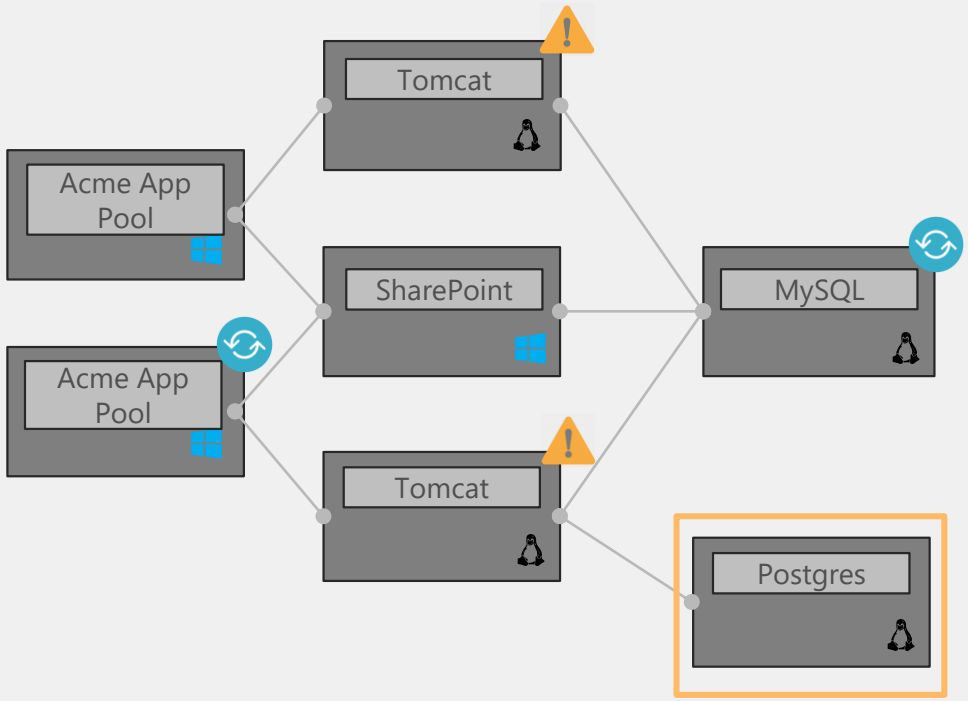
Operations Management Suite | Insight & Analytics

Operations Management Suite Environment



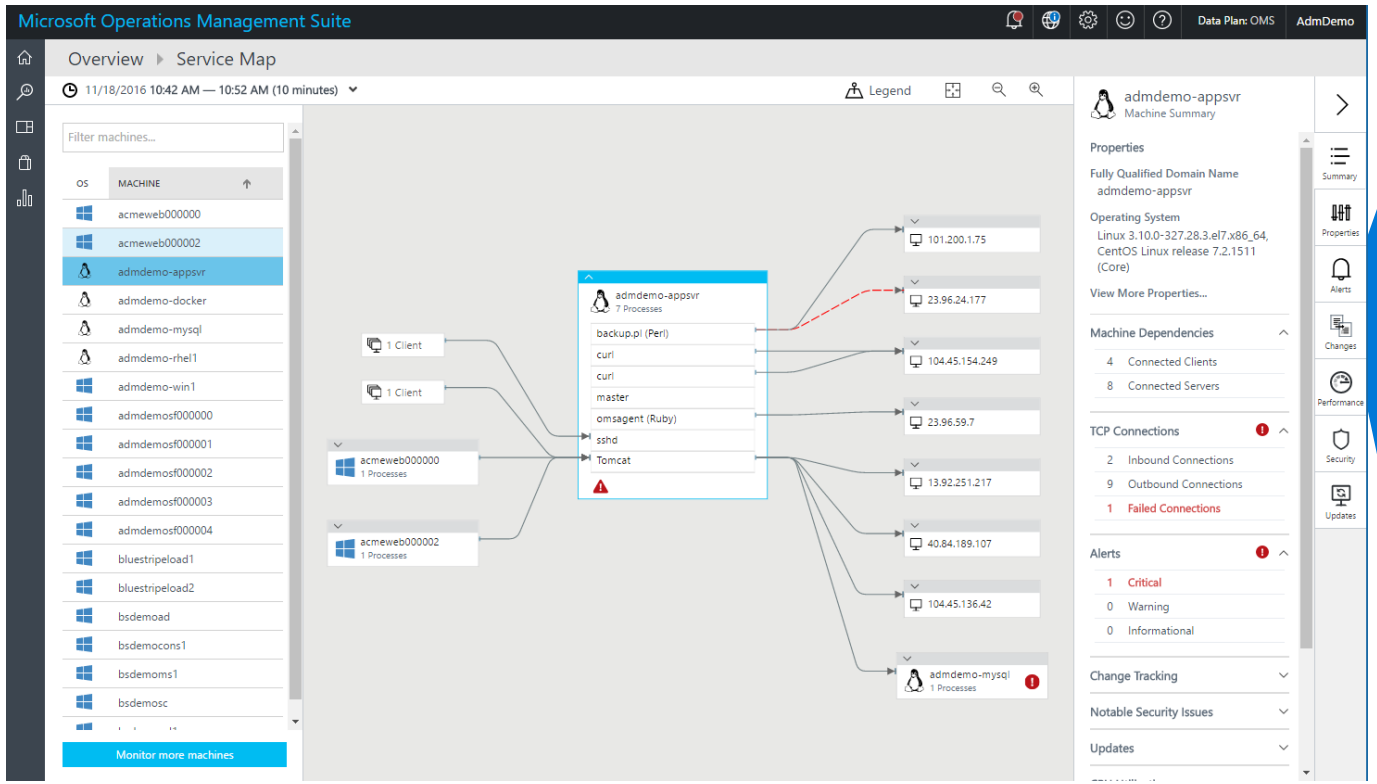
Gain full insights into applications and their dependencies

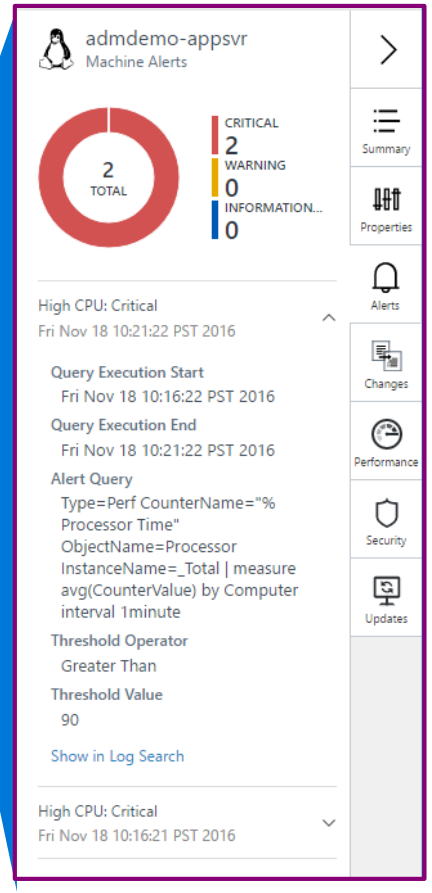
- Real-time performance visibility
- Dynamic application dependency mapping
- Faster fault analysis



Operations Management Suite | Application Management

Accelerated troubleshooting and root-cause analysis





- You have been notified with an Alert for a specific server
- You can identify all dependent services for this specific server

Linux management

Key benefits

- Integrates with existing open source management tools (Nagios, Zabbix)
- Use open source collector (Fluentd)
- Centralized view of syslog, perf metrics and alert data
- Supports Docker containers
- Backup and restore of Linux server
- Unified configuration and update management

OS	Red Hat	Ubuntu	Oracle	CentOS	SUSE	Amazon Linux
Collector	Fluentd (Open Source)					
Data Sources	Syslog	Perf	Nagios	Zabbix	Containers	Custom Logs

Increase control with automation and configuration management

- Enable responsive IT operations
- Use across on-premises and the cloud
- Maintain compliant IT resources

Operations Management Suite | Automation & Control

OMS automation and control

Continuous IT services

Enable responsive IT services and deliver continuous application availability. Increase velocity with improved SLAs to support IT lifecycle activities.

Consistent enterprise control

Maintain compliant IT resources and manage rapid change with ease. Mitigate risks and keep systems updated with patching on your terms.

Hybrid IT automation

Deliver efficient IT operations with a flexible platform across heterogeneous IT environments. Leverage your existing investments in Microsoft System Center and improve efficiency.

Key capabilities

- Manage all automation and configuration assets from a centralized repository with granular access
- Retain control of when and how to patch, without unplanned downtime and with application owner's approval
- Apply and monitor configurations using a highly available pull service, choose to fix configuration drift without manual intervention
- Resolve alerts and orchestrate backup and disaster recovery with automated remediation scripts and recovery plans.
- Get the flexibility to run automated processes from Azure or locally from an on-premises datacenter with hybrid runbook workers

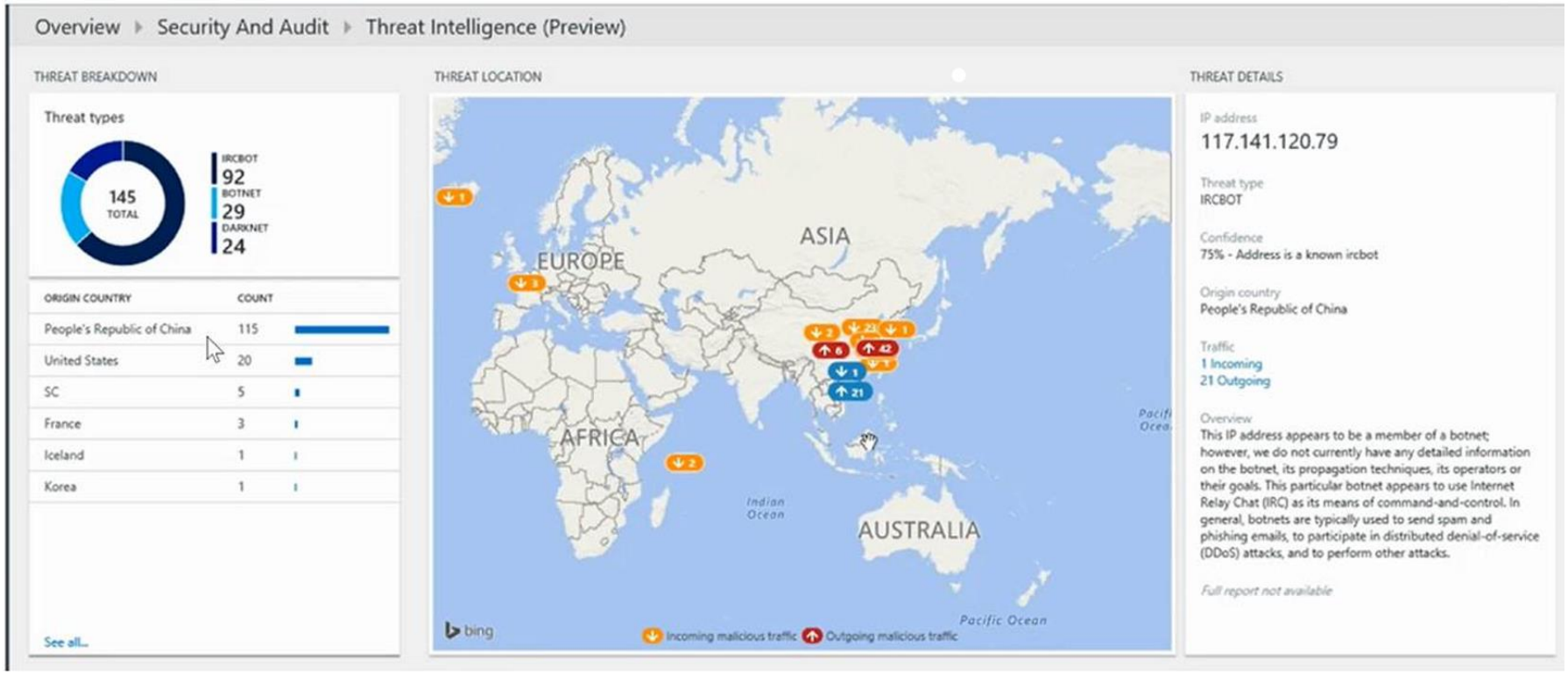
Threat detection and prevention through advanced cloud security

- Analyze and investigate security incidents
- Detect threats before they happen
- Streamline security audits

Operations Management Suite | Security & Compliance

Security and Audit Dashboard – Threat Intelligence

- Integrates with Microsoft Advanced Threat Analytics (ATA)
  - Install Microsoft Monitoring Agent on ATA Center Machines
- Why are my servers sending data to China?



Ensure data protection with cloud backup and disaster recovery

- Protect your critical assets wherever they are
- Simplify disaster recovery across your entire environment
- Free up resources on-premises with cloud backup

Operations Management Suite | Protection & Recovery

Azure Backup

Protection everywhere

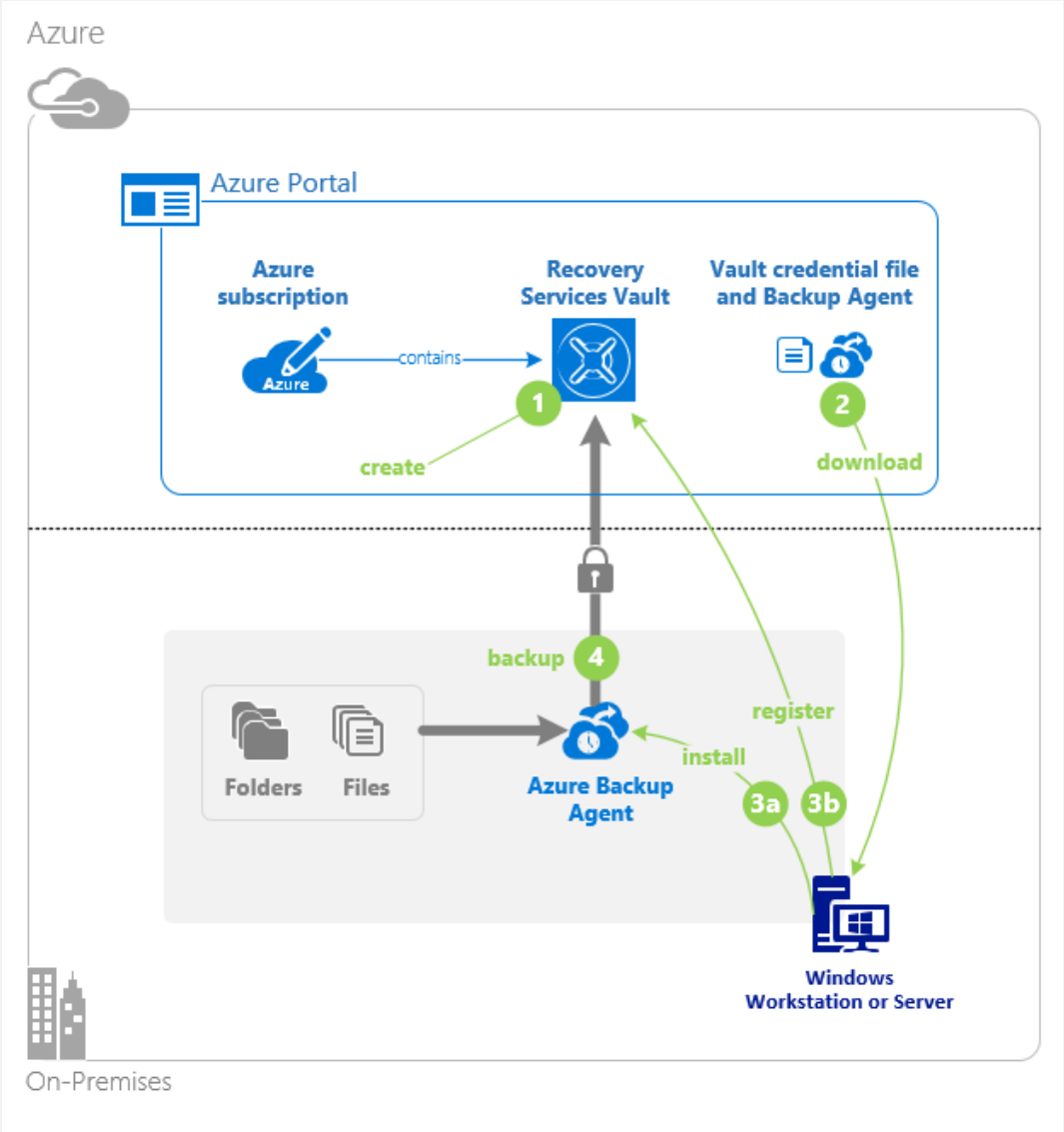
Your data and applications are everywhere—on servers, on clients, and in the cloud. Azure Backup can protect your critical applications including SharePoint, Exchange, SQL, files and folders, Windows Servers, Windows Clients, and Azure IaaS virtual machines.

Alternative to tapes

Traditionally, tape has been used for long-term retention. Azure Backup provides a compelling alternative to tape with increased reliability and agility, significant cost savings, shorter recovery times, and up to 99 years of retention.

Simple and consistent management

Azure Backup aims to provide a simple, consistent management experience delivered directly from the cloud. As an example, you can enable protection in three simple steps: choose the scenario, choose the retention period, and enable backup.



Azure Site Recovery

Disaster recovery

Tested and proven disaster recovery solution for a wide range of workloads, including Microsoft workloads such as Exchange, SharePoint, and SQL Server.

Migration

Seamlessly move individual applications or entire heterogeneous environments to Azure with minimal cutover times or business impact.

Dev / Test

Test new versions of applications by quickly spinning up copies of production workloads in Azure, with no impact to production users.

The Site Recovery service ensures your servers, virtual machines, and apps are resilient by replicating them so that when disasters and outages occur you can easily fail over to your replicated environment and continue working.

When services are resumed, you simply failback to your primary location with uninterrupted access. Site Recovery helps protect a wide range of Microsoft and third-party workloads.

Zabezpečení cloudových služeb a a uživatelských přístupů

Tomáš Králik

Modern Workplace

Enterprise Mobility & Security

Tomas Kralik, SSP

Agenda

Zabezpečenie cloudových služieb

Zabezpečenie koncových zariadení

Ochrana zneužitia identít

EU General Data Protection Regulation

- Zabezpečiť ochranu údajov on-prem a v cloude
- Povoliť a obmedziť prístup k údajom
- Získať viditeľnosť a kontrolu údajov v cloude
- Chrániť dáta v mobilných zariadeniach
- Detekcia úniku údajov, skôr ako spôsobia ujmu

How to gain visibility and control of data in cloud apps

Supporting your GDPR compliance journey with Microsoft Cloud App Security

Cloud Discovery

Discover 14K+ cloud apps in your environment, gain visibility into shadow IT and assess risk

Information Protection

Shape your cloud environment with granular controls and use out-of-the-box or custom policies for data sharing, and data loss prevention

Threat Protection

Identify high-risk usage and cloud security issues, detect abnormal user behavior, and prevent threats

Discovery

Risk Assessment

Ongoing analytics

Collect logs from firewalls and proxies - no agents required on user devices

Use log anonymization to protect employee privacy while uncovering Shadow IT

Policy Setting

DLP & Data Sharing

Policy Enforcement

Policies

- Activity
- Anomaly Detection
- App Discovery
- Discovery Anomaly
- File

Policy Enforcement

Protect file

Quarantine

Make private

Behavioral Analytics

Identify anomalies in your cloud environment that may be indicative of a breach

Enhanced by Microsoft Intelligent Security Graph

Leverage Microsoft's threat intelligence to detect anomalies, prevent threats, and stop risky behavior right away.

Integrated with Azure Information Protection

Create policies for files classified by Azure Information Protection and govern sensitive data in the cloud

Investigate and gather unique insights

Gain a deeper understanding of what's happening in your cloud environment by pivoting on users, files, accounts, apps and activities.

Microsoft Cloud App Security

Learn more at www.cloudappsecurity.com

How to protect data on mobile devices and apps

Supporting your GDPR compliance journey with Microsoft Intune

Mobile Device Management (MDM)

Protect data at the device level and ensure that enrolled devices are up to date and compliant

Mobile Application Management (MAM)

Manage apps on enrolled devices and keep data secure at the app level on enrolled and unenrolled devices

PC Management

Keep PC endpoints secure from threats and ensure that data stays protected by enforcing firewall and malware policies

Manage access and control what happens to data after it's been accessed

End-user transparency

Provide end-users with terms and conditions and privacy statements, helps make sure they are aware of what data is collected and visible to IT on devices

Remotely wipe all data on lost or stolen devices

Remotely enable passcode reset, device lock, or data encryption

Deploy certificates, Wi-Fi, VPN, and email profiles

App encryption at rest

Save as/copy/paste restrictions

App access control-PIN or credentials

App SDK and App Wrapping Tool

Incorporate Intune MAM capabilities in your mobile and line-of-business apps using the Intune App SDK and App Wrapping Tool

Enforce Windows Defender, Windows Information Protection, and overall device compliance to protect user and company data

Multi-identity support

App-level selective wipe

Not compliant

Guide to compliance

Company data

Compliant

CONDITIONAL ACCESS

- Enrollment
- Encryption
- Pin
- OS Requirements
- Location
- Apps
- Risk
- Device

How to detect threats before they cause damage

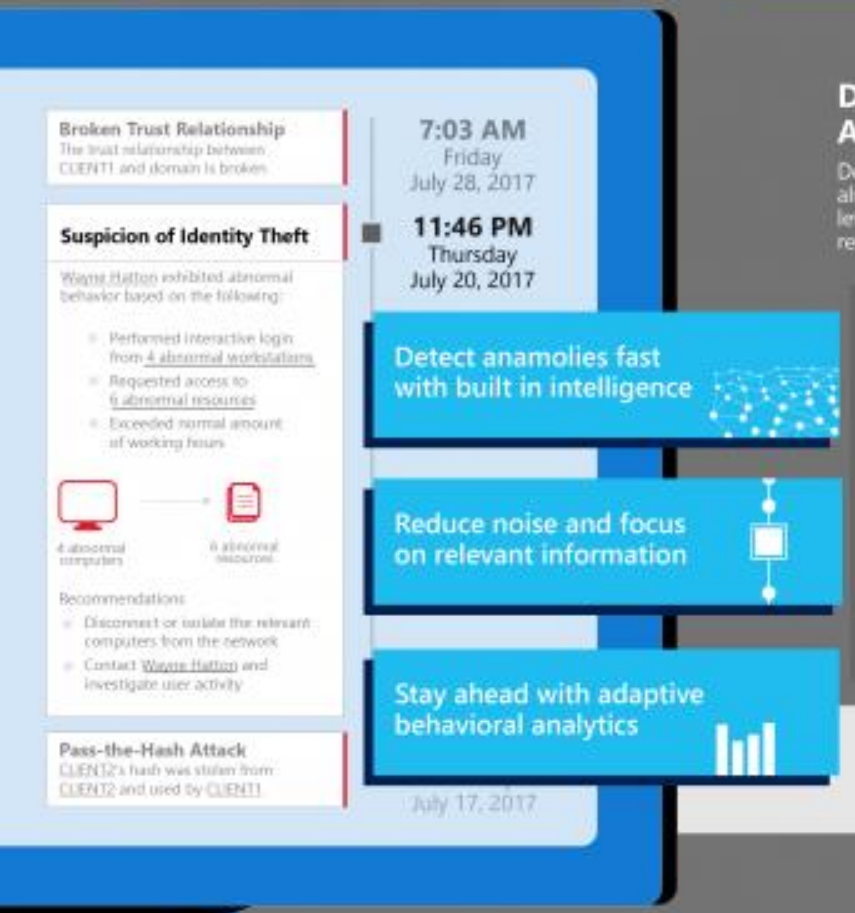
Supporting your GDPR compliance journey with Microsoft Advanced Threat Analytics

Analyze
Monitors network traffic and events on the domain controller with non-intrusive port mirroring while remaining invisible to attackers

Learn
Automatically starts learning and profiling normal behavior for entities (users, devices, and resources)

Detect
Looks for abnormal behavior and suspicious activities. Leverages security research to detect risks and malicious attacks

Alert
Reports suspicious activities on a simple and actionable attack timeline, provides recommendations and remediation, integrates with SIEM



Detect Malicious Attacks

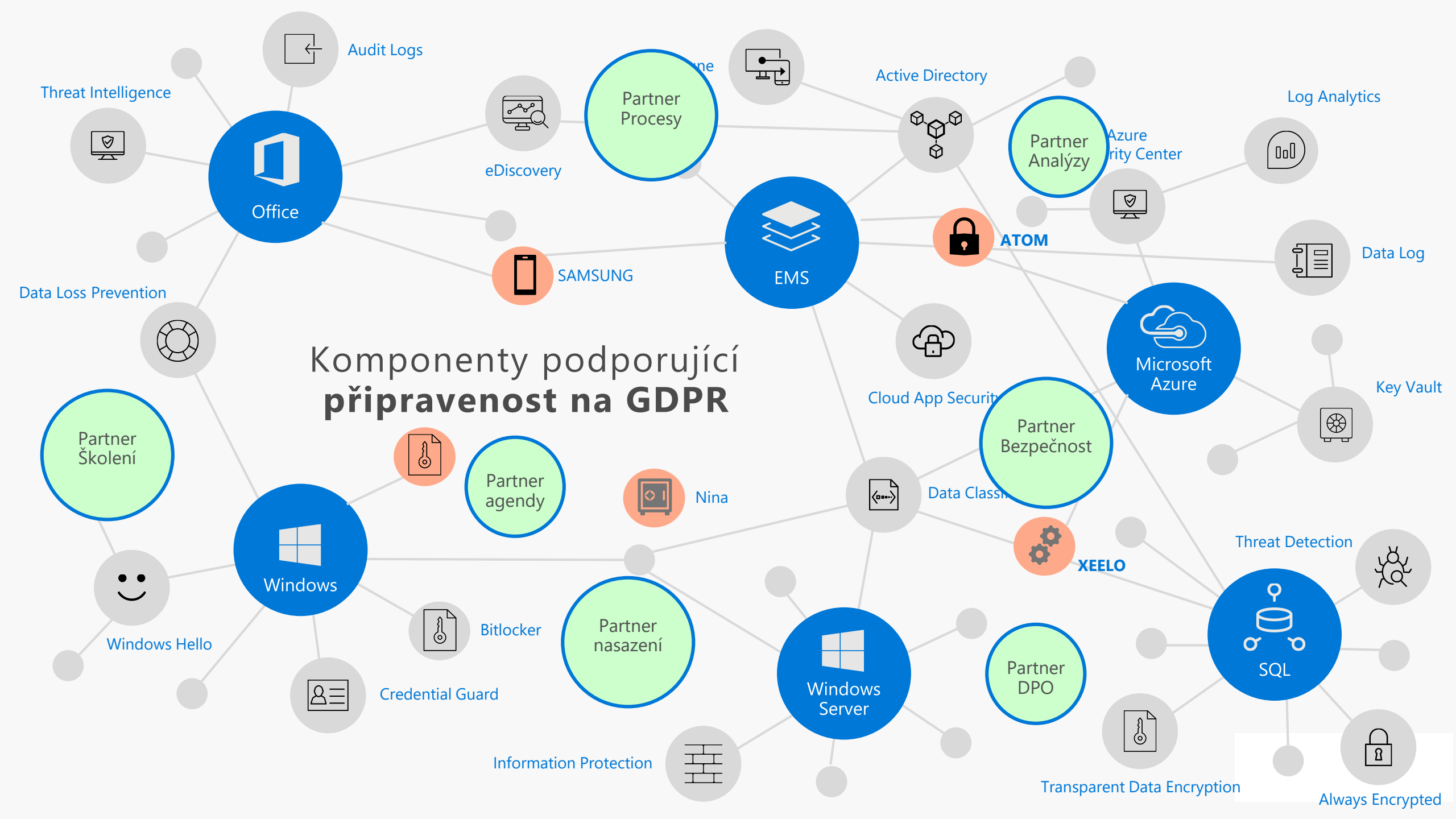
Detect known malicious attacks almost as instantly as they occur, leveraging world-class security research

Monitor Security Vulnerabilities

Identify known security vulnerabilities in your system and mitigate risk (i.e. broken trust, weak protocol, cleat text passwords)

Detect Suspicious Activities

Leverage Machine Learning to uncover questionable activities and abnormal behavior (i.e. anomalous logins, password sharing, lateral movement, privilege escalation)


Audit Logs
Threat Intelligence
Office
eDiscovery
Partner Procesy
Active Directory
Log Analytics
Partner Analýzy
Azure
rity Center
Data Log
ATOM
SAMSUNG
EMS
Data Loss Prevention
Cloud App Securit
Microsoft Azure
Key Vault
Komponenty podporující
připravenost na GDPR
Partner Školení
Partner agendy
Nina
Partner Bezpečnost
Data Classi
XEELO
Threat Detection
Windows
Windows Hello
Bitlocker
Credential Guard
Partner nasazení
Windows Server
Partner DPO
SQL
Information Protection
Transparent Data Encryption
Always Encrypted

Partnerská řešení pro GDPR

KPCS
Safetica
Xeelo GDPR

KPCS

ATOM

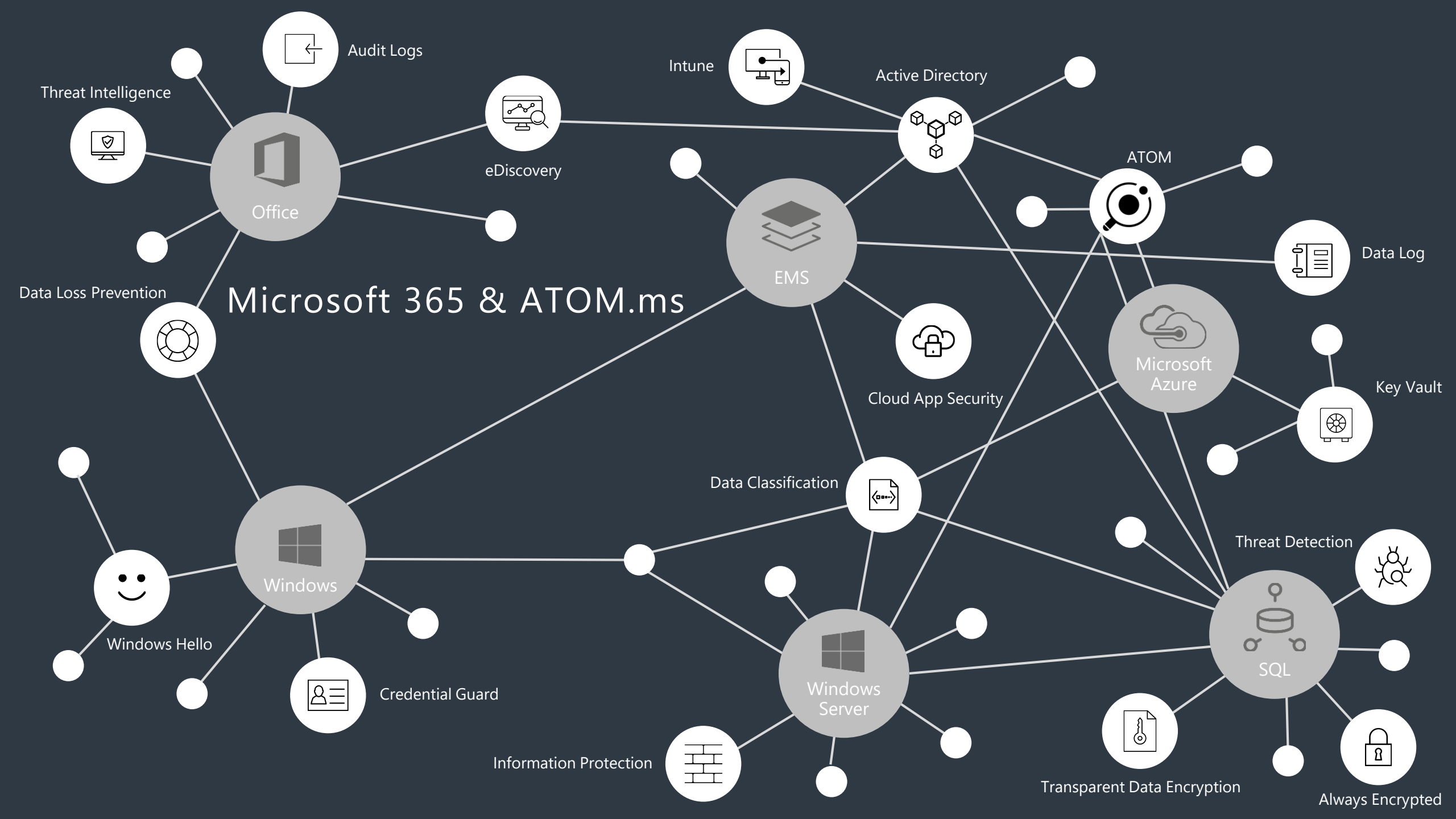
Advanced Threat & Organization Monitoring

Ondrej Vysek | Chief Sales Officer | Microsoft MVP | www.atom.ms

World has changed, already

§

ATOM


Audit Logs
Threat Intelligence
Office
eDiscovery
Intune
Active Directory
ATOM
Data Log
Data Loss Prevention
Microsoft 365 & ATOM.ms
EMS
Cloud App Security
Microsoft Azure
Key Vault
Data Classification
Windows
Windows Hello
Credential Guard
Threat Detection
SQL
Windows Server
Information Protection
Transparent Data Encryption
Always Encrypted

Security is a challenge

- Lack of resources – human / technical
- Too much (or no) tools for monitoring
- Needs to be GDPR compliant in 2018

ATOM: collect and analyzes data to detect potential breaches

System mgmt. too complex

- Hard to understand to the diagnostical data from different tools
- Or simply too much information
- Hybrid multi OS environment

ATOM: reports contain knowledge „how to“ with important issues – security & operations

Don’t want to invest

- Model Pay-as-you go.
- No implementation needed, no investments
- Can connect existing systems
- Continuous development

ATOM: ready in 5 minutes, report after first week. Can connect SCOM, Zabbix and more

GDPR
Article 32 section 1 lit b. defines

Integrity	Availability	Resilience	Confidentiality
• Service state change • Server availability • Network traffic • End point login / access	• Network monitoring • Performance monitoring • Event management • Health check lite	• Baseline comparison • Best practice evaluation • Service Map, relationship between services, processes and systems	• AD group check • Local group check • ATA and SIEM integration • E.g. DNS access / changes • File system access / attemp

No time for analysis

Lack of knowledge

Environment too complex

ATOM report

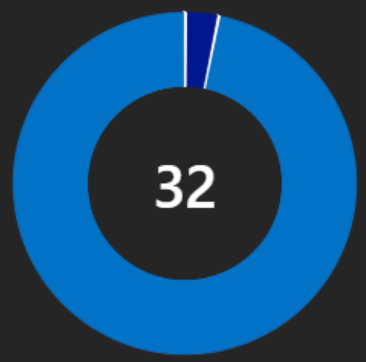
- Contain C-level overview incl. remediation
- Focus on top issues in the environment
- Track changes, have environment documented
- Don’t need to be an expert to keep IT up and running
- Optionally – we can help with remediation, SLA guaranteed (in EU) for critical and security incidents

Do correct decisions in the right time

ATOM Dashboard

Exit fullscreen

Analytics
DEFENSE-OPS-OMS-KQL



192.168.88.8
31.0

80.82.78.35
1.0

Logon to Remote Desktop Service

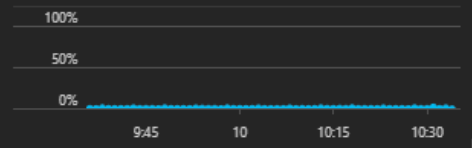
321
Failed Logon

4
Success Logon

AZVM1

Running

Percentage CPU for the past hour
AZVM1

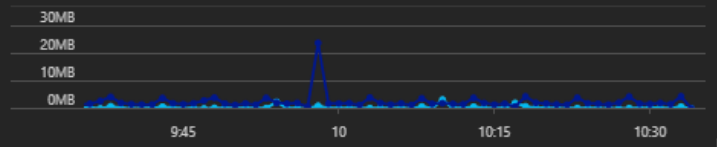


Best Practice Analyzer

Configuration
860
Operation
7
Prerequisite
5

Change in privileged groups

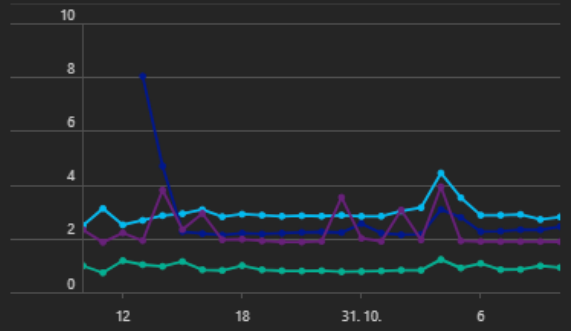
Disk Read Bytes and Disk Write Bytes for the past hour
AZVM1



Advanced Threat Analytics

Warning
1

Analytics
DEFENSE-OPS-OMS-KQL

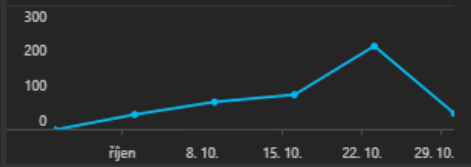


DC2.DEFENSE...
SCCM01.DEFE...
WEB1.DEFENS...
HYPERV

Analytics
DEFENSE-OPS-OMS-KQL

BOX1
BOX2

Enterprise applications
USERS SIGN-INS



Overview

Logon to Remote Desktop Service

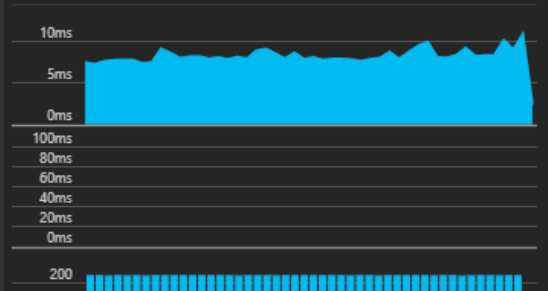
321
Failed Logon

4
Success Logon

Total of Server Requests by Request Performance
EXCHAPPINSIGHT

REQUEST PE...	TOTAL	% TOTAL
<250ms	11,83 K	100,0 %
250ms-50...	2	0,0 %

Overview timeline
EXCHAPPINSIGHT

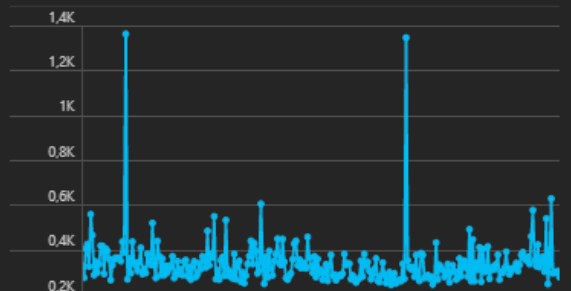


SERVER RESPONSE TI...
8,28 ms

PAGE VIEW LOAD TIME
--

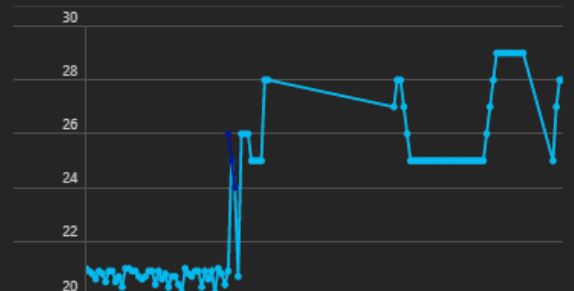
SERVER REQUESTS

Analytics
DEFENSE-OPS-OMS-KQL



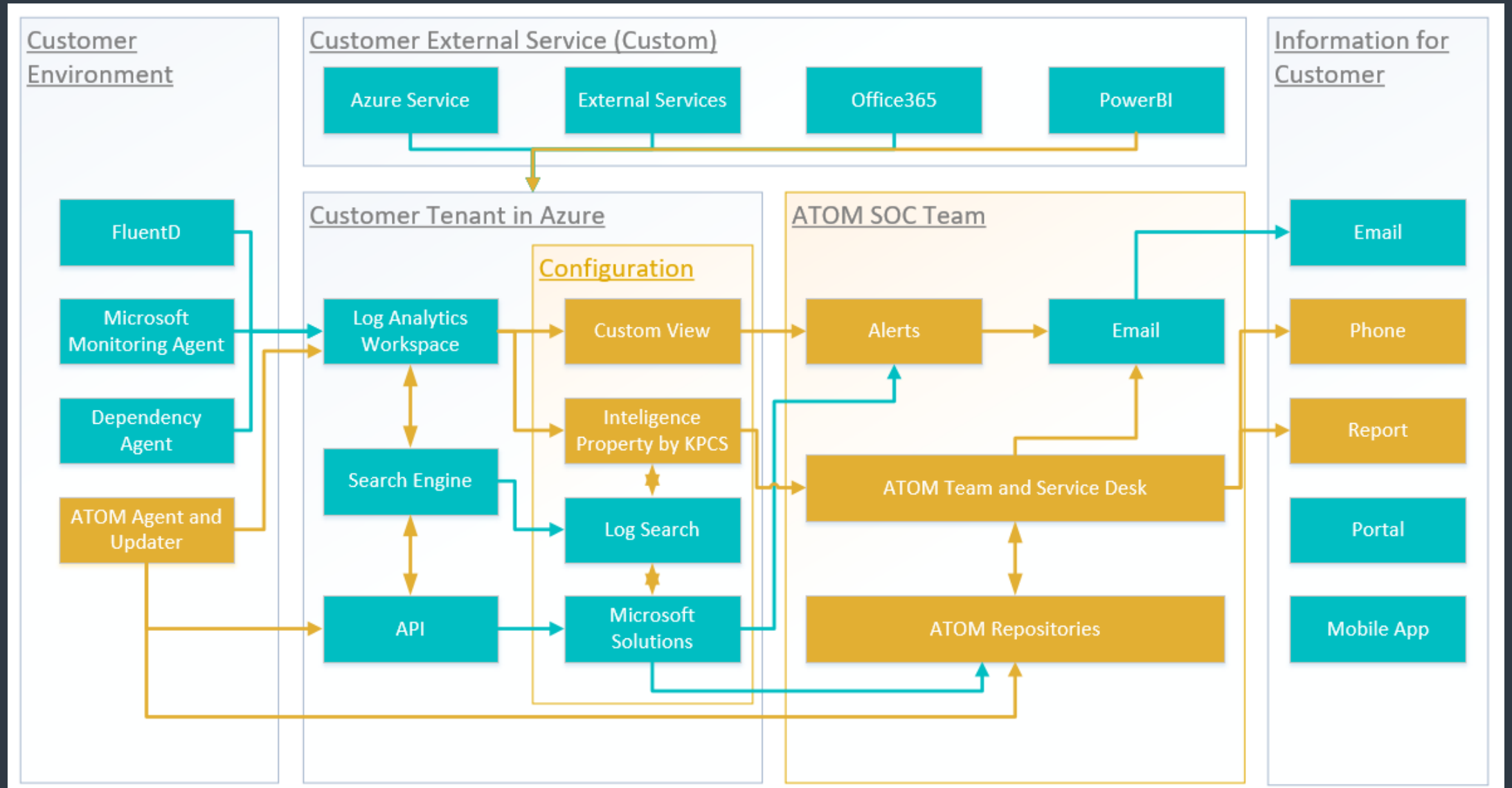
WWW.DEFEN...

Analytics
DEFENSE-OPS-OMS-KQL



BOX1
["BOX1", "BO...

ATOM Architecture



Active Directory Health Check

No data found

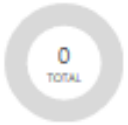
Click here to troubleshoot.

AD Replication Status

No data found

Click here to troubleshoot.

Advanced Threat Analytics



Agent Health

4
Total count of agents

0
Count of unresponsive agents in the last 24 hours

Alert Management

Welcome!

With the Alert Management Intelligence Pack, you can now view all alerts from System Center Operations Manager. Within an hour after any alert is raised or changed in your environment, the alert data shows up in the portal.

Antimalware Assessment

Active Threats
0
Remediated Threats
0
Insufficient Protection
1

ATOM Agent Status

5
Servers health

Azure Activity Logs

Performing Assessment

To use this solution, please connect an Azure Subscription for collecting activity logs. A subscription can be connected using the activity logs blade of a workspace in the Azure portal.

Azure Automation

Enabled. Allows creation of Hybrid Runbook Workers for your Automation accounts.

Azure Network Security Group Analytics

Performing Assessment

Learn how to configure solution:
http://go.microsoft.com/fwlink/?linkid=839623

Best Practices Analyzer

Configuration
454
Prerequisite
9
Performance
2

Bitlocker Status

#Computer data decrypted
0
#Computer data encrypted
0
Computer not scanned
4

Capacity and Performance (Preview)

0
Hosts

0
Virtual Machines

DNS Analytics (Preview)

0
Malicious Activity
(Last 24 hours)

0
DNS Servers

Free Tier Data Consumption Tracker

WireData2
20.6
LogManagement
13.6
Security
4.5

ChangeTracking

IIS Status

:-(oops... looks like we couldn't get the data

IT Service Management Connector(Preview)

Solution requires additional configuration

Logon Activity Web Service

0
Types of data

Logon to Remote Desktop Service

0
Failed Logon

0
Success Logon

Network Performance Monitor

Data aggregation in progress

Network Performance Monitor is collecting data from your environment.
Note: Network Performance Monitor MUST be enabled on at least two machines for this process to succeed.
In some cases, first time data collection can take several hours to complete.

Office 365

Performing Assessment

We're still getting things ready. At most it should take 24 hours to start getting data into the system.

SCOMEffectiveConfiguration

Performing Assessment

Please use PowerShell Module 'SendEffectiveConfiguration' to populate the view. Module is available on PowerShell Gallery.

Security and Audit

4
Active Computers

5 ↘ 6
Active Accounts

Server Performance

0
Servers currently reporting to OMS

4
Servers not currently reporting to OMS

Service Map

4
Machines reporting
(Last 30 min)

4
All-time machines reporting

4 0

SQL Health Check

No data found

Click here to troubleshoot.

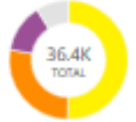
System Center Operations Manager Health Check (Preview)

Solution requires additional configuration

System Update Assessment

Need Critical Updates
2
Need Security Updates
0
Need Other Updates
1
Up To Date
1

Task Scheduler Status



w10cl1.defense-ops.local
18.3K
adfs1.defense-ops.local
10K
swp.defense-ops.local
4.8K

Update Compliance

1
Total devices

0
Devices need attention

Last updated on 02/06/2018 at 07:00 PM

Upgrade Readiness

User related security events

VMware Monitoring

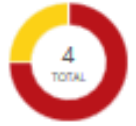
:-(oops... looks like we couldn't get the data

WannaCry MS17-010

0
Vulnerable Patchs per Computer

0
Updates Replaced per Computer

WannaCrypt Update Assessment



Vulnerable to WannaCrypt
3
Not Assessed
1
Protected from WannaCrypt
0

Windows Free Storage

0
Disk volumes with less than 10% free space

0

Windows Inventory

Virtual Machine
4

Windows Update Management

Update not installed
27
Update installed
28

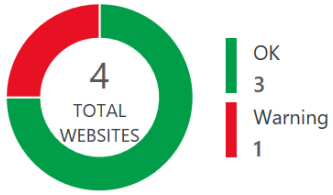
Wire Data 2.0

4
Agents in the last 24 hours

2
Local Subnets in the last 24 hours

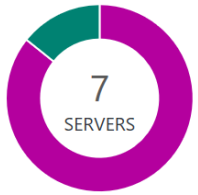
Own solutions in ATOM

Web Probe



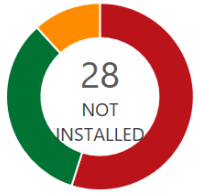
OK
3
Warning
1

Windows Hardware and Software Inventory



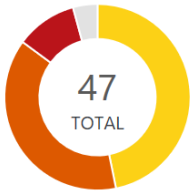
Virtual Machine
6
PowerEdge R610
1

Windows Update Management



Update not installed
28
Update installed
17
Not Installed OS Updates
6

Advanced Threat Analytics



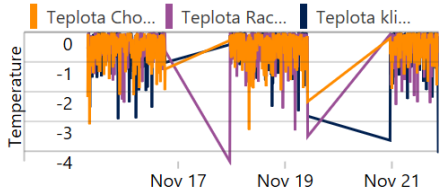
Information
22
Warning
18
Error
5

Logon Activity Web Service

8.5K
Types of data

Environment Probe - Sample Data

MAX
0.0

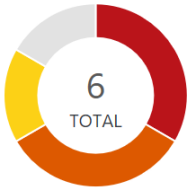


Logon to Remote Desktop Service

82.6K
Failed Logon

42
Success Logon

Change in privileged groups

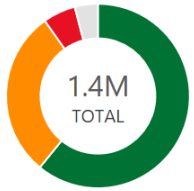


4728 - A member was added...
2
4720 - A user account was cr...
2
4729 - A member was remov...
1

Local Certificates Status

Critical
1
Warning
0
Expired
0

IIS Status

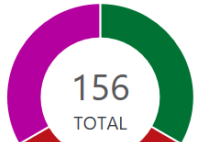


200
841.8K
401
405K
302
79.3K

Best Practice Analyzer

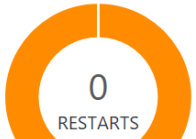
Configuration
905
Prerequisite
7
Operation
7

Monitoring Access Project Honolulu



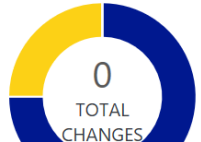
Pass logon
52
Failed logon
52

Operating system HealthCheck Lite



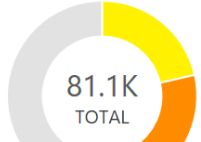
Server Down
1
Unexpected shutdown
0

Local Users and Groups Assessment



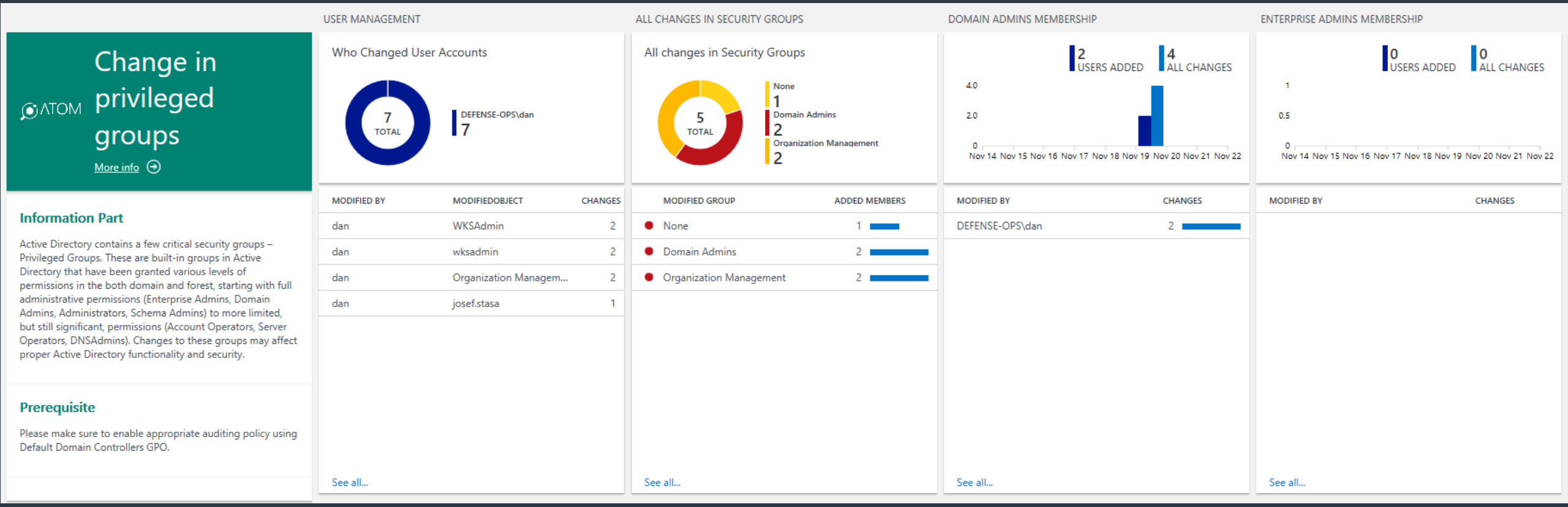
Top local admins
6
Top changes by server
2

Task Scheduler Status



ex16s2.defense-ops.local
17.4K
ex16s1.defense-ops.local
16.6K

Every solution has a detail



Or complete detail – audit trail

Data based on custom time range

1 bar = 6hrs

7:00:00 AM
Nov 19, 2017

TYPE (1)

SecurityEvent 7

LEVEL (1)

8 7

DOMAINNAME (0)

OBJECTNAME (0)

ACCOUNT (1)

DEFENSE-OPS\dan 7

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

ATOM

Complex things, easy to understand

KPCS

ATOM

IT produkt

COMPUTERWORLD 2017

www.ATOM.ms | atom@atom.ms

Ochrana dat se Safetica

safetica

Martin Imrich
Delivery & Project Leader

BMW Invelt

ochrana firemních dat před nekalým konkurenčním bojem

Řešení je Safetica DLP

- Data Loss Prevention
- Chrání zaměstnance před vlastními chybami
- A firmy před únikem dat
- Snižuje riziko ztráty reputace, konkurenčních výhod a peněz
- Udržuje vaše data v bezpečí
- Pomáhá splnit GDPR

Safetica Technologies

- česká společnost
- od roku 2008
- 65+ bezpečnostních expertů
- 120 000+ chráněných zařízení
- v 55 zemích světa

Tři jednoduché kroky

Hlavní panel
Bezpečnost dat
Souhrn
Tok dat
Správce zařízení
Bezpečnostní incidenty
Označená data
Produktivita
Využití IT zdrojů
Správa
Nastavení
Nápověda

148 (209,7 kB) >
Soubory odeslané přes e-mail a IM

0 >
Pokusy o přístup na zakázaný disk

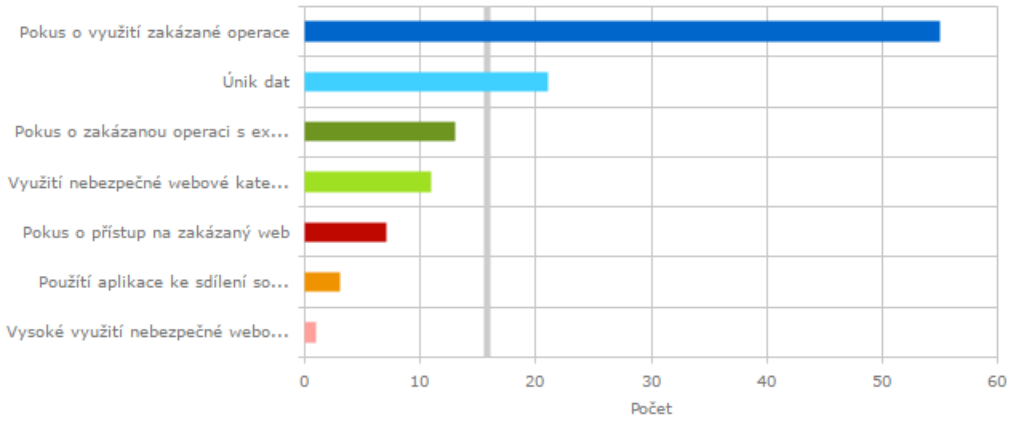
12 >
Uživatelé s bezpečnostními incidenty

624 >
Zakázané operace s označenými daty

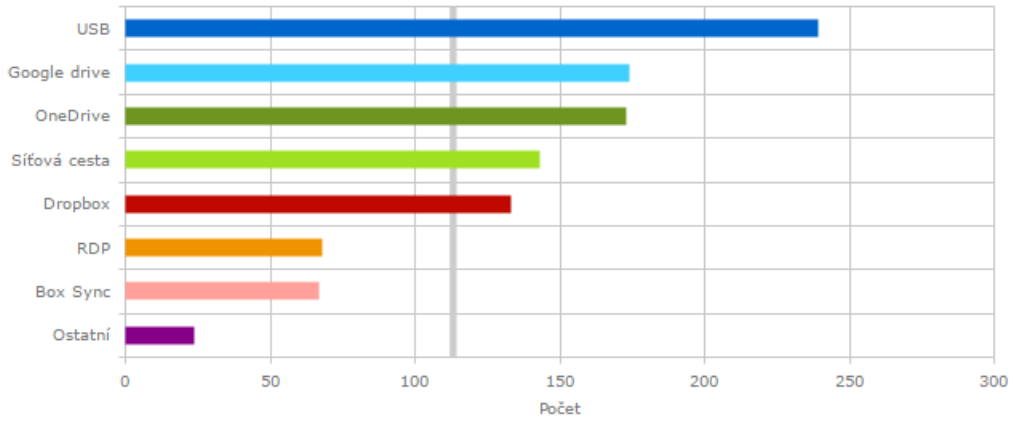
GRAFY

Export do .pdf

BEZPEČNOSTNÍ INCIDENTY >



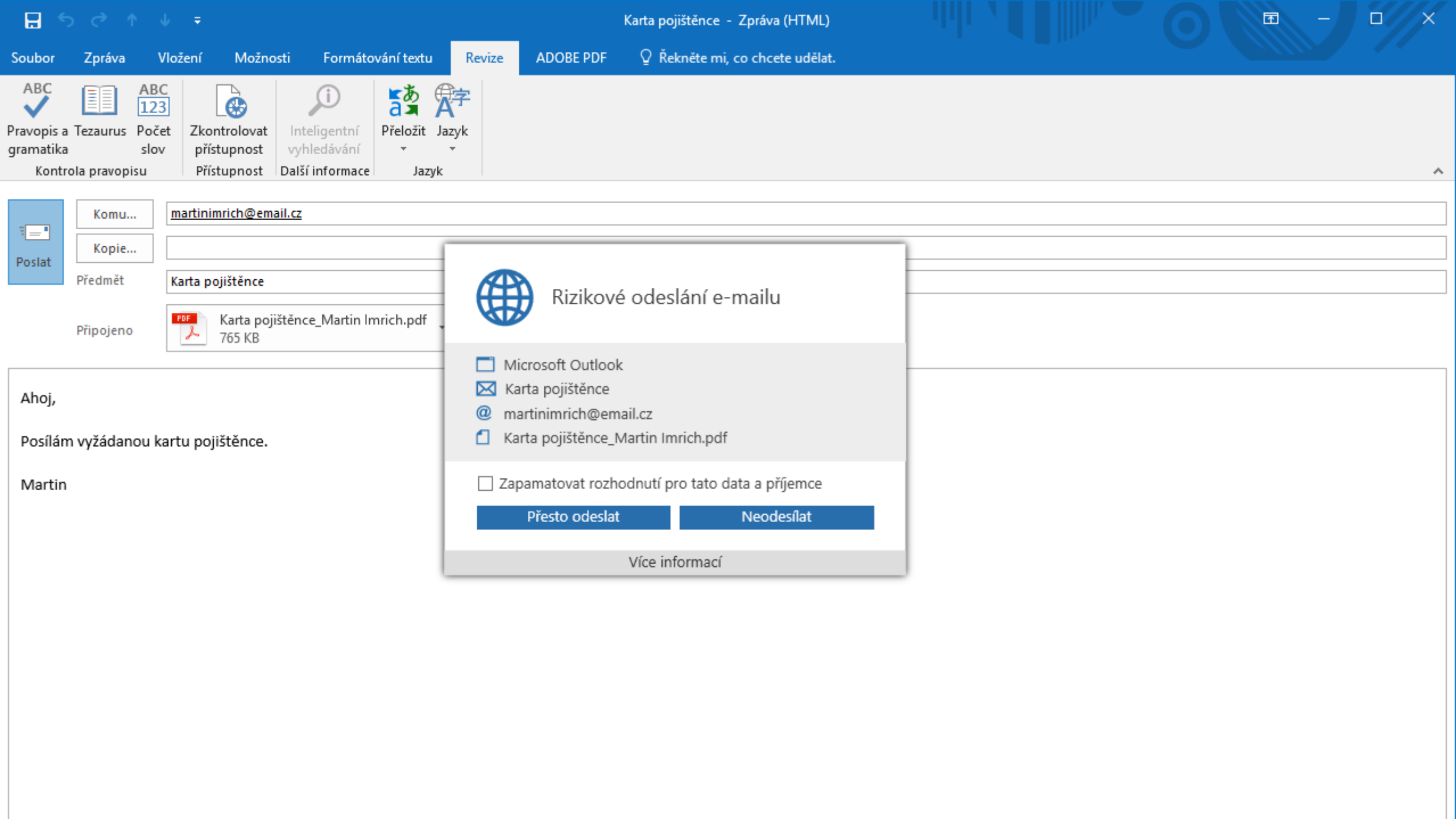
KANÁLY TOKU DAT >

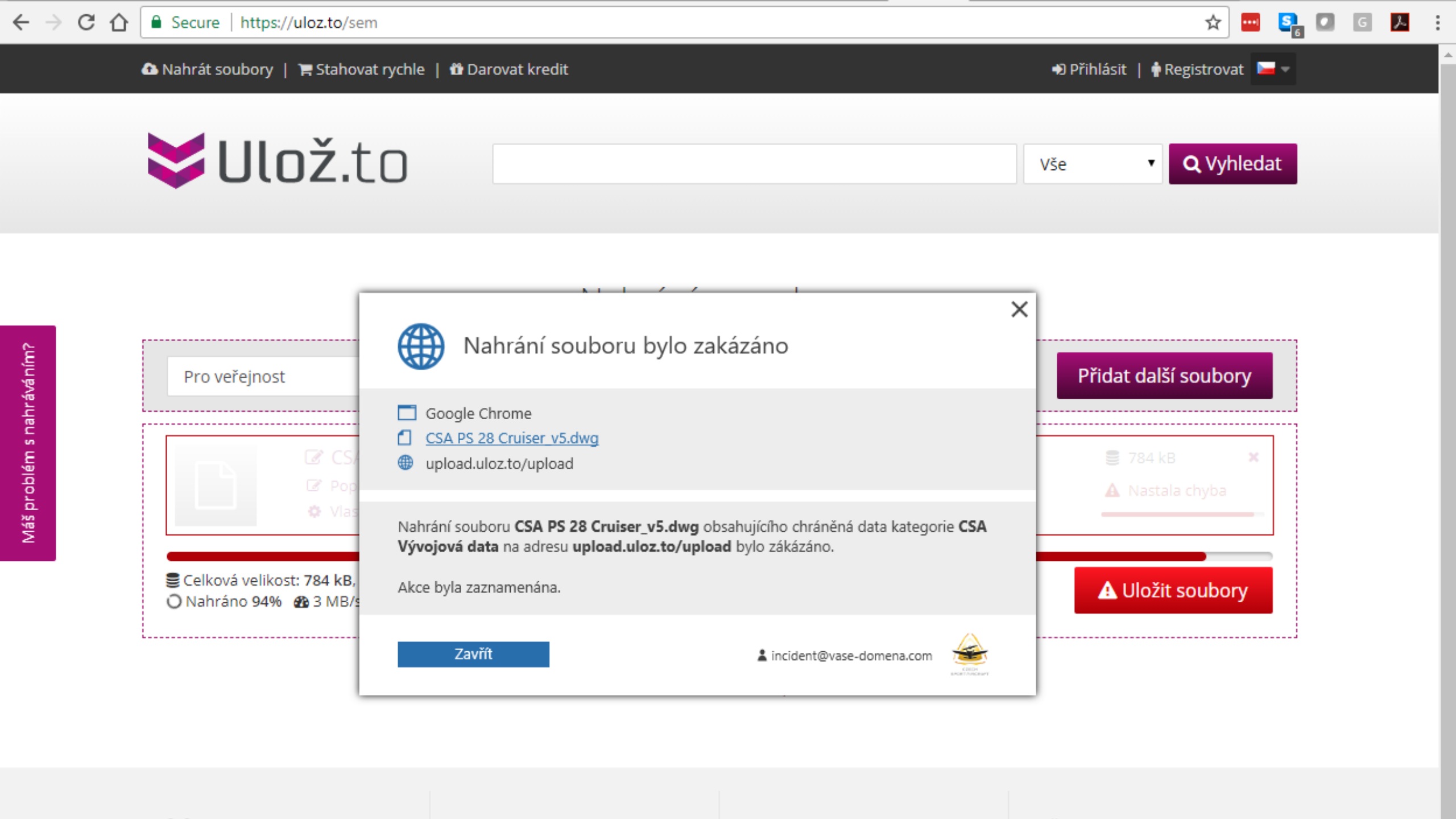


ZÁZNAMY

Export do .csv
Export do .xlsx

Počítač	Uživatelské j...	Počet incidentů	Počet operací ...	Počet soubor...	Počet soubor...	Počet soubor...	Počet soubor...	Počet vytiště...
Alfred Combs	PC-Sandoval	1	0	0	0	0	0	0
Carl Mooney	PC-Zimmerman	8	0	0	0	0	0	0
Carl Mooney	PC-Clark	8	120	14	1	0	26	0
Daphne Estrada	PC-Baird	1	0	0	0	0	0	0
Devin Franco	PC-Cobb	3	0	0	0	0	0	2
Devin Franco	PC-Harrington	3	4	0	0	0	46	0
Don Gonzalez	PC-Ortega	11	123	14	1	9	5	1
Erika Vargas	PC-Tyler	2	0	4	0	0	0	0


Karta pojištěnce - Zpráva (HTML)
Soubor
Zpráva
Vložení
Možnosti
Formátování textu
Revize
ADOBE PDF
Řekněte mi, co chcete udělat.
Pravopis a gramatika
Tezaurus
Počet slov
Kontrola pravopisu
Zkontrolovat přístupnost
Přístupnost
Inteligentní vyhledávání
Další informace
Přeložit
Jazyk
Jazyk
Poslat
Komu...
martinimrich@email.cz
Kopie...
Předmět
Karta pojištěnce
Připojeno
Karta pojištěnce_Martin Imrich.pdf
765 KB
Ahoj,
Posílám vyžádanou kartu pojištěnce.
Martin
Rizikové odeslání e-mailu
Microsoft Outlook
Karta pojištěnce
martinimrich@email.cz
Karta pojištěnce_Martin Imrich.pdf
Zapamatovat rozhodnutí pro tato data a příjemce
Přesto odeslat
Neodesílat
Více informací


Secure | https://uloz.to/sem
Nahrát soubory | Stahovat rychle | Darovat kredit
Přihlásit | Registrovat
Ulož.to
Vše
Vyhledat
Máš problém s nahráváním?
Pro veřejnost
Přidat další soubory
784 kB
Nastala chyba
Celková velikost: 784 kB,
Nahráno 94%
Uložit soubory
Nahrání souboru bylo zakázáno
Google Chrome
CSA PS 28 Cruiser_v5.dwg
upload.uloz.to/upload
Nahrání souboru CSA PS 28 Cruiser_v5.dwg obsahujícího chráněná data kategorie CSA Vývojová data na adresu upload.uloz.to/upload bylo zakázáno.
Akce byla zaznamenána.
Zavřít
incident@vase-domena.com

Safetica a Microsoft

Naši zákazníci

A co vaše data?

XEELO

Don’t complain. Just comply

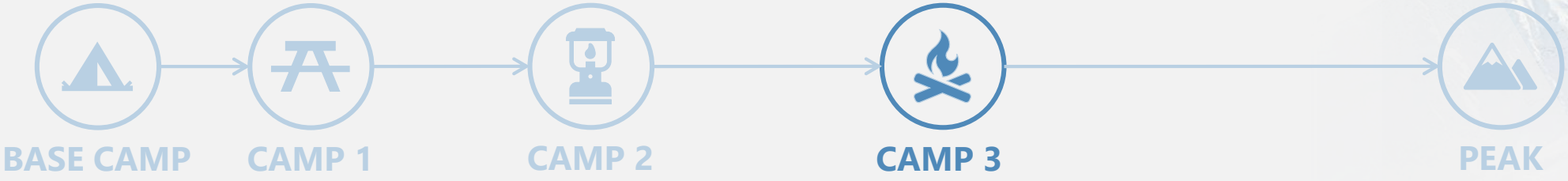
_ XEELO GDPR SOLUTION

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

Stoupání na vrchol – **ten menší**

Posuďte vliv na ochranu osobních údajů

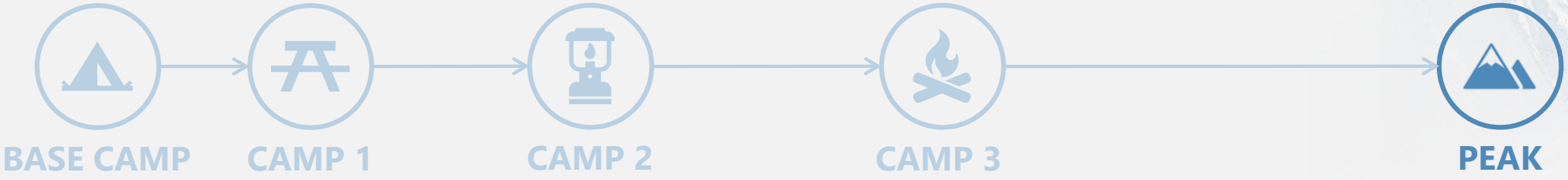
Zjistěte, **s jakými daty pracujete**, kde jsou uložena, kdo k nim má přístup a mnoho dalšího pomocí datového auditu.
Xeelo GDPR **nevytváří jen statický obrázek**, ale poskytuje **řadu výstupů**, které se vám můžou **hodit v budoucnu**.



Stoupání 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.



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...

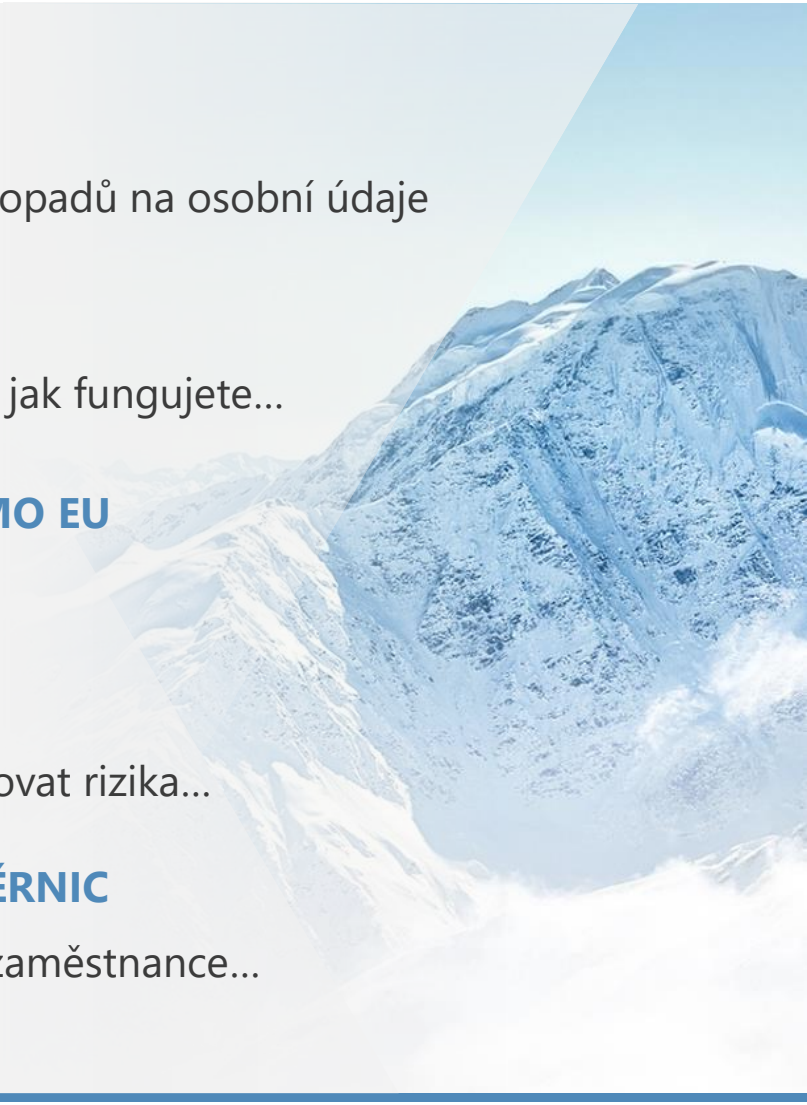
REGISTR PROCESŮ
Pro evidenci procesů a jejich dopadů na osobní údaje

ZÁZNAMY O ZPRACOVÁNÍ
Když se rozhodnete změnit to, jak fungujete...

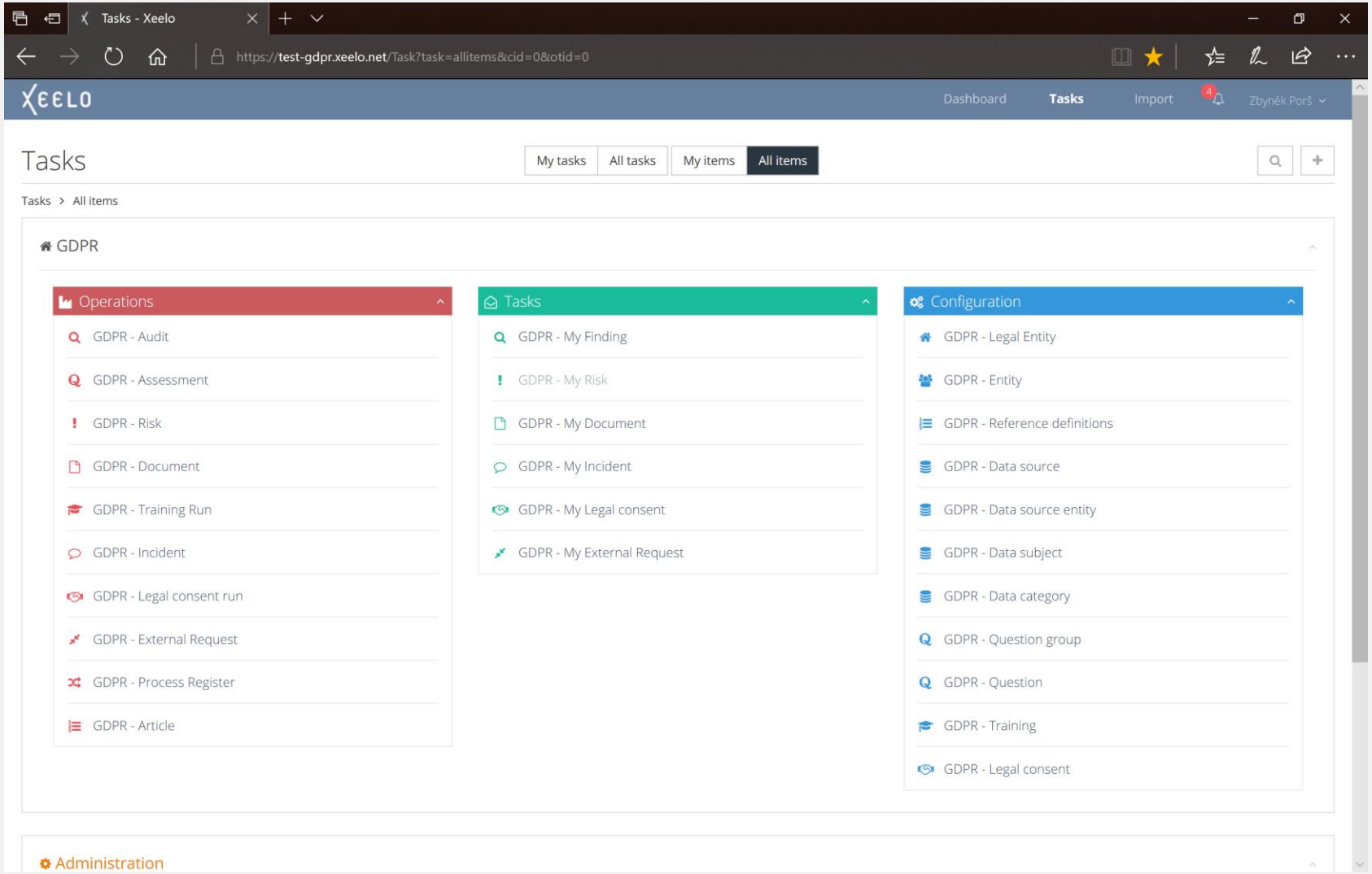
MIGRACE DAT DO ZEMÍ MIMO EU
Když moje data opouští EU...

ŘÍZENÍ RIZIK
Abyste mohli řídit a vyhodnocovat rizika...

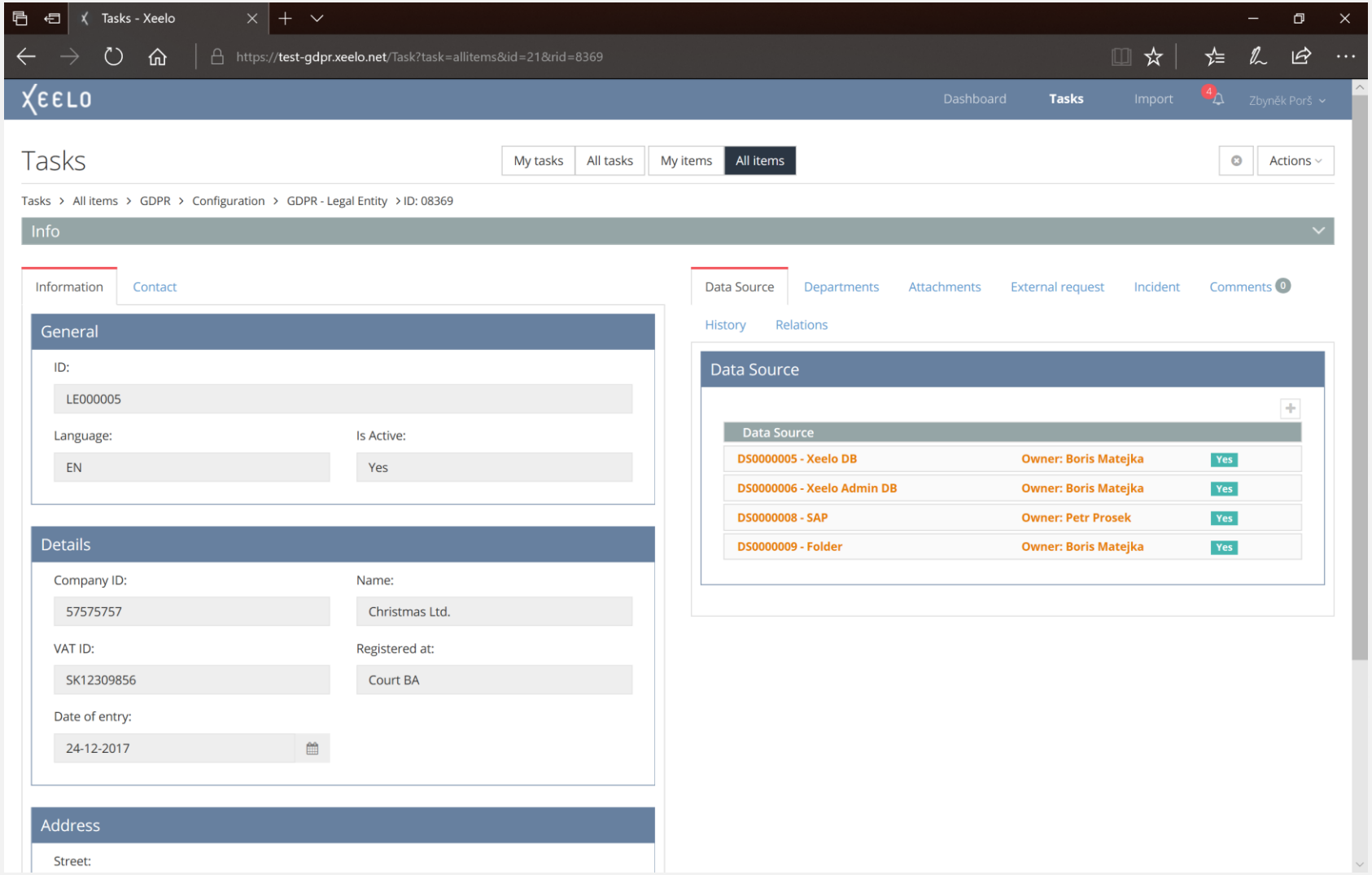
DISTRIBUCE INTERNÍCH SMĚRNIC
Pro prokázání, že informujete zaměstnance...



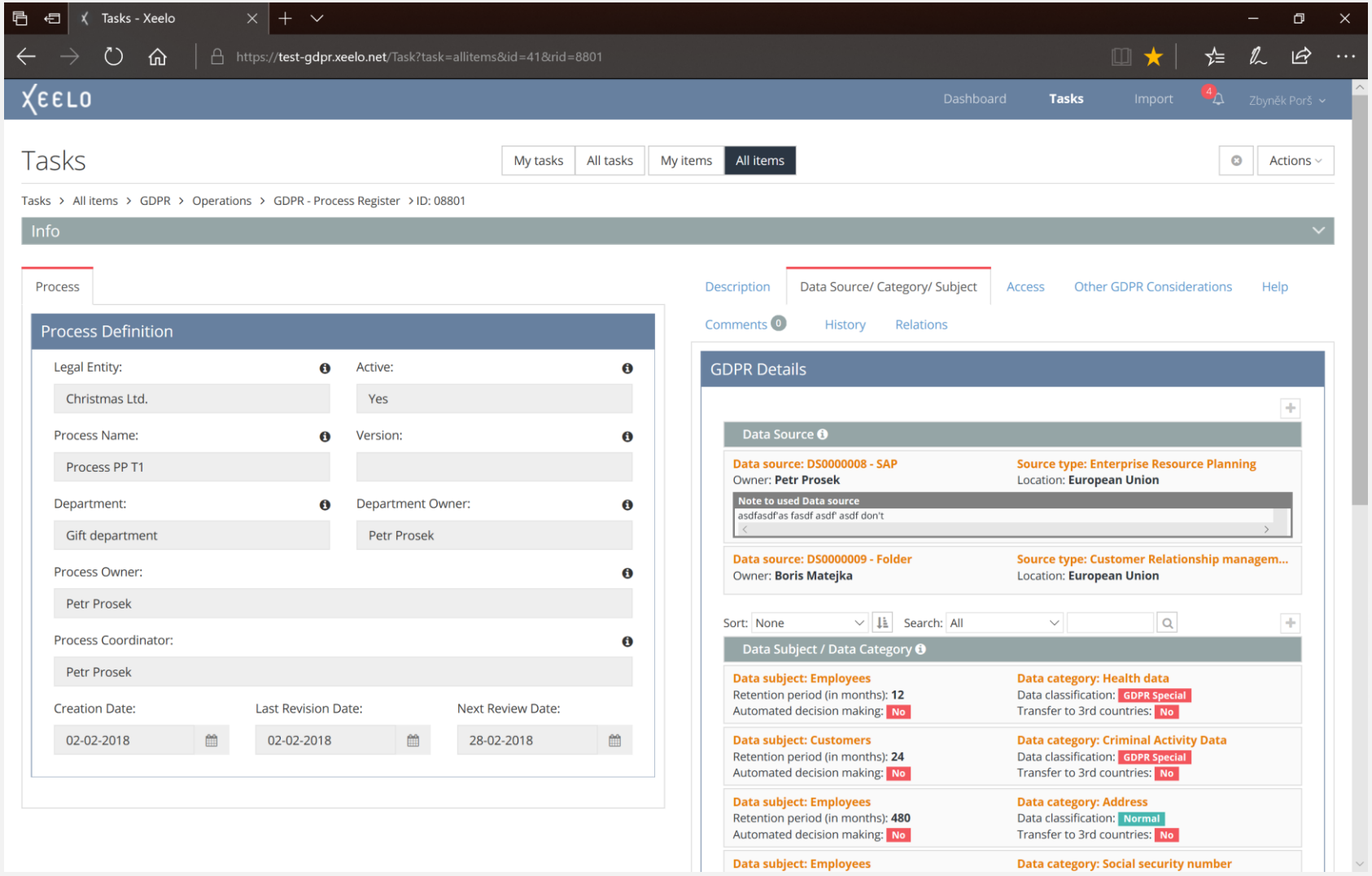
Jak **Xeelo GDPR** vypadá



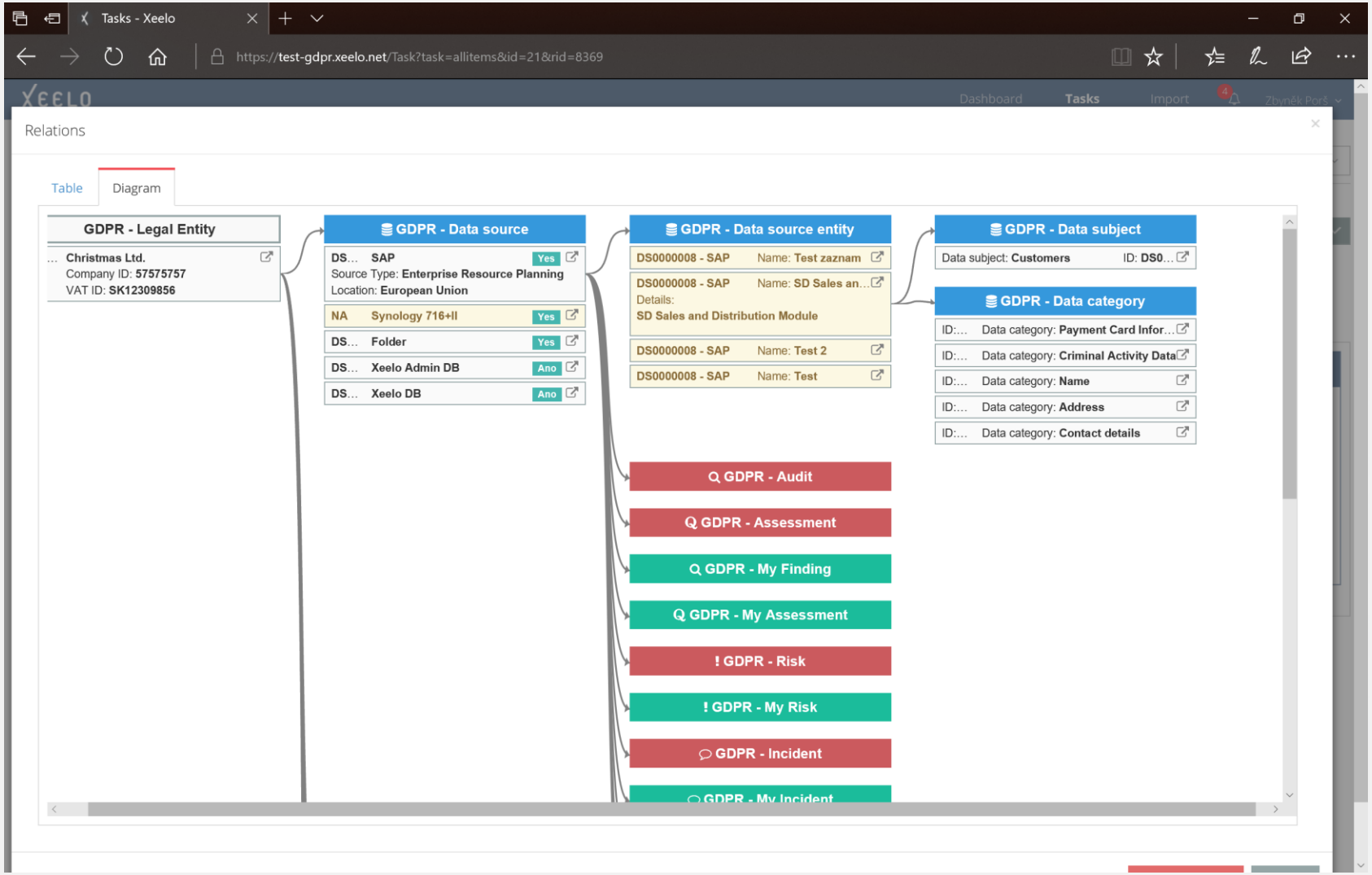
Jak **Xeelo GDPR** vypadá



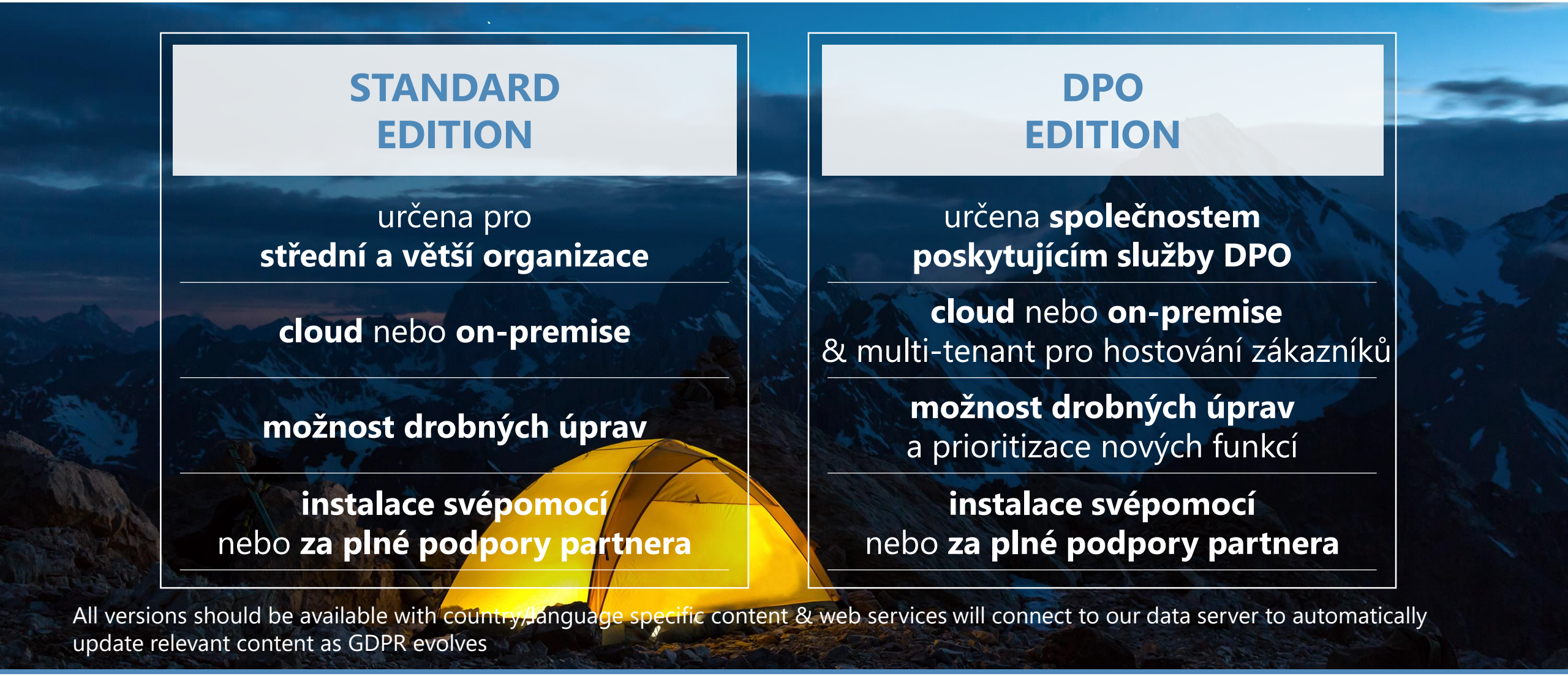
Jak **Xeelo GDPR** vypadá



Jak **Xeelo GDPR** vypadá



Dvě verze Xeela GDPR **k dispozici**



STANDARD EDITION

určena pro
střední a větší organizace

cloud nebo **on-premise**

možnost drobných úprav

instalace svépomocí
nebo **za plné podpory partnera**

DPO EDITION

určena **společnostem**
poskytujícím služby DPO

cloud nebo **on-premise**
& multi-tenant pro hostování zákazníků

možnost drobných úprav
a prioritizace nových funkcí

instalace svépomocí
nebo **za plné podpory partnera**

All versions should be available with country/language specific content & web services will connect to our data server to automatically update relevant content as GDPR evolves

Standard edition

DO 250 ZAMĚSTNANCŮ

800 EUR

MĚSÍČNĚ ZA JEDNU PRÁVNICKOU OSOBU

S 251 – 1 000 ZAMĚSTNANCI

2 400 EUR

MĚSÍČNĚ ZA JEDNU PRÁVNICKOU OSOBU

S 1 001 – 10 000 ZAMĚSTNANCI

4 800 EUR

MĚSÍČNĚ ZA JEDNU PRÁVNICKOU OSOBU

S VÍCE NEŽ 10 000 ZAMĚSTNANCI

individually

MĚSÍČNĚ ZA JEDNU PRÁVNICKOU OSOBU

Hosting costs not included.

Co jsme **zabalili do Xeela GDPR**

45

ČLÁNKŮ, KTERÉ SE VZTAHUJÍ NA ORGANIZACE

〉

40

Z NICH POKRÝVÁME V XEELU GDPR

5 ČLÁNKŮ nelze systémově nijak pokrýt.

www.xeelo.com/gdpr

Zdroje k GDPR:

Microsoft Corp hlavní stránka
microsoft.com/GDPR

Online Services Terms
Online Services Terms Download

Microsoft Trust Center
microsoft.com/trust

Service Trust Platform – podklady k certifikacím, audity
aka.ms/STP (requires log-in, NDA level)

Prezentace a zdroje v češtině:
aka.ms/jaknaGDPR

Partnerské stránky
Aka.ms/gdprpartners

GDPR Compliance Demo
http://www.microsoftgdprscenarios.com/en-us/databreach

Office 365 Information Protection for GDPR
https://docs.microsoft.com/en-us/office365/enterprise/office-365-information-protection-for-gdpr

Microsoft

Děkujeme Vám za pozornost

V případě dotazů kontaktujte prosmb@microsoft.com

Příště uvidíte:

- *Představení skutečného příběhu zákazníka*
- *Praktické kroky, jak malá firma o 20 lidech vyřešila GDPR*