Využití komerčních cloudových služeb pro splnění požadavků VKB

Zdeněk Jiříček, Tomáš Mirošník
Microsoft CZ/SK

Mít nebo nemít externího zpracovatele?

Je využití komerčního cloudu slabinou nebo výhodou z hlediska požadavků VKB č. 82/2018 Sb. a případně GDPR?

Standardy v oblasti bezpečnostních opatření

Bezpečnostní opatření ve VKB	Mapování na oblasti opatření v ISO 27001:2013 / ISO 27018:2014
§ 3 Systém řízení bezpečnosti informací	A.5 Information security policies
§ 4 Řízení aktiv	A.8 Asset management
§ 5 Řízení rizik	Viz ISAE 3000 report spol. PwC Czech: Zpráva o metodologii posuzování rizik Microsoft Online Services na základě požadavků, vyplývajících ze ZKB a VKB
§ 6 Organizační bezpečnost	A.6 Organization of information security
§ 7 Bezpečnostní role	A.6.1 Internal organization
§ 8 Řízení dodavatelů	A.15 Supplier relationships
§ 9 Bezpečnost lidských zdrojů	A.7 Human resource security
§ 10 Řízení provozu a komunikací	A.12 Operations security, A.13 Communications security
§ 11 Řízení změn	A.14.2 Security in development and support processes
§ 12 Řízení přístupu	A.9 Access control
§ 13 Akvizice, vývoj a údržba	A.14 System acquisition, development and maintenance
§ 14 Zvládání kybernetických bezpečnostních událostí a incidentů	A.16 Information security incident management
§ 15 Řízení kontinuity činností	A.17 Information security aspects of business continuity management
§ 16 Audit kybernetické bezpečnosti	A.12.7 Information systems audit considerations; A.18 Compliance
§ 17 Fyzická bezpečnost	A.11 Physical and environmental security
§ 18 Bezpečnost komunikačních sítí	A.13 Communications security, A.13.1 Network security management
§ 19 Správa a ověřování identit	A.9.2 User access management; A.10.8 Unique use of user IDs (ISO 27018)
§ 20 Řízení přístupových oprávnění	A.9.4 System and application access control
§ 21 Ochrana před škodlivým kódem	A.12.2 Protection from malware
§ 22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů	A.12.4 Logging and monitoring
§ 23 Detekce kybernetických bezpečnostních událostí	A.12.2 Protection from malware; A.16.1.6; A.16.1.7 Security Incident Management
§ 24 Sběr a vyhodnocování kybernetických bezpečnostních událostí	A.16.1 Management of information security incidents and improvements
§ 25 Aplikační bezpečnost	A.14.2 Security in development and support processes
§ 26 Kryptografické prostředky	A.10 Cryptography
§ 27 Zajišťování úrovně dostupnosti informací	A.17.1 Information security continuity
§ 28 Průmyslové, řídicí a obdobné specifické systémy	Neaplikuje se na Microsoft cloud
§ 29 Digitální služby	Aplikuje se v členském státě sídla poskytovatele (Microsoft Ireland)
§ 30 Bezpečnostní politika a bezpečnostní dokumentace	A.5 Information security policies

Microsoft cloud Trust Center: certifikace a audity

https://www.microsoft.com/en-us/trustcenter/compliance/complianceofferings

Global	Government	Industry	Regional
CIS Benchmark	CJIS	23 NYCRR Part 500	BIR 2012 (Netherlands)
CSA Cloud Control Matrix	CNSSI 1253	AFM + DNB (Netherlands)	C5 (Germany)
CSA-STAR-Attestation	DFARS	APRA (Australia)	CCSL/IRAP (Australia)
CSA-Star-Certification	DoD DISA L2, L3, L5	AMF and ACPR (France)	CS Mark (Gold) (Japan)
CSA STAR Self-Assessment	DoE 10 CFR Part 810	CDSA	Cyber Essentials Plus (UK)
ISO 20000-1:2011	EAR (US Export Administration Regulations)	CFTC 1.31 (US)	Canadian Privacy Laws
ISO 22301	FedRAMP	DPP (UK)	DJCP (China)
ISO 27001	FIPS 140-2	EBA (EU)	EN 301 549 (EU)
ISO 27017	IRS 1075	FACT (UK)	ENS (Spain)
ISO 27018	ITAR	FCA (UK)	ENISA IAF (EU)
ISO 27701	NIST 800-171	FDA CFR Title 21 Part 11	EU-Model-Clauses
ISO-9001	NIST Cybersecurity Framework (CSF)	FERPA	EU-U.S. Privacy Shield
SOC 1	Section 508 VPATS	FFIEC (US)	GB 18030 (China)
SOC 2		FINMA (Switzerland)	GDPR (EU)

VKB – ISMS, řízení rizik, bezp. politika

VKB č. 82/2018 Sb.	Co je třeba udělat	Jak může Microsoft pomoci
§5 Řízení rizik (volba metodiky, posouzení rizik, volba opatření)	Posouzení rizik ochrany aktiv v rámci vymezeného ISMS	**PwC Czech – zpráva o posuzování rizik** v Microsoft Online Services
	Nástroj pro kontinuální řízení rizik a dokumentaci zavedených opatření	**Microsoft Compliance Manager,** dokumentace na aka.ms/STP
	Výběr bezpečnostních opatření / zmírnění inherentních rizik	**Zapojit opatření na straně Microsoftu** dle ISO 27k / NIST
§6 Organizační bezpečnost	Stanovení bezpečnostní politiky pro ISMS	Využít jako základ **bezpečnostní politiku** online služeb **Microsoft**
	Zajištění dostupnosti zdrojů pro ISMS	**Smluvní závazky** v „Podmínkách pro služby online“
	Pravidla pro administrátory a jejich mlčenlivost	Office 365 **Lockbox**, Azure **Lockbox**, závazek důvěrnosti, přístup jen v případě potřeby – JIT Access

Co když budu mít cloudové služby v ISMS?

ZKB č. 181/2014 Sb. a jeho VKB č. 82/2018 Sb.

- ZKB §3 – Microsoft standardně v roli poskytovatele dig. služeb (DSP)
- ZKB §4 (4) povinnost zohlednit bezp. opatření při výběru dodavatele
- ZKB §4 (5) smluvní podmínky – viz zhodnocení souladu od kanceláře Pierstone
- ZKB §5: Bezp. opatření viz Podmínky OST, ISO 27k a auditní zprávy SSAE18

- VKB §8: Řízení dodavatelů: rizika – PWC ISAE 3000 report, opatření – OST a ISO
- VKB Příloha č. 2 – hodnocení rizik: použít MS vzorové dokumenty
- VKB Příloha č. 4 – Likvidace dat do úrovně důvěrnosti 3. – „vysoká" včetně
- VKB Příloha č. 7 – Řízení dodavatelů: viz zhodnocení souladu (Pierstone)

Česká stránka na STP Portálu

www.aka.ms/CZCR (CZ Compliance Resources)

Právní analýza souladu s požadavky ZKB

GDPR DPIA | Compliance Guides | GRC Assessment Reports | Legal Opinions

Document	Description	Report Date
Soulad smluvní dokumentace online služeb společnosti Microsoft s požadavky na obsah smlouvy uzavírané s významnými dodavateli ve smyslu vyhlášky o kybernetické bezpečnosti	Právní posouzení souladu smluvních podmínek cloudových služeb společnosti Microsoft s požadavky vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti na obsah smlouvy uzavírané s významnými dodavateli	2019-05-30
Zákonné požadavky na smlouvy o poskytování cloud computingových služeb ve smyslu zákona o kybernetické bezpečnosti	Právní posouzení souladu smluvních podmínek cloudových služeb společnosti Microsoft s požadavky §4 novely Zákona o kybernetické bezpečnosti (ZKB), účinné od 1.8.2017.	2018-06-06

Sdílená odpovědnost **Správce - Zpracovatel**

Řízení rizik na straně Správce

Kategorizace údajů a stanovení politik ochrany

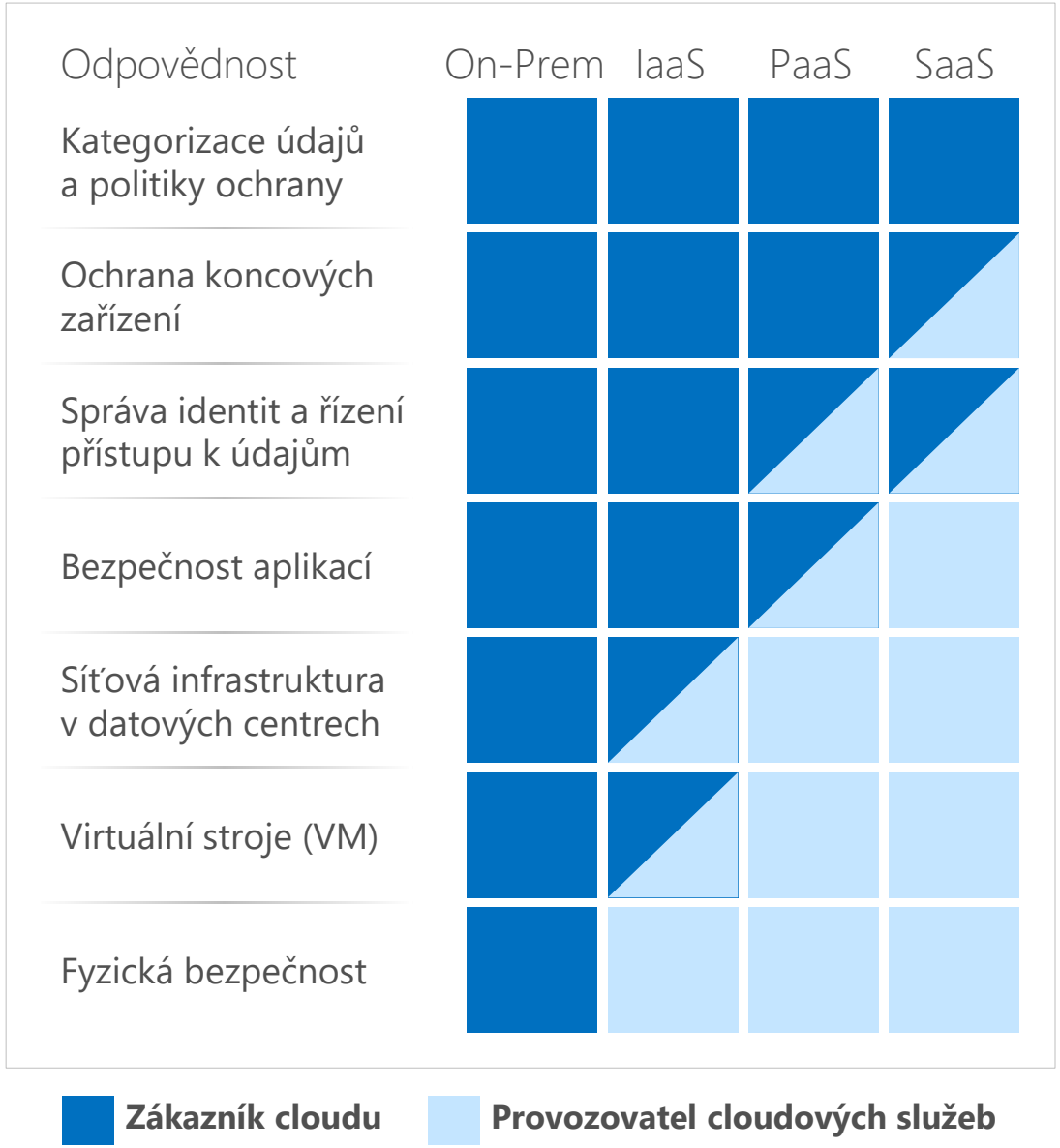
Sdílené řízení rizik

Správa identit a řízení přístupu k údajům

Řízení rizik na straně Zpracovatele

Fyzická bezpečnost a infrastruktura datových center

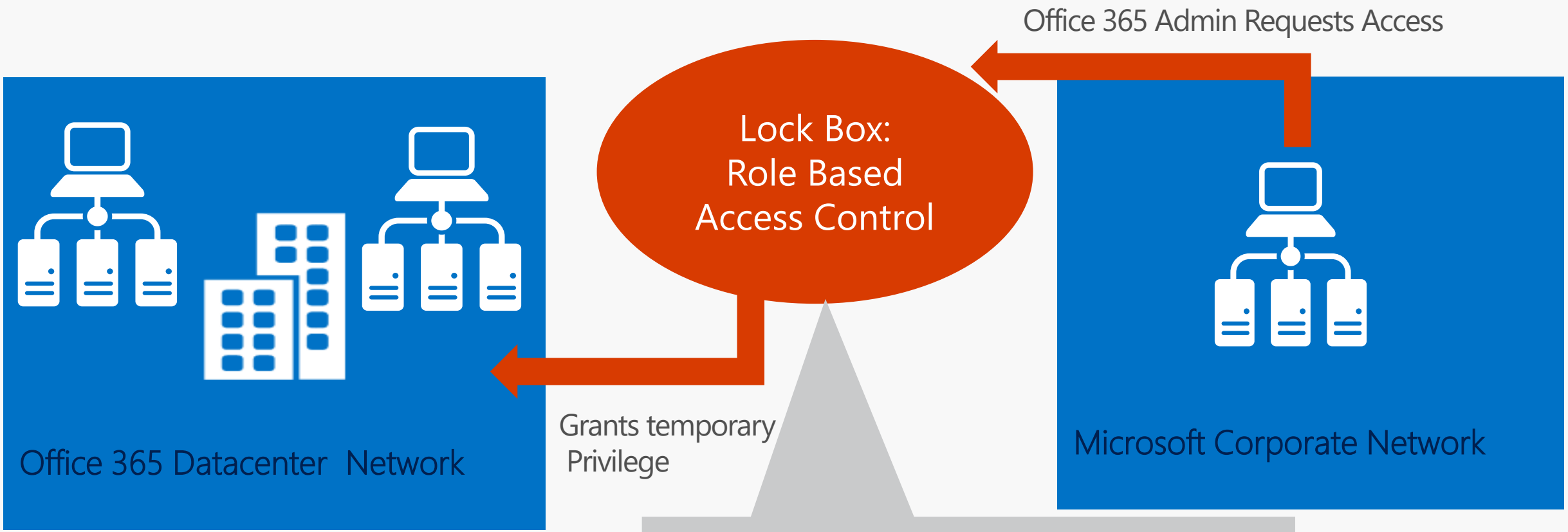
[Shared responsibility](#) – Microsoft whitepaper



VKB – §4 – Řízení aktiv

VKB č. 82/2018 Sb.	Co je třeba udělat	Jak může Microsoft pomoci
§4 Řízení aktiv (1) h) – Pravidla ochrany aktiv (1) i) – Způsoby používání aktiv (1) j) – Způsob likvidace dat	Zařadit aktiva do úrovní důležitosti	Uživatelsky přívětivé **„štítkování" aktiv** (dokumenty, emaily… Office 365 Labels)
	Stanovit přiměřená pravidla pro zabezpečení	Politiky pro automatické nastavení ochrany (dokumenty, emaily) – **Azure Information Protection (AIP)**
	Pravidla pro bezpečné elektronické sdílení aktiv	Nástroje pro klasifikaci dokumentů, emailů, úložišť, sdílení: Teams / Sharepoint / Outlook. s pomocí **AIP**
	Způsob likvidace dat v souladu s VKB Příloha č. 4	Azure, Office 365, Dynamics 365: • Úroveň **střední**: šifrování na úrovni média • Úroveň **vysoká**: šifrování s uložením klíčů v certifikovaném HSM modulu pod exkluzívní kontrolou zákazníka (**KeyVault**)

Restrikce přístupu na zákaznická data



Office 365 Plan **E5 „Customer Lock Box“** requires explicit customer approval to issue one-time credentials

Grants least privilege required to complete task.
Verify eligibility by checking if

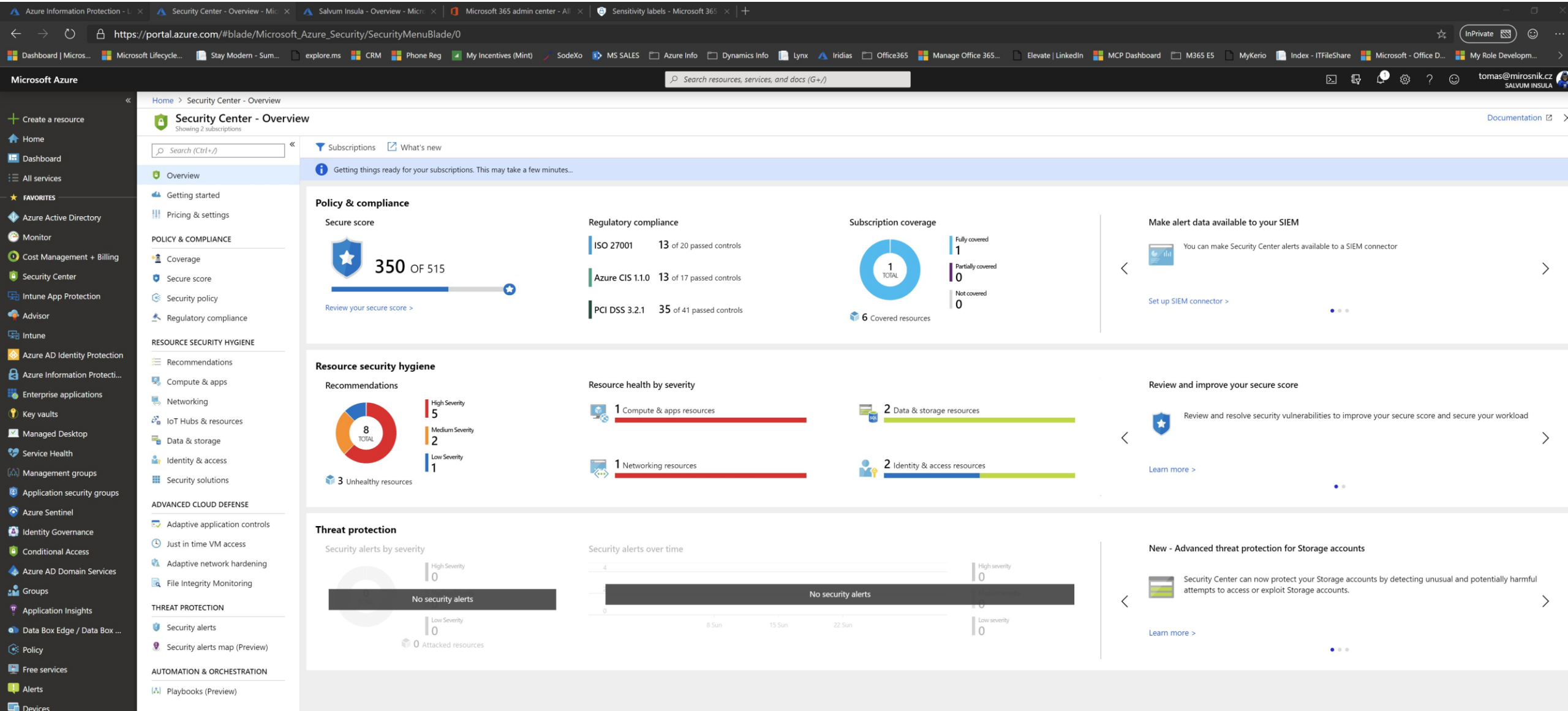
1. Background Check Completed
2. Fingerprinting Completed
3. Security Training Completed

VKB – Řízení provozu a komunikací

VKB č. 82/2018 Sb.	Co je třeba udělat	Jak může Microsoft pomoci
§10 Řízení provozu a komunikací, (1) Provozní pravidla a postupy §18 Bezpečnost kom. sítí §21 Ochrana před škodlivým kódem	Sledování kyber událostí	Široké možnosti **logování vč. API**
	Ochrana před škodlivým kódem	Microsoft **Defender ATP**, **O365 ATP**
	Ochrana informací v celém živ. cyklu	Azure Information Protection – **AIP,** Office 365 Data Loss Prevention (**DLP**) policies, **Intune - mobility**
	Zálohování a kontrola použitelnosti	Georedundantní **BC/DR, ISO 22301**
§22 Zaznamenávání událostí (logy)	Logování bezpečnostních a provozních událostí	Office 365 **audit logging** a **mailbox auditing** s možností forenzní analýzy šlodlivých aktivit. **Office 365 Alert Policies**
	Dlouhodobé ukládání logů (12/18 měs.)	Office 365 **Management Activity API** reference a integrace **SIEM**
	Synchronizace času min. 1x za 24 hod.	Ano, nejpozději každou hodinu a s přesností na 1 milisekundu.

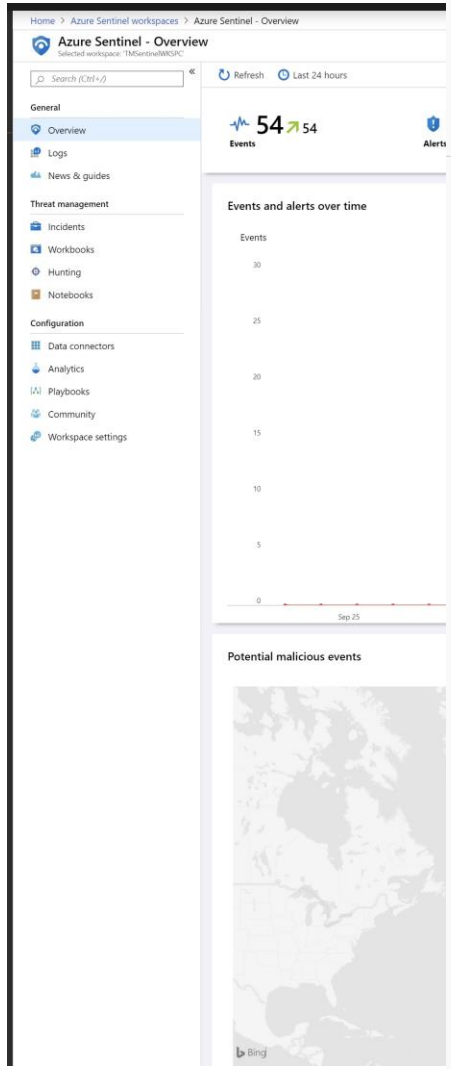
Řízení provozu a komunikací

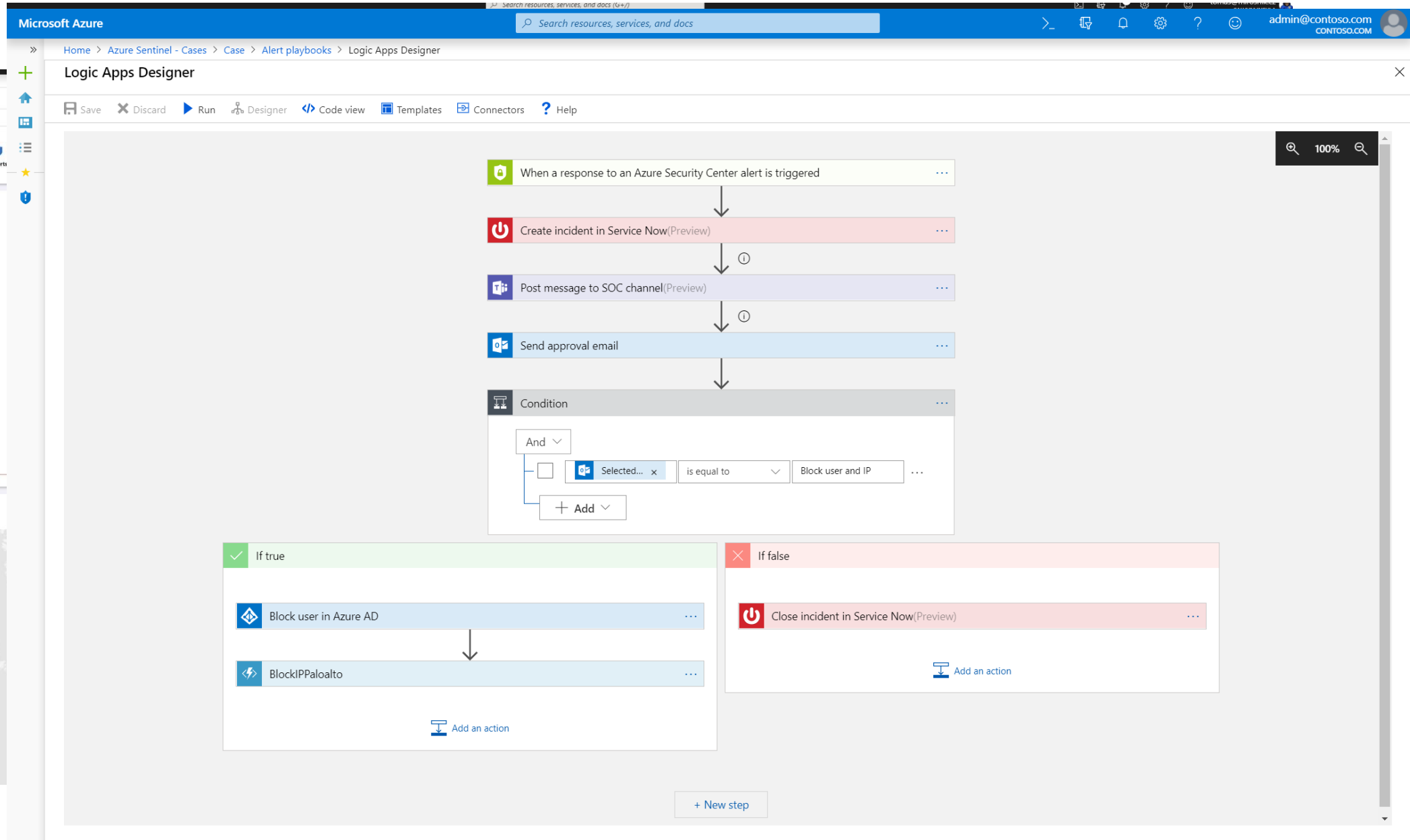
Sledování kyber událostí: Security Center - základ

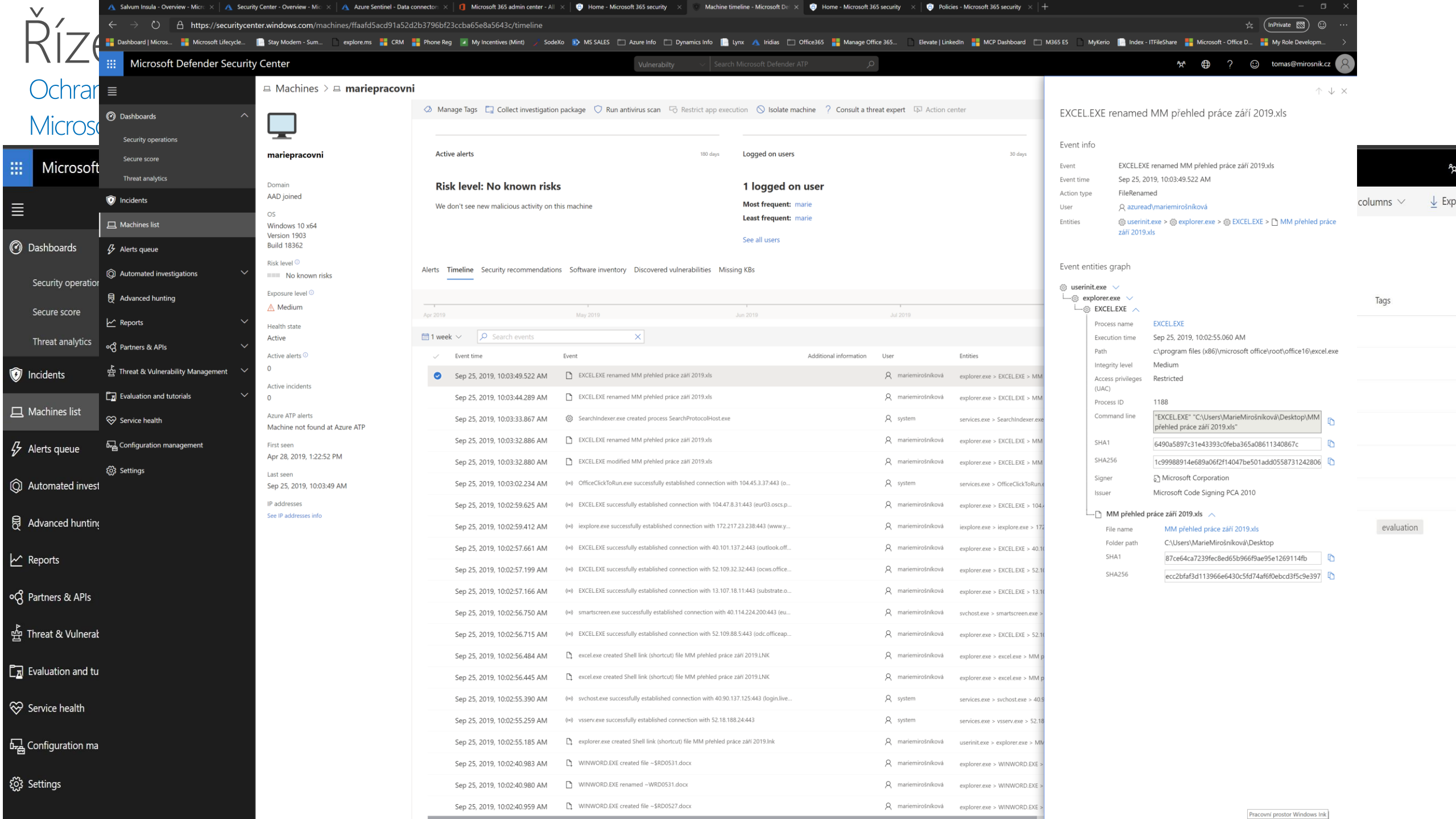


Řízení provozu a komunikací

Pokročilé sledování kyber událostí: Azure Sentinel

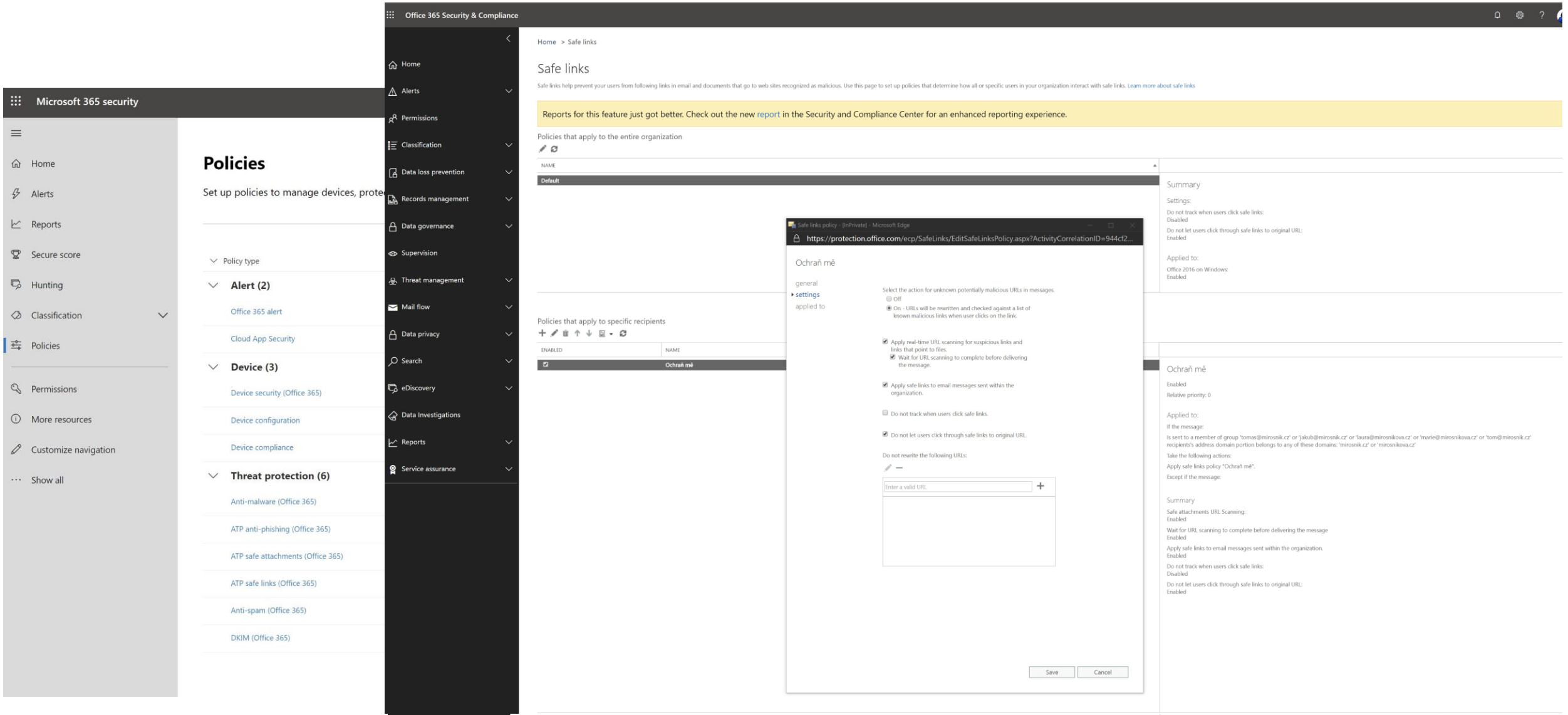





Microsoft Defender Security Center
Machines > mariepracovni
marieprocovni
Manage Tags
Collect investigation package
Run antivirus scan
Restrict app execution
Isolate machine
Consult a threat expert
Action center
Active alerts
Risk level: No known risks
We don't see new malicious activity on this machine
Logged on users
1 logged on user
Most frequent: marie
Least frequent: marie
See all users
Alerts
Timeline
Security recommendations
Software inventory
Discovered vulnerabilities
Missing KBs
Event time
Event
Additional information
User
Entities
EXCEL.EXE renamed MM přehled práce září 2019.xls
Event info
Event
Event time
Action type
User
Entities
Event entities graph
userinit.exe
explorer.exe
EXCEL.EXE
Process name
Execution time
Path
Integrity level
Access privileges (UAC)
Process ID
Command line
SHA1
SHA256
Signer
Issuer
MM přehled práce září 2019.xls
File name
Folder path
SHA1
SHA256

Řízení provozu a komunikací

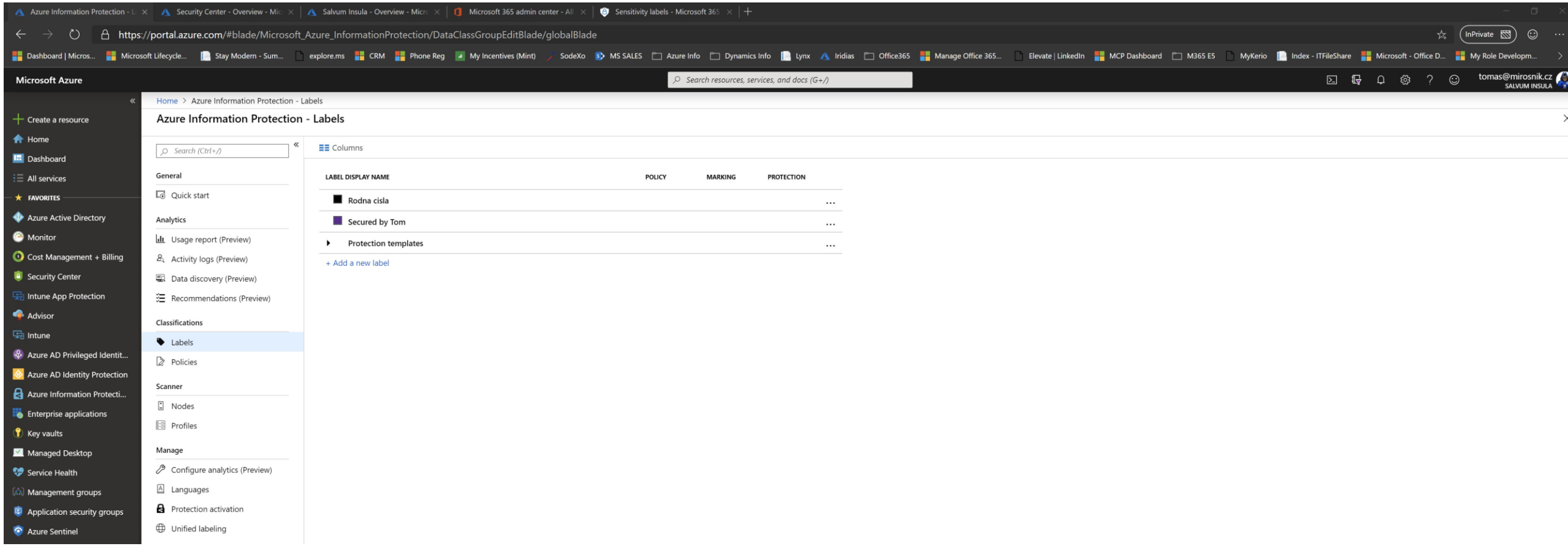
Office 365 ATP



Řízení provozu a komunikací

Ochrana informací v celém životním cyklu

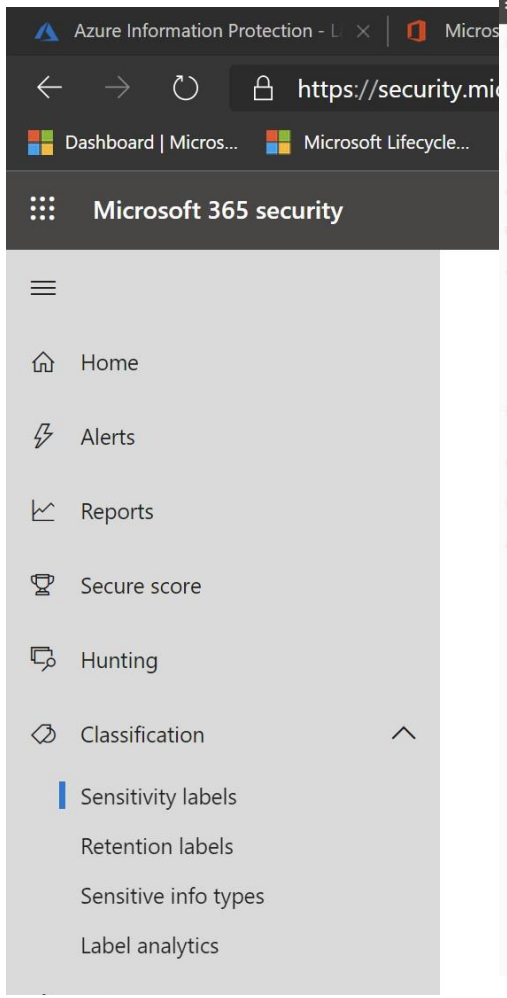
AIP – Azure Information Protection

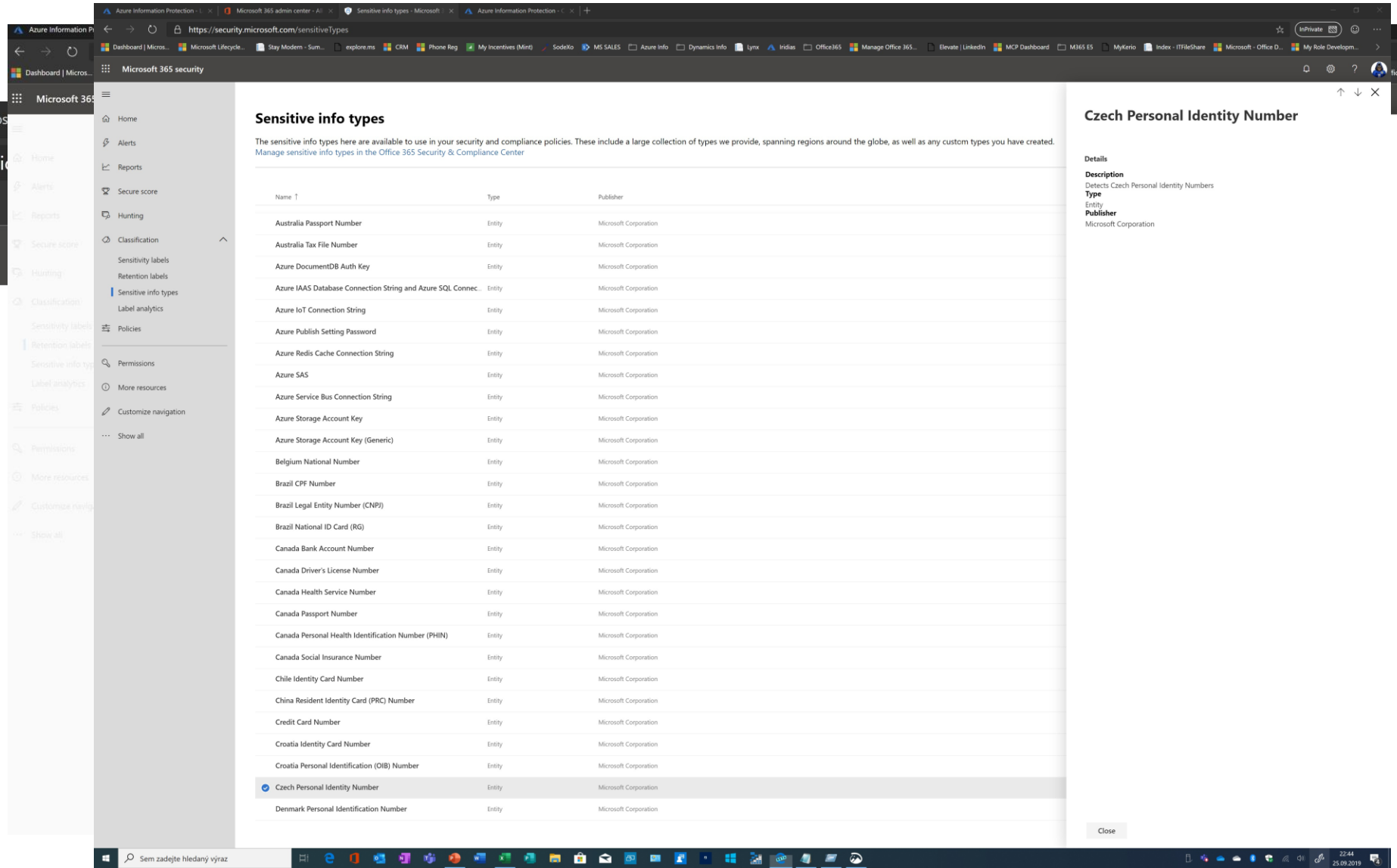


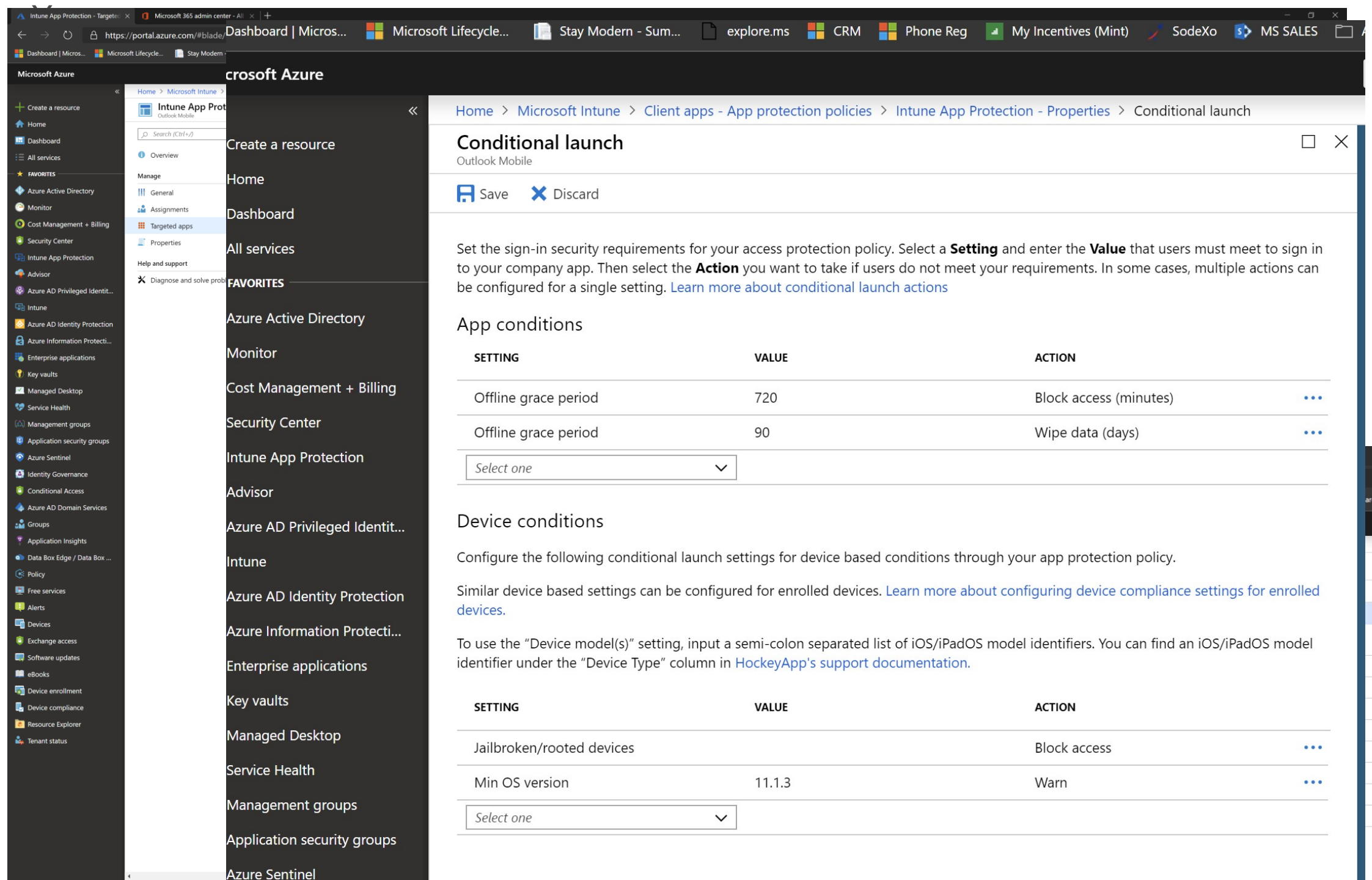
Řízení provozu a komunikací

Ochrana informací v celém životním cyklu

DLP M 365



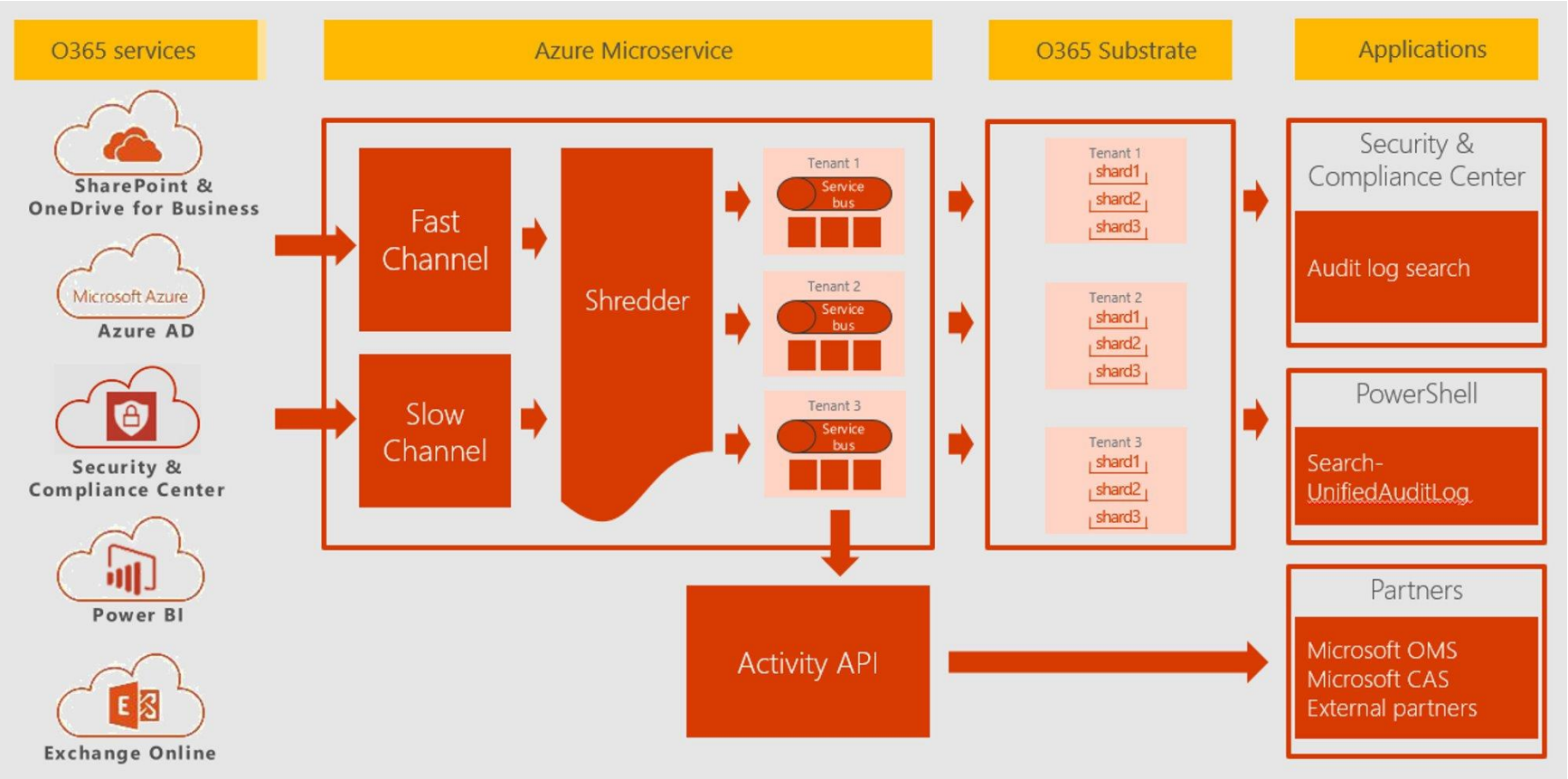


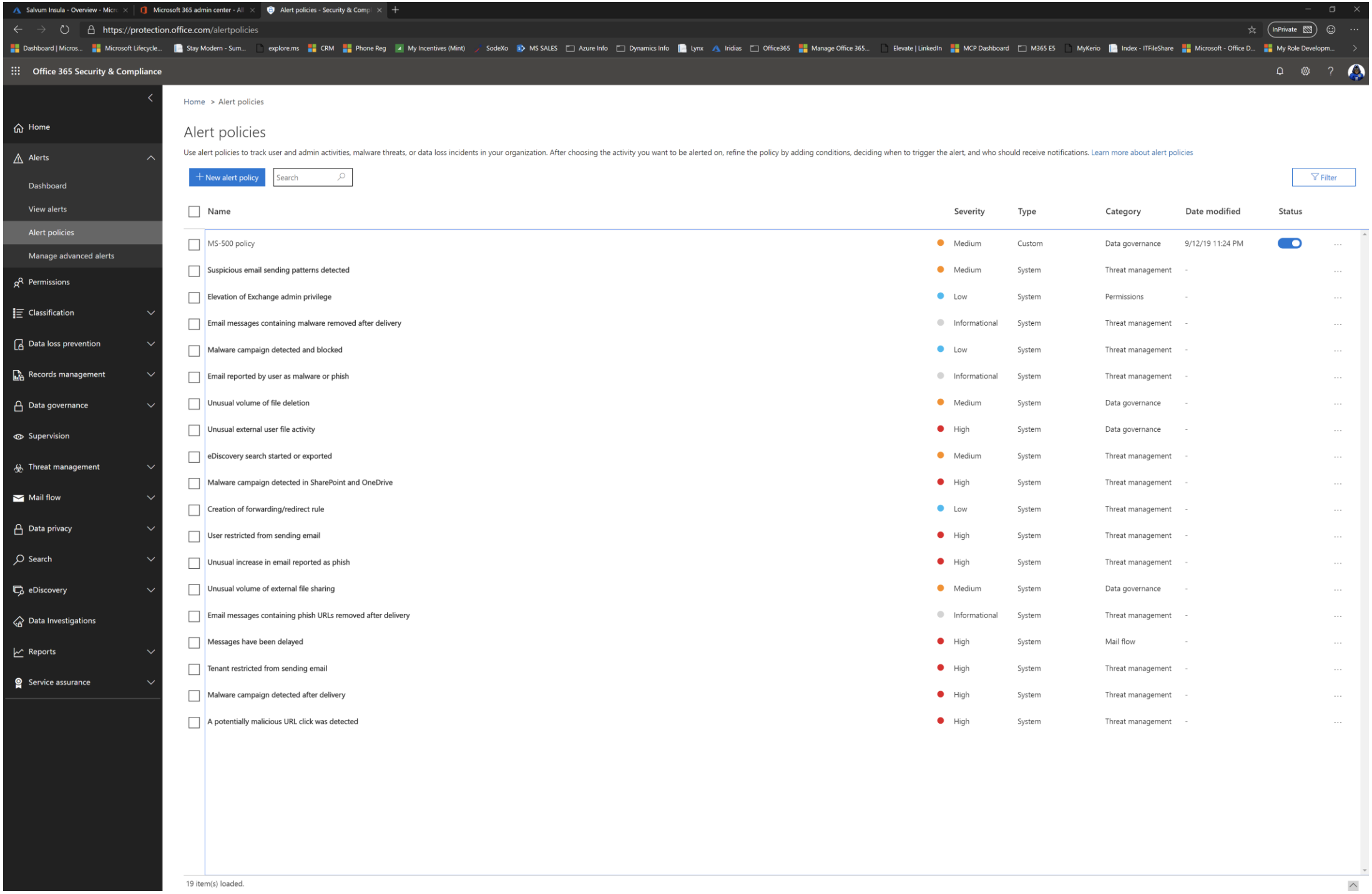

Intune App Protection - Targete
Microsoft 365 admin center - All
https://portal.azure.com/#blade/
Dashboard | Micros...
Microsoft Lifecycle...
Stay Modern - Sum...
explore.ms
CRM
Phone Reg
My Incentives (Mint)
SodeXo
MS SALES
Microsoft Azure
crosoft Azure
Create a resource
Home
Dashboard
All services
FAVORITES
Azure Active Directory
Monitor
Cost Management + Billing
Security Center
Intune App Protection
Advisor
Azure AD Privileged Identit...
Intune
Azure AD Identity Protection
Azure Information Protecti...
Enterprise applications
Key vaults
Managed Desktop
Service Health
Management groups
Application security groups
Azure Sentinel
Identity Governance
Conditional Access
Azure AD Domain Services
Groups
Application Insights
Data Box Edge / Data Box ...
Policy
Free services
Alerts
Devices
Exchange access
Software updates
eBooks
Device enrollment
Device compliance
Resource Explorer
Tenant status
Home > Microsoft Intune
Intune App Prot
Outlook Mobile
Search (Ctrl+/)
Overview
Manage
General
Assignments
Targeted apps
Properties
Help and support
Diagnose and solve prob
Create a resource
Home
Dashboard
All services
FAVORITES
Azure Active Directory
Monitor
Cost Management + Billing
Security Center
Intune App Protection
Advisor
Azure AD Privileged Identit...
Intune
Azure AD Identity Protection
Azure Information Protecti...
Enterprise applications
Key vaults
Managed Desktop
Service Health
Management groups
Application security groups
Azure Sentinel
Home > Microsoft Intune > Client apps - App protection policies > Intune App Protection - Properties > Conditional launch
Conditional launch
Outlook Mobile
Save
Discard
Set the sign-in security requirements for your access protection policy. Select a Setting and enter the Value that users must meet to sign in to your company app. Then select the Action you want to take if users do not meet your requirements. In some cases, multiple actions can be configured for a single setting. Learn more about conditional launch actions
App conditions
SETTING
VALUE
ACTION
Offline grace period
720
Block access (minutes)
Offline grace period
90
Wipe data (days)
Select one
Device conditions
Configure the following conditional launch settings for device based conditions through your app protection policy.
Similar device based settings can be configured for enrolled devices. Learn more about configuring device compliance settings for enrolled devices.
To use the "Device model(s)" setting, input a semi-colon separated list of iOS/iPadOS model identifiers. You can find an iOS/iPadOS model identifier under the "Device Type" column in HockeyApp's support documentation.
SETTING
VALUE
ACTION
Jailbroken/rooted devices
Block access
Min OS version
11.1.3
Warn
Select one
InPrivate
Microsoft - Office D...
My Role Developm...
tomas@mirosni
SALVUM INS

Řízení provozu a komunikací

Dlouhodobé ukládání logů

Office 365 Management Activity API reference a integrace SIEM

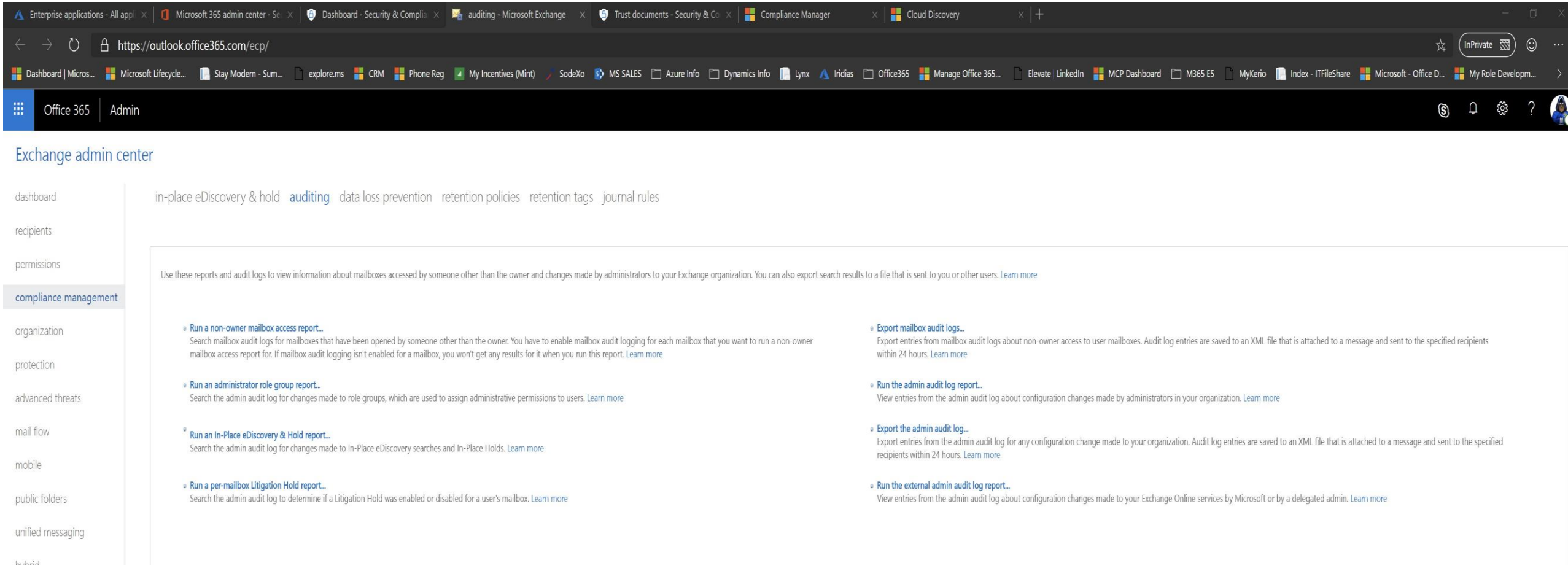



Salvum Insula - Overview - Micr
Microsoft 365 admin center - All
Alert policies - Security & Compl
https://protection.office.com/alertpolicies
InPrivate
Dashboard | Micros...
Microsoft Lifecycle...
Stay Modern - Sum...
explore.ms
CRM
Phone Reg
My Incentives (Mint)
SodeXo
MS SALES
Azure Info
Dynamics Info
Lynx
Iridias
Office365
Manage Office 365...
Elevate | LinkedIn
MCP Dashboard
M365 E5
MyKerio
Index - ITFileShare
Microsoft - Office D...
My Role Developm...
Office 365 Security & Compliance
Home
Alerts
Dashboard
View alerts
Alert policies
Manage advanced alerts
Permissions
Classification
Data loss prevention
Records management
Data governance
Supervision
Threat management
Mail flow
Data privacy
Search
eDiscovery
Data Investigations
Reports
Service assurance
Home > Alert policies
Alert policies
Use alert policies to track user and admin activities, malware threats, or data loss incidents in your organization. After choosing the activity you want to be alerted on, refine the policy by adding conditions, deciding when to trigger the alert, and who should receive notifications. Learn more about alert policies
New alert policy
Search
Filter
Name
Severity
Type
Category
Date modified
Status
MS-500 policy
Medium
Custom
Data governance
9/12/19 11:24 PM
Suspicious email sending patterns detected
Medium
System
Threat management
Elevation of Exchange admin privilege
Low
System
Permissions
Email messages containing malware removed after delivery
Informational
System
Threat management
Malware campaign detected and blocked
Low
System
Threat management
Email reported by user as malware or phish
Informational
System
Threat management
Unusual volume of file deletion
Medium
System
Data governance
Unusual external user file activity
High
System
Data governance
eDiscovery search started or exported
Medium
System
Threat management
Malware campaign detected in SharePoint and OneDrive
High
System
Threat management
Creation of forwarding/redirect rule
Low
System
Threat management
User restricted from sending email
High
System
Threat management
Unusual increase in email reported as phish
High
System
Threat management
Unusual volume of external file sharing
Medium
System
Data governance
Email messages containing phish URLs removed after delivery
Informational
System
Threat management
Messages have been delayed
High
System
Mail flow
Tenant restricted from sending email
High
System
Threat management
Malware campaign detected after delivery
High
System
Threat management
A potentially malicious URL click was detected
High
System
Threat management
19 item(s) loaded.

Řízení provozu a komunikací

Logování bezpečnostních a provozních událostí

Office 365 audit logging a mailbox auditing s možností forenzní analýzy šlodlivých aktivit.

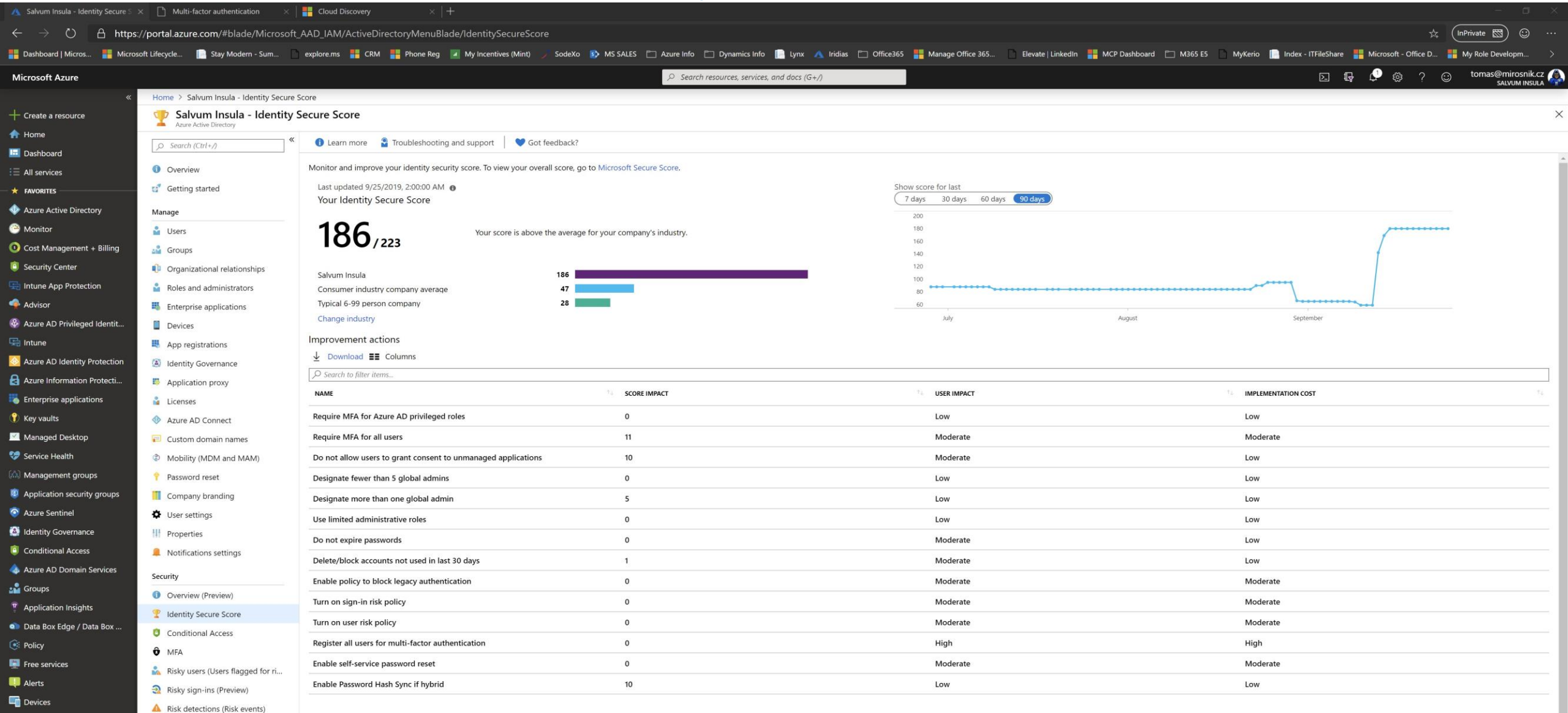


VKB – Řízení přístupu

VKB č. 82/2018 Sb.	Co je třeba udělat	Jak může Microsoft pomoci
§12 Řízení přístupu §19 Správa a ověřování identit §20 Řízení přístupových oprávnění §22 Zaznameávání událostí uživatelů a administrátorů	Vícefaktorová autentizace, příp. politiky pro silná hesla	Identity and device **access policies**, **MFA**, strong password policies
	Přidělování privilegovaných oprávnění jen na nezbytně nutnou úroveň/dobu, pravidelný přezkum přidělených oprávnění	Azure AD **Privileged Identity Management**, **Privileged Access Mgmt in O365**
	Kontrola cizích přístupů do mailboxu	Audit **non-owner mailbox access**
	Kontroly neúspěšné manipulace s účty nebo oprávněními	Office 365 **Alert Policies**, **Data Loss Prevention** reports and Microsoft **Cloud App Security**
	Řízení oprávnění na úrovni aktiva	Azure Information Protection – **AIP**

Řízení přístupu

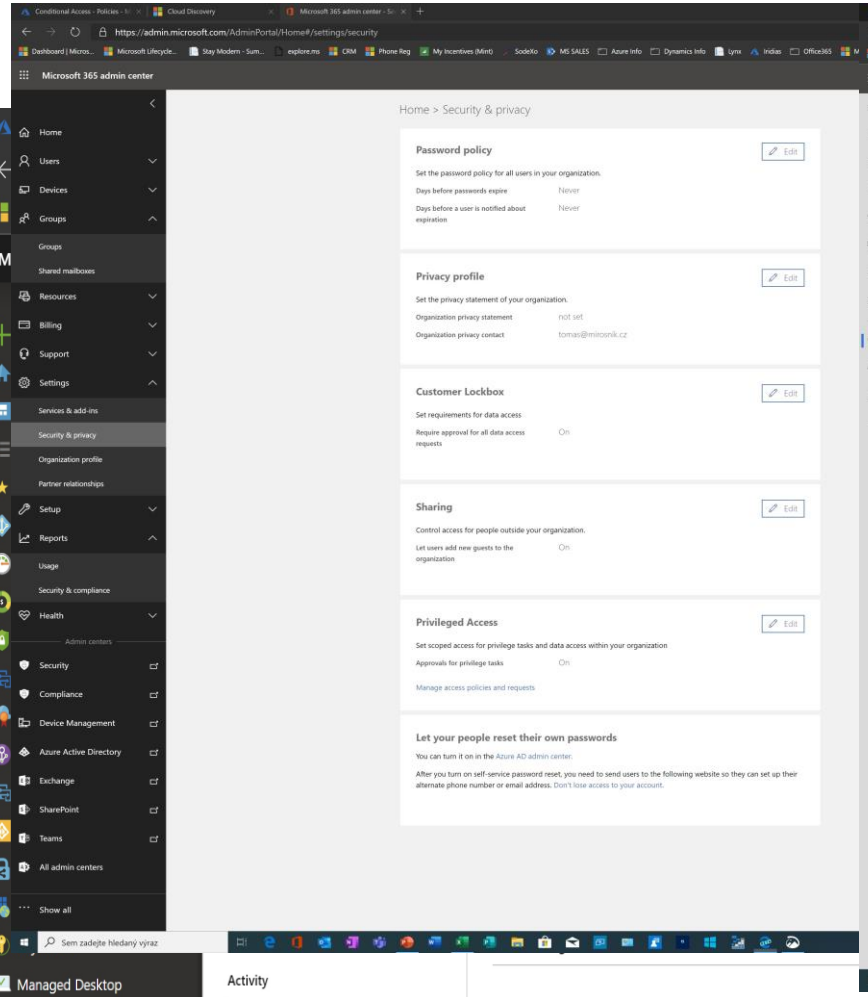
Vícefaktorová autentizace, příp. politiky pro silná hesla, MFA

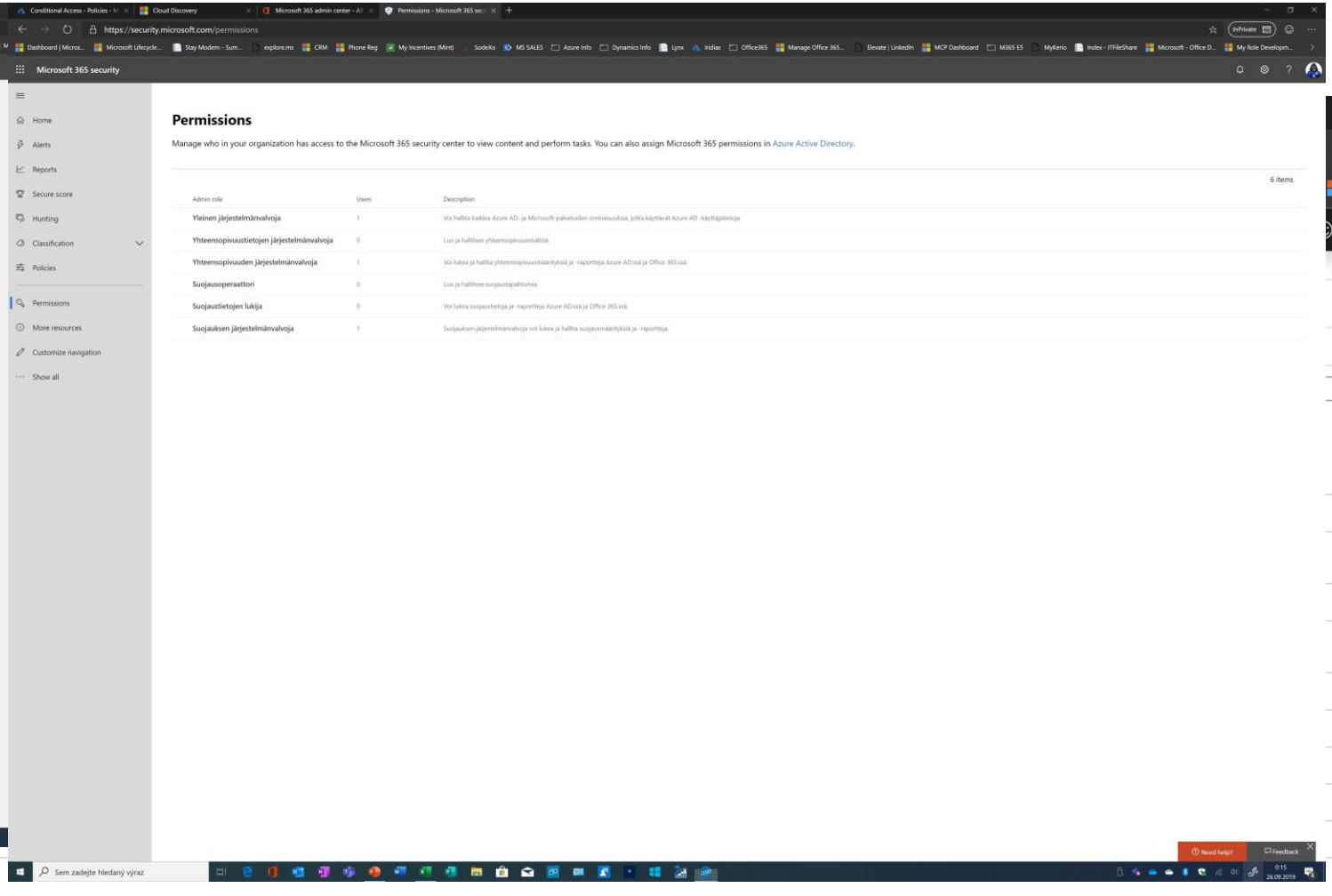


Řízení přístupu

Přidělování privilegovaných oprávnění jen na nezbytně nutnou úroveň/dobu, pravidelný přezkum přidělených oprávnění

Azure AD Privileged Identity Management , Privileged Access Management in Office 365

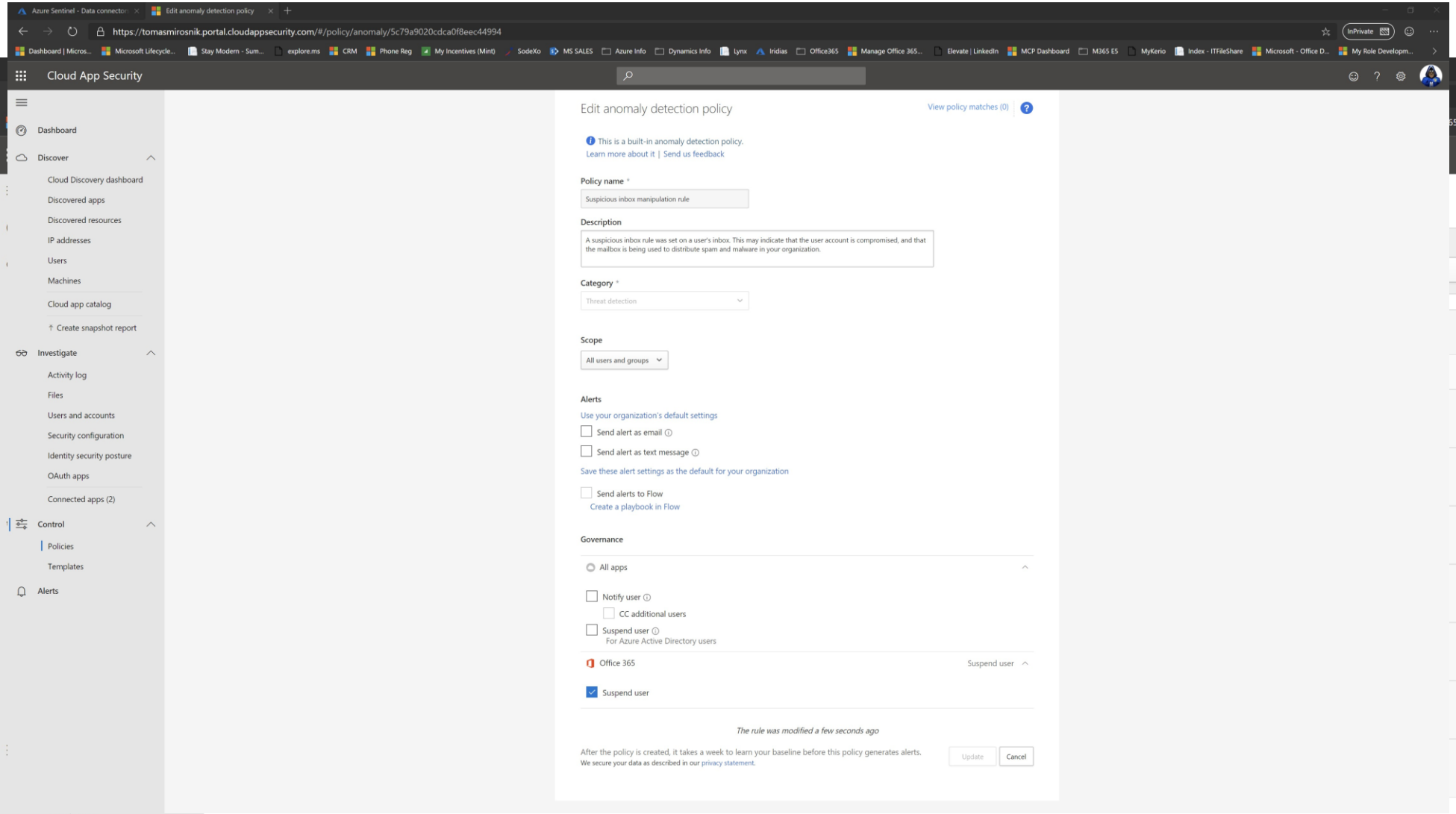


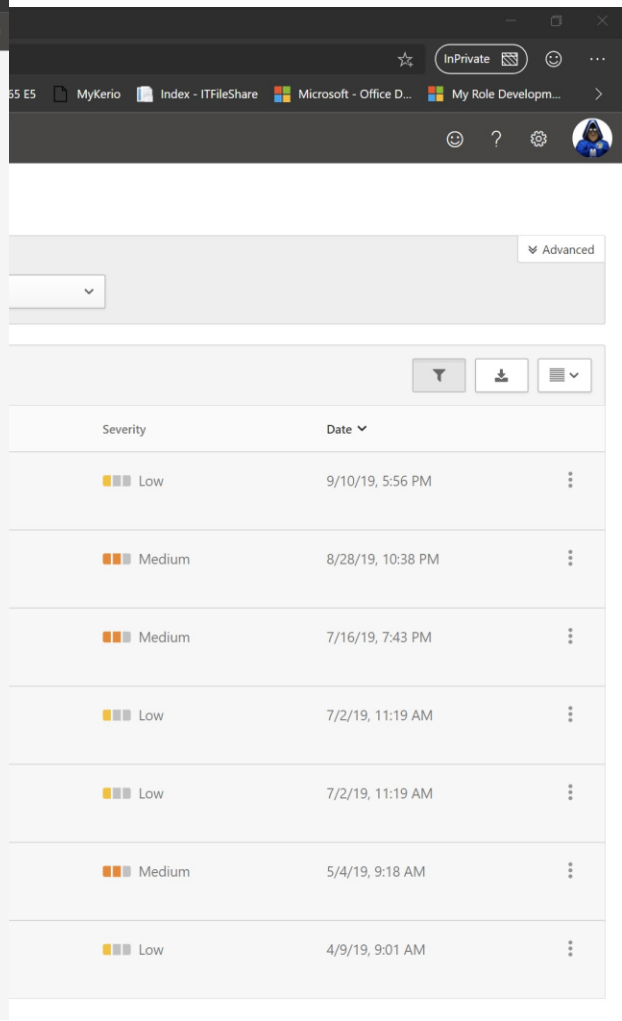


Řízení přístupu

Kontroly neúspěšné manipulace s účty nebo oprávněními

Office 365 Alert Policies, Data Loss Prevention reports and Microsoft Cloud App Security

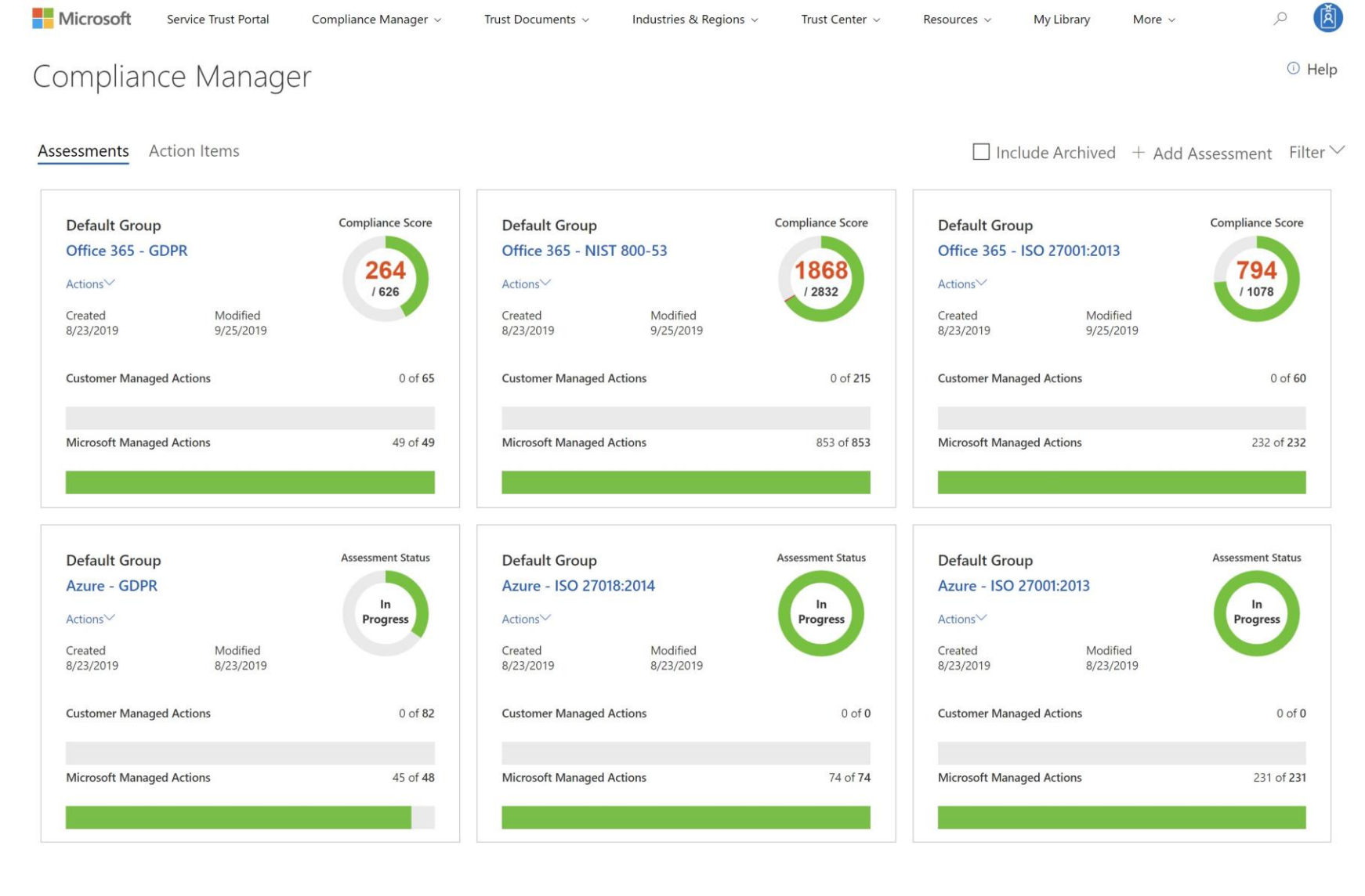




Microsoft Compliance Manager

Microsoft Compliance Manager

Dohled nad stavem zvolených opaření v reálném čase – blog; Main page; 2 min video



More

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
Control ID: 6.11.1 **Control Title:** Securing application services on public networks **Supported GDPR Article(s):** Article (5)(1)(f), Article (32)(1)(a) **Description:** Article (5)(1): Personal data shall be: (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'). Article (32)(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data	8	Implemented	8/31/2018	Third-party independent auditor	✓

More

Controls / Articles	Compliance Score	Status	Test date	Tested By	Test result
Control ID: 6.7 **Control Title:** Cryptography **Supported GDPR Article(s):** Article (32)(1)(a) **Description:** Article (32)(1): Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data	3	Implemented	8/31/2018	Third-party independent auditor	✓

More

Customer Managed Controls

Conditions for collection and processing — 0/7 Assessed

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: 7.2.1 **Control Title:** Identify and document purpose **Supported GDPR Article(s):** Article (5)(1)(b) **Description:** Article (5)(1): Personal data shall be: (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation')	6	No related articles found	TM Manage Documents	Planned	Enter Date	Enter Date	Select

More

Controls / Articles	Compliance Score	Related Controls / Articles	Assigned User	Implementation Status	Implementation Date	Test date	Test result
Control ID: 7.2.2 **Control Title:** Identify lawful basis **Supported GDPR Article(s):** Article (10), Article (17)(3)(a), Article (17)(3)(b), Article (17)(3)(c), Article (17)(3)(d), Article (17)(3)(e), Article (18)(2), Article (22)(2)(a), Article (22)(2)(b), Article (22)(2)(c), Article (5)(1)(a), Article (6)(1)(a), Article (6)(1)(b), Article (6)(1)(c), Article (6)(1)(d), Article (6)(1)(e), Article (6)(1)(f), Article (6)(3), Article (9)(1), Article (9)(2)(b), Article (9)(2)(c), Article (9)(2)(d), Article (9)(2)(e), Article (9)(2)(f), Article (9)(2)(g), Article (9)(2)(h), Article (9)(2)(i), Article (9)(2)(j), Article (9)(3), Article (9)(4) **Description:** Article (10): Processing of personal data relating to criminal convictions and offences or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority. Article (17)(3)(a): Paragraphs 1 and 2 shall not apply to the extent that processing is	6	GDPR: 7.2.3, 7.3.1, 7.3.4, 7.3.5, 7.3.7, 7.3.8	Assign Manage Documents	Select	Enter Date	Enter Date	Select

Závěrem

- Řízení přístupů, provozu a komunikace je pomocí cloudových nástrojů mnohem agilnější a poskytuje větší možnosti, zejména s ohledem na analýzu pomocí AI
- Nasazení cloudových prostředků dohledu a ochrany je rychlejší a pružnější

Microsoft

Děkujeme za pozornost!