



# Martin Haller





## 《Microsoft Entra ID RBAC: The Shady Place Behind Basic Entra ID Security》







# Entra ID: Why Bother?

- »  **Systemic Importance:** As a Tier 0 service (Identity Provider), compromising Entra ID puts the entire system at risk.
- »  **Cloud Accessibility:** Entra ID's cloud service is globally accessible, introducing unique security challenges.
- »  **Market Penetration:** Its widespread adoption makes it nearly universal, indicating a significant reliance across companies.
- »  **Evolving Practices:** The technology's novelty and complexity mean that best practices are still forming, leading to a higher chance of misconfigurations.



# Microsoft Entra ID: Gateway to Supply Chain Attacks on a Global Scale

DISOBEY

## Perceptions from Ransomware Incident Response

- « Critical step is „Lateral movement“
- « Attackers know Active Directory better than defenders.



Source: <https://www.youtube.com/watch?v=QF6HOA7oqnk>

PATRÓN-IT s.r.l. | Microsoft Entra ID: Gateway to Supply Chain Attacks on a Global Scale

Martin Haller  
Microsoft Entra ID: Gateway to Supply Chain Attacks on a Global Scale

Source: <https://www.youtube.com/watch?v=QF6HOA7oqnk>



# Where We Stand - Defenders

## » Plenty of materials

- » Entra.News (<https://entra.news>)
- » Talks
- » Research

## » Auditing Tools

- » ScubaGear (<https://github.com/cisagov/ScubaGear>)
- » Maester (<https://maester.dev/>)
- » BloodHound (<https://github.com/SpecterOps/BloodHound>)
- » PingCastle (<https://www.pingcastle.com/>)
- » PurpleKnight (<https://www.semperis.com/purple-knight/>)

# Where We Stand - Attackers

## » APTs

- » Antique Typhoon (Storm-0558) – stole an inactive MSA consumer signing key and used it to forge authentication tokens for Azure AD enterprise and MSA consumer to access OWA and Outlook.com
- » Storm-1084 – pivot from AD to Entra ID through Azure AD connect, mail exfiltration, mass Azure resource deletion
- » Midnight Blizzard (Nobelium) – Golden SAML, AD FS backdoor MagicWeb, DAP misuse, Enterprise Apps misuse

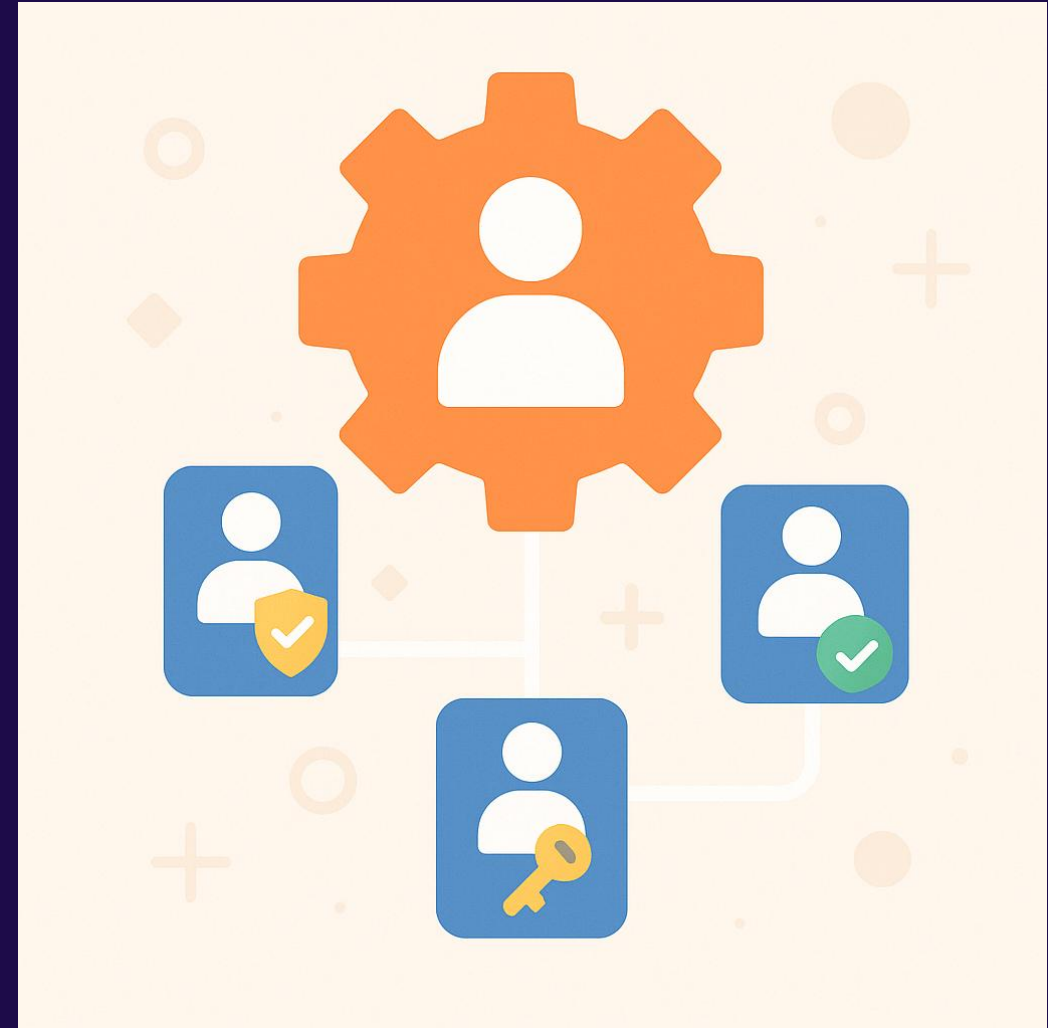
## » Regular threat actors

- » Need a business model
- » From cookie theft to BEC - Attackers use AiTM phishing sites as entry point to further financial fraud
- » The Legacy Loophole - How Attackers Are Exploiting Entra ID and What to Do About It

# Where We Stand – My point of view

- »  I see future in attacks against Entra ID
- »  Defenders are hardening
  - » MFA
  - » Conditional Access Policies
  - » Auditing tools
  - » Logging
- »  With the basics covered, attackers will be forced to adjust

# RBAC: Role-Based Access Control





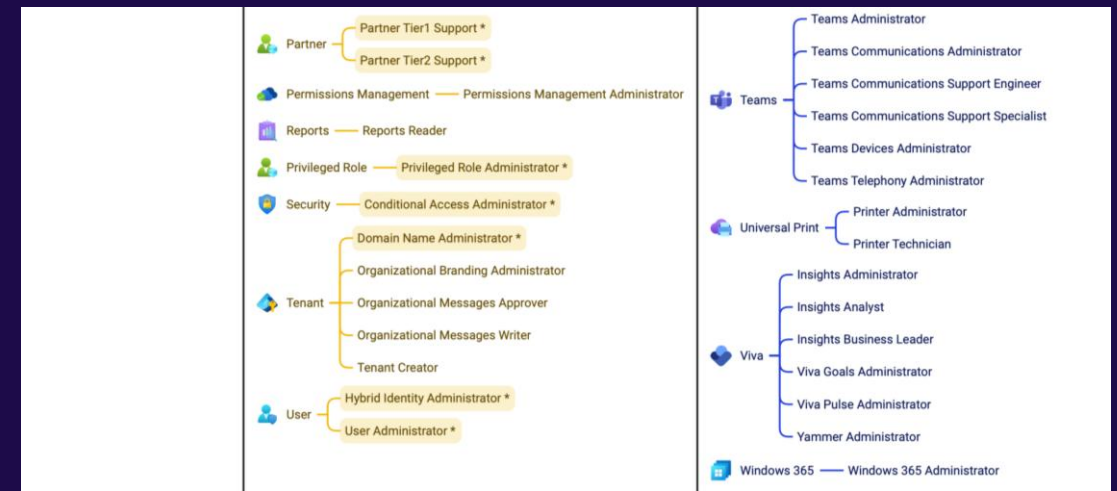
„RBAC is a method of enforcing access controls by assigning users to predefined roles, and associating each role with specific permissions or privileges.“

# Entra ID – RBAC – Single pane of glass

The screenshot displays the Microsoft Entra admin center interface. The left navigation pane shows the 'Users' section selected. The main content area shows the 'Assigned roles' for the user 'Admin MH'. The table below lists the assigned roles:

Role	Principal name	Scope	Membership	State	Start time
Global Administrator	[redacted]@patron-i...	Directory	Direct	Active	-

# Entra ID – RBAC - Admin Roles

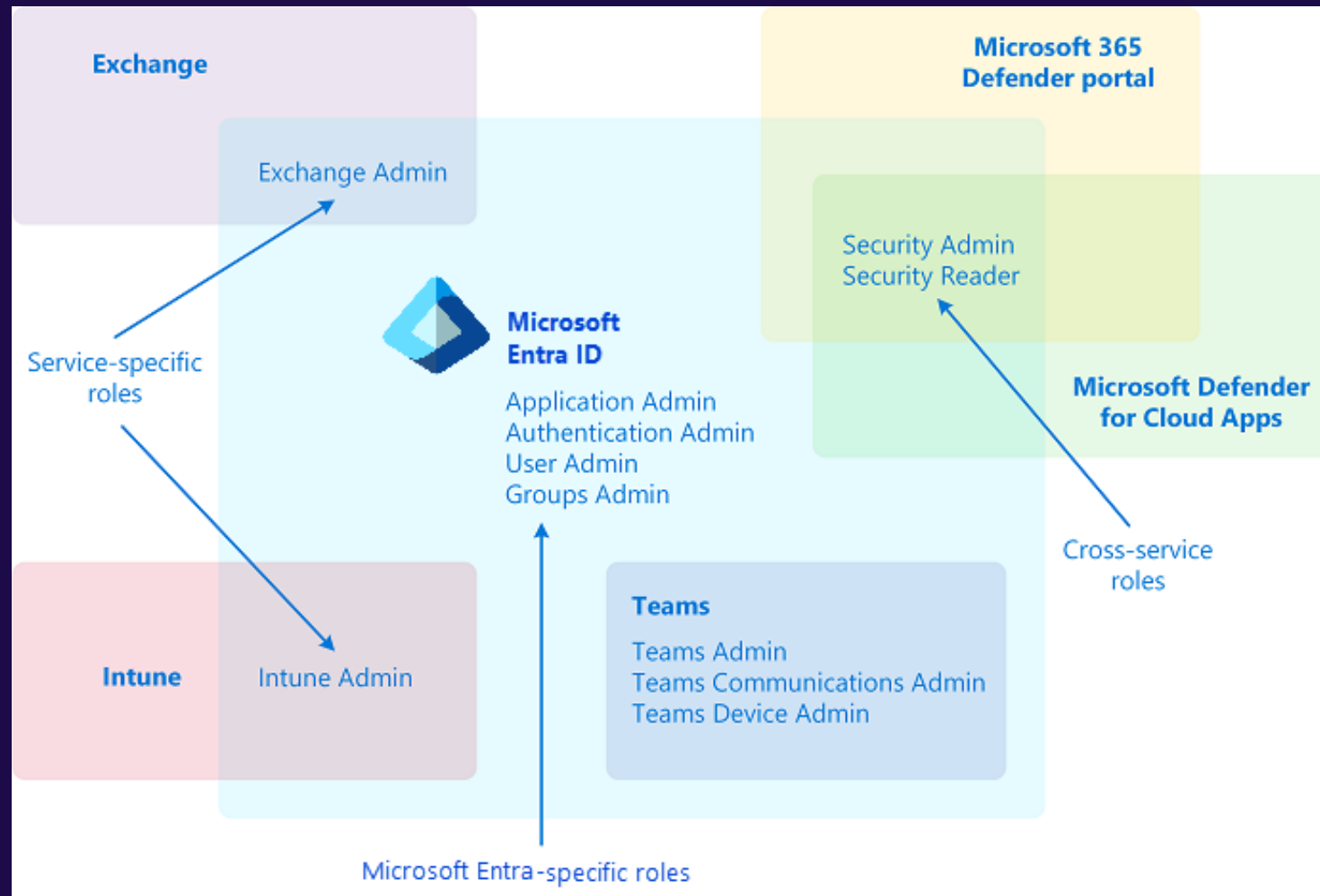


Source: <https://entra.news/p/entra-mind-maps>





# Entra ID – RBAC – The reality



# Entra ID – RBAC – Auditing tools

- » ScubaGear (<https://github.com/cisagov/ScubaGear>)
- » Maester (<https://maester.dev/>)
- » BloodHound (<https://github.com/SpecterOps/BloodHound>)
- » PingCastle (<https://www.pingcastle.com/>)
- » PurpleKnight (<https://www.semperis.com/purple-knight/>)

😬 APP SPECIFIC RBAC ISN'T COVERED 😬

# RBAC: Exchange





# RBAC: Exchange

- » The most problematic in audits
- » Often breaks tiering model

Exchange admin center

Copy role group Delete

Role group ↑	Description
Privacy Management Administrators	Manage access control for Privacy Management Center.
Privacy Management Investigators	Analysts of privacy management solution that ca meta data, and take remediation actions.
<input checked="" type="checkbox"/> Recipient Management	Members of this management role group have r Exchange recipient objects in the Exchange orga
Records Management	Members of this management role group have p content.
RIM-MailboxAdmins5dab333c7e6a4a96ba2ca866a5e299f1	
Security Administrator	Membership in this role group is synchronized a role group is not manageable through the admin may include cross-service administrators, as well Support. By default, this group may not be assign the Security Administrators role groups and will i
Security Operator	Membership in this role group is synchronized a role group is not manageable through Microsoft (SCC). Members of this role group may include c beyond Exchange and SCC. By default, this group a member of the 'Records Management' and 'Co Exchange and 'Compliance Data Administrator' n permissions of these role groups.
Security Reader	Membership in this role group is synchronized a role group is not manageable through the admin may include cross-service administrators, as well Support. By default, this group may not be assign the Security Reader role groups and will inherit t
SecurityReaders_421168135	Membership in this role group is synchronized a role group is not manageable through Microsoft Center(UCC). By default, this group is not assigne

Recipient Management

General **Assigned** Permissions

These are the admins assigned to this role. You can add or remove admins from this role group here.

+ Add 1 item Search

Admin name	Type
Robert Malina	UserMailbox

# RBAC: Exchange

## » Misconfigurations lead to:

- » **Lateral movement / privilege escalation:** access to other mailboxes, contacts, calendars, internal phishing
- » **Security alteration:** audit log weakening
- » **Data exfiltration / BEC / ransom:** forwarding rules, full access permission to mailbox

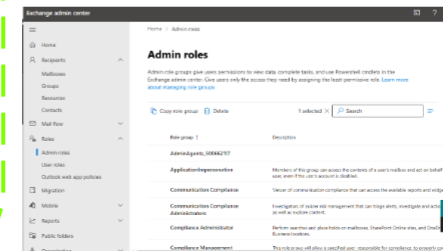
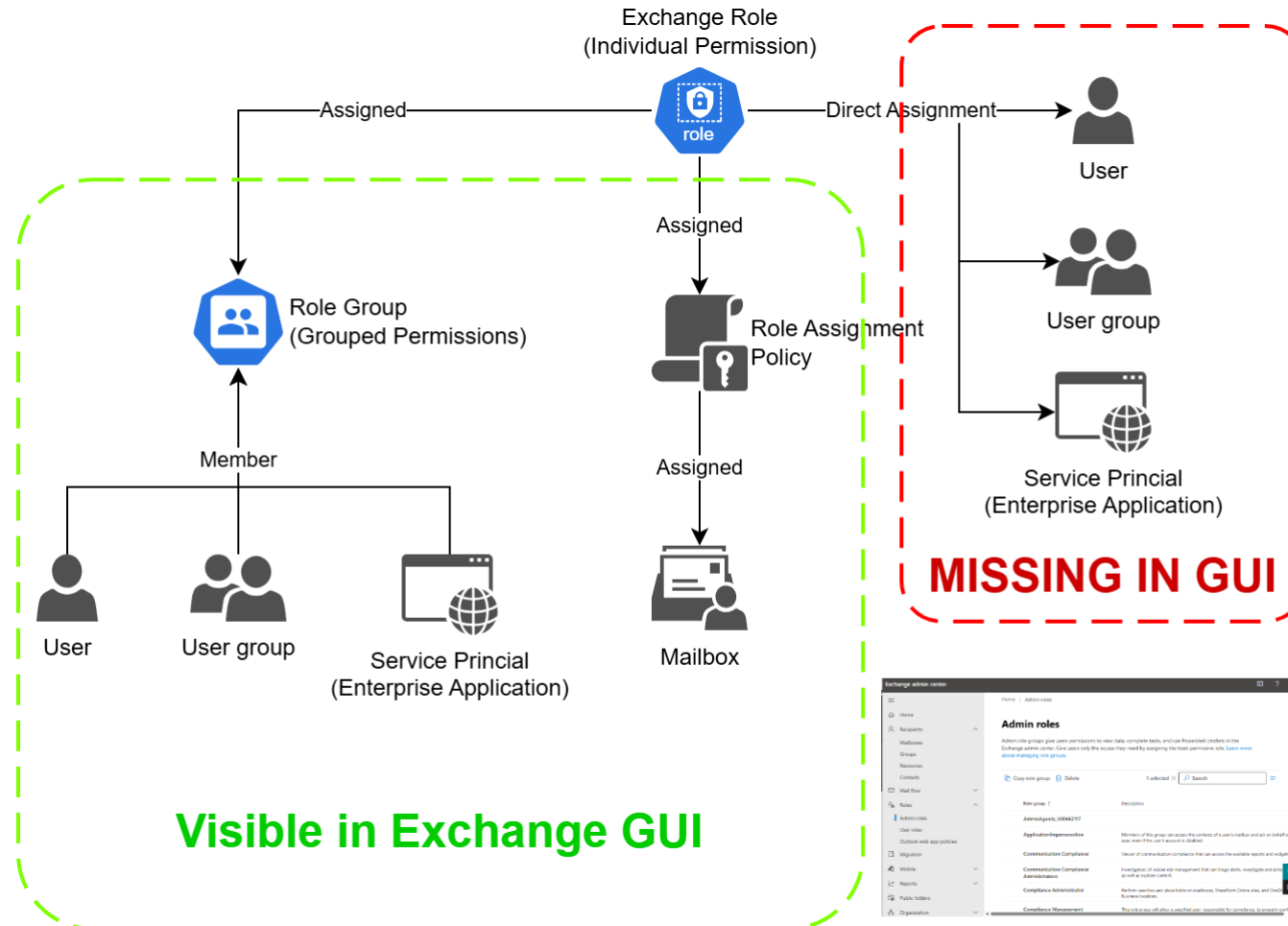
## » Privileged persistence

# RBAC: Exchange – DEMO Priv. Escalation





# RBAC: Exchange – Assignment possibilities

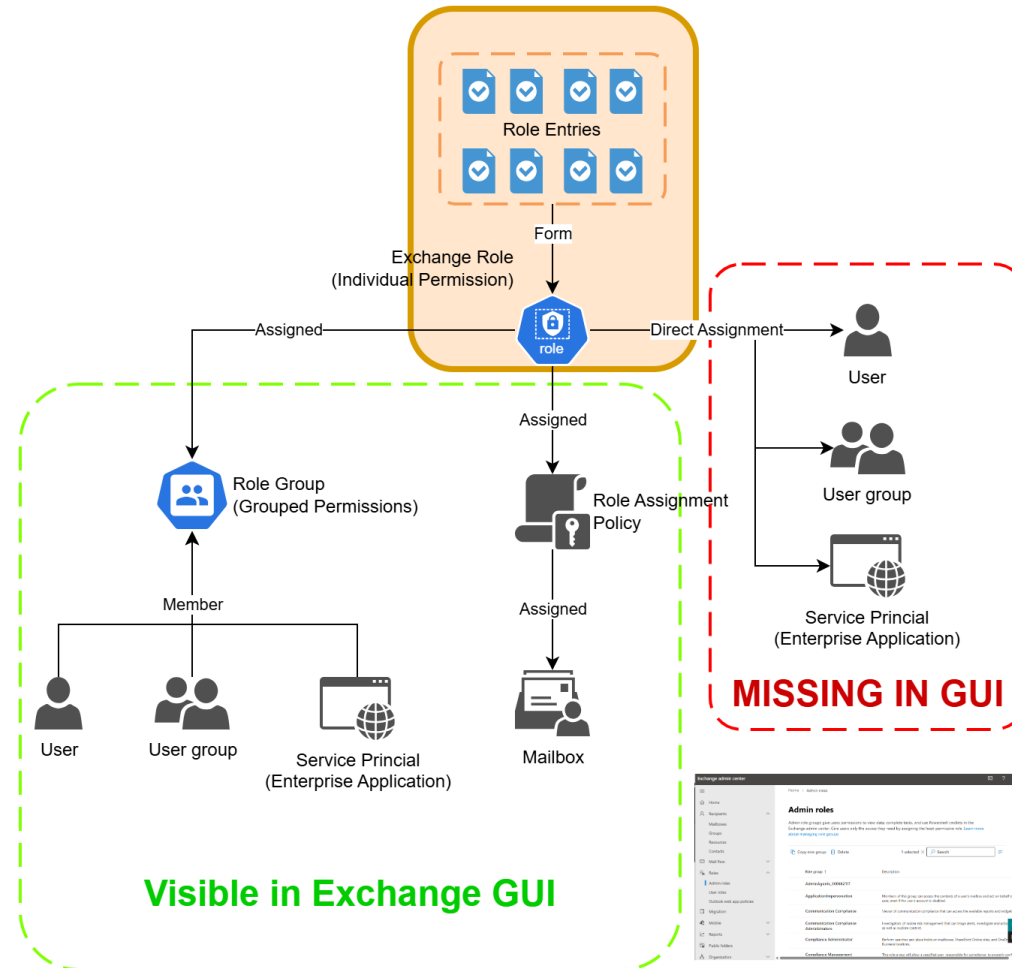


# RBAC: Exchange – DEMO Persistence

The screenshot displays the Microsoft Entra admin center interface. The left-hand navigation pane shows the 'Users' section with 'All users' selected. The main content area displays a list of 11 users. The table below represents the data shown in the interface.

	Display name	User principal name	User type	On-premises sync	Identities	Company name	Creation type
<input type="checkbox"/>	Adam Jensen	adam.jensen@mhlab.cz	Member	No	mhlabcz.onmicrosoft.com		
<input type="checkbox"/>	Chloe Richards	chloe.richards@mhlab.cz	Member	No	mhlabcz.onmicrosoft.com		
<input type="checkbox"/>	Daniel Webb	daniel.webb@mhlab.cz	Member	No	mhlabcz.onmicrosoft.com		
<input type="checkbox"/>	Emily Foster	emily.foster@mhlab.cz	Member	No	mhlabcz.onmicrosoft.com		
<input type="checkbox"/>	Ethan Harris	ethan.harris@mhlab.cz	Member	No	mhlabcz.onmicrosoft.com		
<input type="checkbox"/>	Grace Simmons	grace.simmons@mhlab.cz	Member	No	mhlabcz.onmicrosoft.com		
<input type="checkbox"/>	Lily Collins	lily.collins@mhlab.cz	Member	No	mhlabcz.onmicrosoft.com		
<input type="checkbox"/>	Lucas Bennett	lucas.bennett@mhlab.cz	Member	No	mhlabcz.onmicrosoft.com		
<input type="checkbox"/>	Martin Haller	adm-mh@mhlabcz.onmic...	Member	No	mhlabcz.onmicrosoft.com		
<input type="checkbox"/>	Noah Carter	noah.carter@mhlab.cz	Member	No	mhlabcz.onmicrosoft.com		
<input type="checkbox"/>	Olivia Turner	olivia.turner@mhlab.cz	Member	No	mhlabcz.onmicrosoft.com		

# RBAC: Exchange – Role isn't atomic



# RBAC: Exchange – DEMO Persistence (v2)



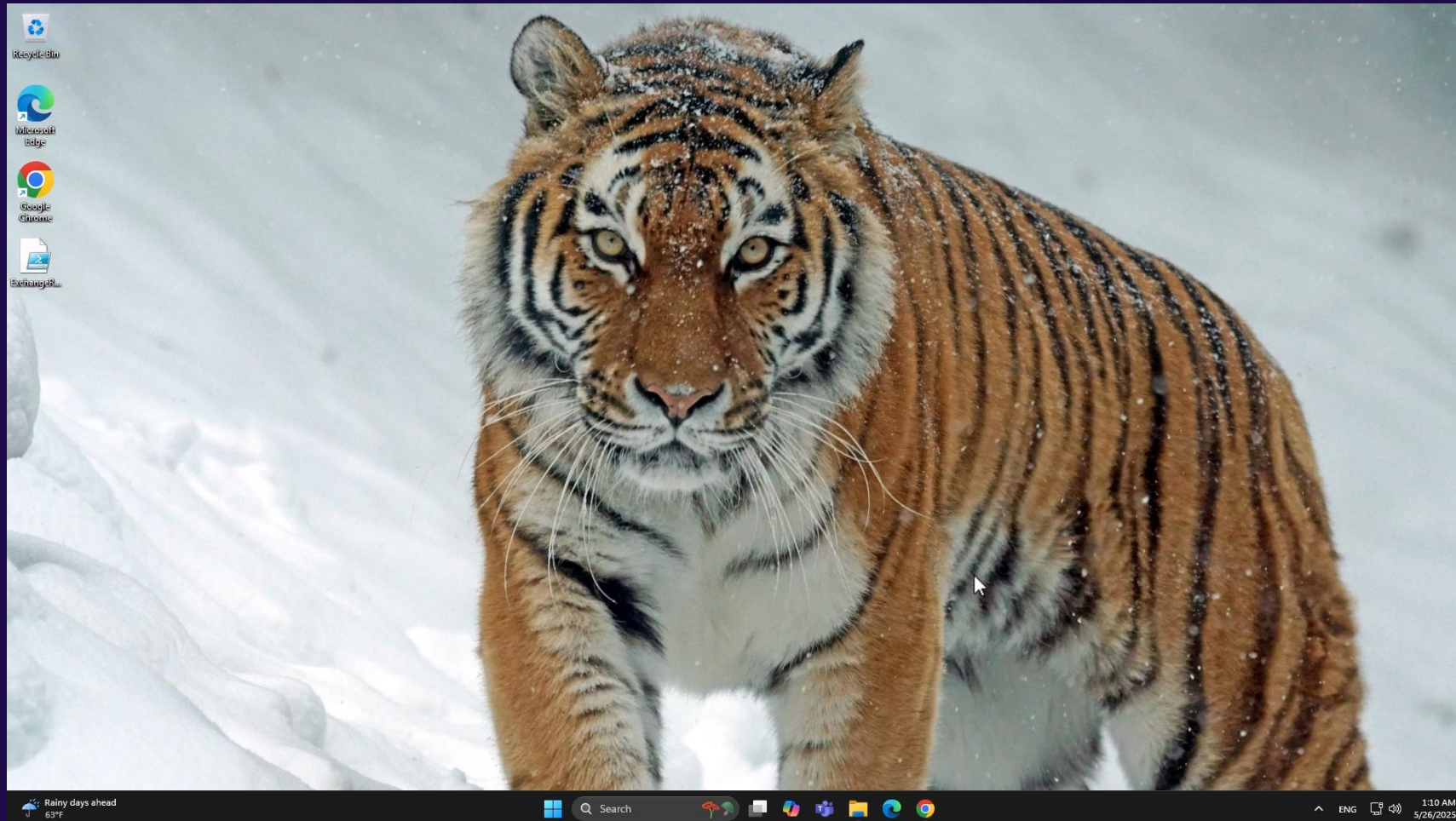


# RBAC: Exchange – Supported Application Roles

Name	Protocol	Permissions List	Description
Application Mail.Read	MS Graph	Mail.Read	Allows the app to read email in all mailboxes without a signed-in user.
Application Mail.ReadBasic	MS Graph	Mail.ReadBasic	Allows the app to read email except the body, previewBody, attachments, and any extended properties in all mailboxes without a signed-in user.
Application Mail.ReadWrite	MS Graph	Mail.ReadWrite	Allows the app to create, read, update, and delete email in all mailboxes without a signed-in user. Doesn't include permission to send mail.
Application Mail.Send	MS Graph	Mail.Send	Allows the app to send mail as any user without a signed-in user.
Application MailboxSettings.Read	MS Graph	MailboxSettings.Read	Allows the app to read user's mailbox settings in all mailboxes without a signed-in user.
Application MailboxSettings.ReadWrite	MS Graph	MailboxSettings.ReadWrite	Allows the app to create, read, update, and delete user's mailbox settings in all mailboxes without a signed-in user.
Application Calendars.Read	MS Graph	Calendars.Read	Allows the app to read events of all calendars without a signed-in user.
Application Calendars.ReadWrite	MS Graph	Calendars.ReadWrite	Allows the app to create, read, update, and delete events of all calendars without a signed-in user.
Application Contacts.Read	MS Graph	Contacts.Read	Allows the app to read all contacts in all mailboxes without a signed-in user.
Application Contacts.ReadWrite	MS Graph	Contacts.ReadWrite	Allows the app to create, read, update, and delete all contacts in all mailboxes without a signed-in user.
Application Mail Full Access	MS Graph	Mail.ReadWrite, Mail.Send	Allows the app to create, read, update, and delete email in all mailboxes and send mail as any user without a signed-in user.
Application Exchange Full Access	MS Graph	Mail.ReadWrite, Mail.Send, MailboxSettings.ReadWrite, Calendars.ReadWrite, Contacts.ReadWrite	Without a signed-in user: Allows the app to create, read, update, and delete email in all mailboxes and send mail as any user. Allows the app to create, read, update, and delete user's mailbox settings in all mailboxes. Allows the app to create, read, update, and delete events of all calendars. Allows the app to create, read, update, and delete all contacts in all mailboxes.
Application EWS.AccessAsApp	EWS	EWS.AccessAsApp	Allows the app to use Exchange Web Services with full access to all mailboxes.

Source: <https://learn.microsoft.com/en-us/exchange/permissions-exo/application-rbac#supported-application-roles>

# RBAC: Exchange – DEMO Persistence (v3)



# RBAC: Exchange - Seen in the Wild

## The Evolution of Business Email Compromise

May 7, 2023

### Introduction

Over the past months, we have provided support to multiple organizations that have fallen victim to Business Email Compromise (BEC) attacks. In this blog we would like to share some of the latest Tactics, Techniques & Procedures (TTPs) we observed during a specific BEC investigation in a Microsoft 365 environment. We hope that this information will be helpful to other incident responders and organizations working on similar cases.

Source: <https://www.invictus-ir.com/news/the-evolution-of-business-email-compromise>

# RBAC: Azure



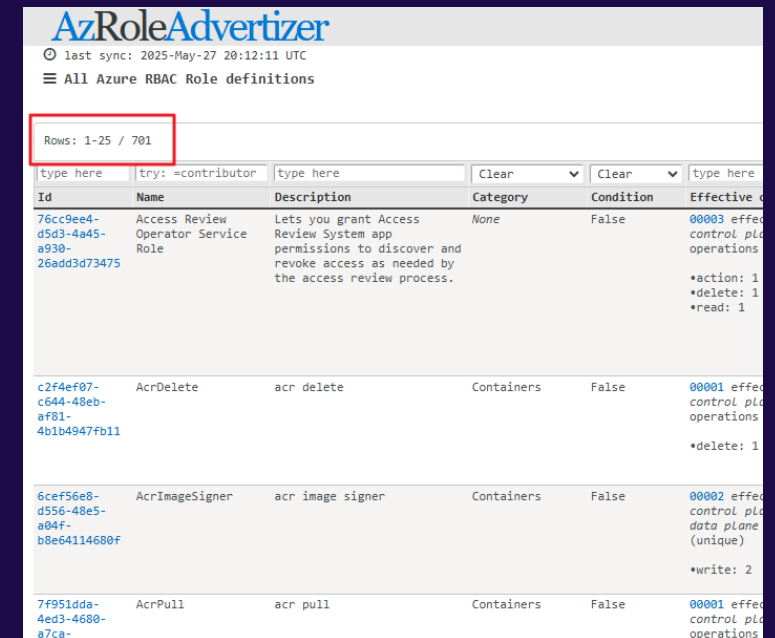


# RBAC: Azure

## » Misconfigurations lead to:

- » **Lateral movement / privilege escalation:** VM control, Azure Key Vault, Azure Managed Identity
- » **Security alteration:** log analytics retention period
- » **Data exfiltration / ransom:** exfiltration data from DB/storage

## » Privileged persistence



AzRoleAdvertiser

last sync: 2025-May-27 20:12:11 UTC

All Azure RBAC Role definitions

Rows: 1-25 / 701

Id	Name	Description	Category	Condition	Effective permissions
76cc9ee4-d5d3-4a45-a930-26add3d73475	Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover and revoke access as needed by the access review process.	None	False	00003 effected control plane operations *action: 1 *delete: 1 *read: 1
c2f4ef07-c644-48eb-af81-4b1b4947fb11	AcrDelete	acr delete	Containers	False	00001 effected control plane operations *delete: 1
6cef56e8-d556-48e5-a04f-b8e64114680f	AcrImageSigner	acr image signer	Containers	False	00002 effected control plane data plane (unique) *write: 2
7f951dda-4ed3-4680-a7ca-	AcrPull	acr pull	Containers	False	00001 effected control plane operations

Source: [https://www.azadvertizer.net/azrolesadvertizer\\_all.html](https://www.azadvertizer.net/azrolesadvertizer_all.html)

# RBAC: Azure – Default Owner Privs for Partner

Check access **Role assignments** Roles Deny assignments Classic administrators

Number of role assignments for this subscription ⓘ  
20 4000






Privileged ⓘ  
16

[View assignments](#)

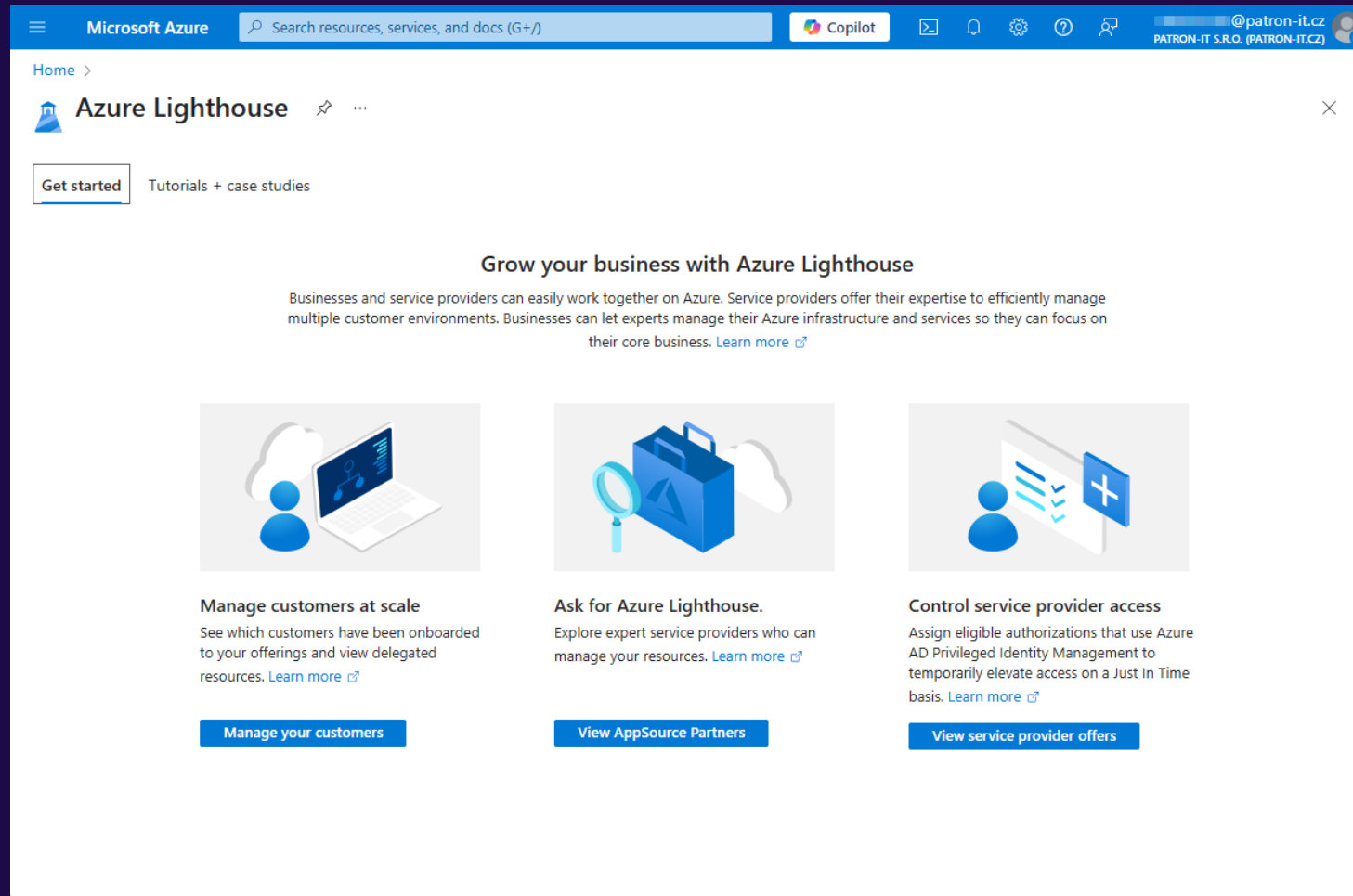
Search by name or email

Type : All Role : All Scope : All scopes State : All End time : All Group by : Role

All (29) Job function roles (13) Privileged administrator roles (16)

Name ↑↓	Type ↑↓	Role ↑↓	Scope ↑↓	State ↑↓	End time ↑↓	Condition ↑↓
▼ Owner (5)						
 [redacted]	User	Owner	🔑 This resource	Active Permanent	Permanent	None
 [redacted]	User	Owner	📦 Management group (Inhe...	Active Permanent	Permanent	None
 Foreign Principal for 'Arrow ECS, a.s.' in Role 'TenantAdmi... 568ac7f3-c2eb-4490-bb44-08f03d343ae2	Foreign group	Owner	🔑 This resource	Active Permanent	Permanent	None
 [redacted]	Service principal	Owner	📦 Management group (Inhe...	Active Permanent	Permanent	None
 [redacted]	User	Owner	🔑 This resource	Active Permanent	Permanent	None

# RBAC: Azure - Lighthouse



The screenshot displays the Microsoft Azure Lighthouse portal. At the top, the navigation bar includes the 'Microsoft Azure' logo, a search bar, and icons for Copilot, mail, notifications, settings, help, and a user profile. The user profile is identified as '@patron-it.cz' and 'PATRON-IT S.R.O. (PATRON-IT.CZ)'. Below the navigation bar, the 'Home' link is followed by the 'Azure Lighthouse' title and a close button. A 'Get started' button is linked to 'Tutorials + case studies'. The main content area is titled 'Grow your business with Azure Lighthouse' and includes a descriptive paragraph about how businesses and service providers can collaborate on Azure. Below this, three key features are highlighted with icons and buttons: 'Manage customers at scale' (with a laptop icon), 'Ask for Azure Lighthouse' (with a magnifying glass and briefcase icon), and 'Control service provider access' (with a person and plus sign icon). Each feature has a brief description and a 'Learn more' link.

Microsoft Azure Search resources, services, and docs (G+)

Copilot


@patron-it.cz PATRON-IT S.R.O. (PATRON-IT.CZ)

Home > Azure Lighthouse

Get started Tutorials + case studies


### Grow your business with Azure Lighthouse

Businesses and service providers can easily work together on Azure. Service providers offer their expertise to efficiently manage multiple customer environments. Businesses can let experts manage their Azure infrastructure and services so they can focus on their core business. [Learn more](#)




**Manage customers at scale**  
See which customers have been onboarded to your offerings and view delegated resources. [Learn more](#)

Manage your customers



**Ask for Azure Lighthouse.**  
Explore expert service providers who can manage your resources. [Learn more](#)

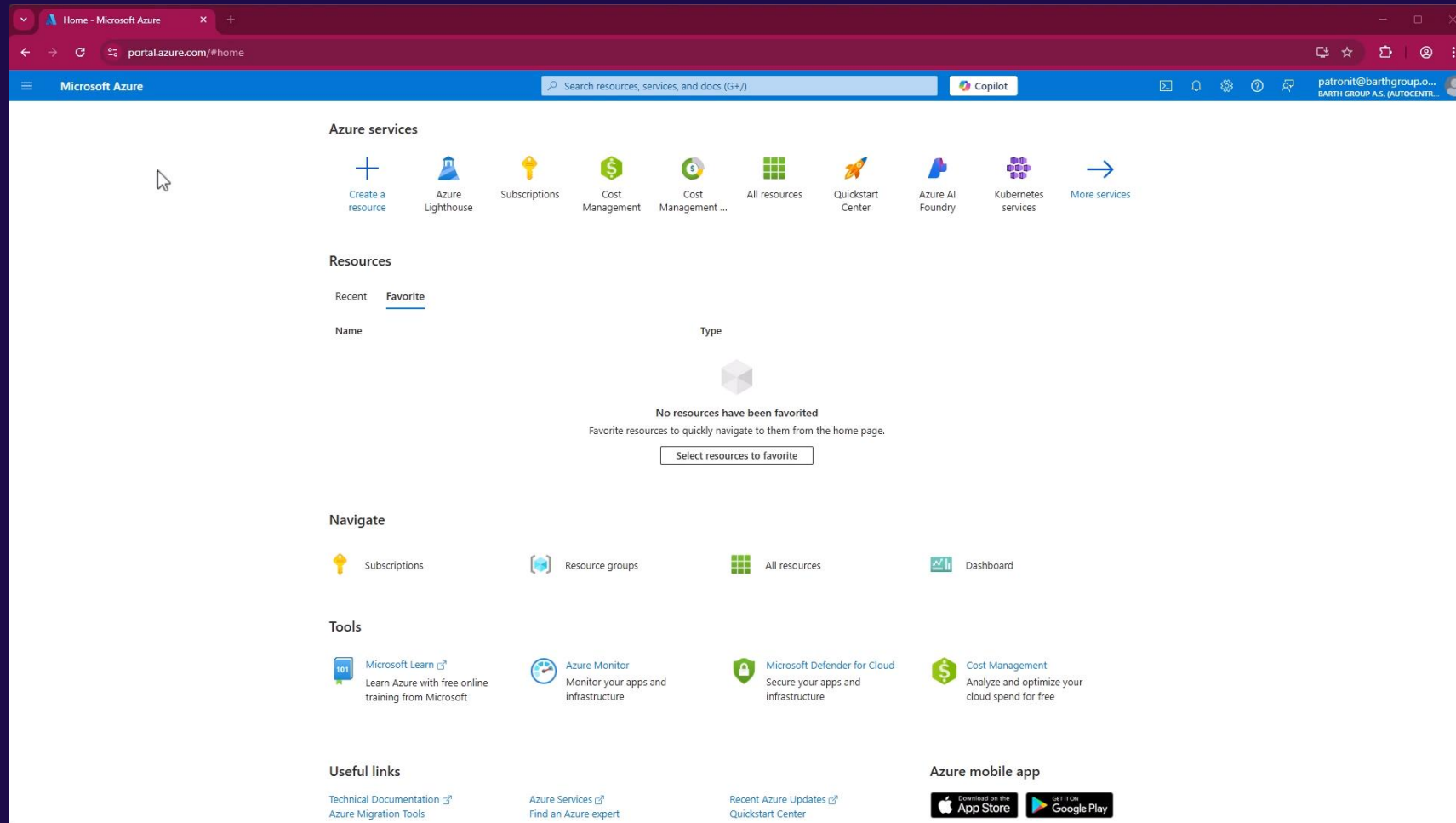
View AppSource Partners



**Control service provider access**  
Assign eligible authorizations that use Azure AD Privileged Identity Management to temporarily elevate access on a Just In Time basis. [Learn more](#)

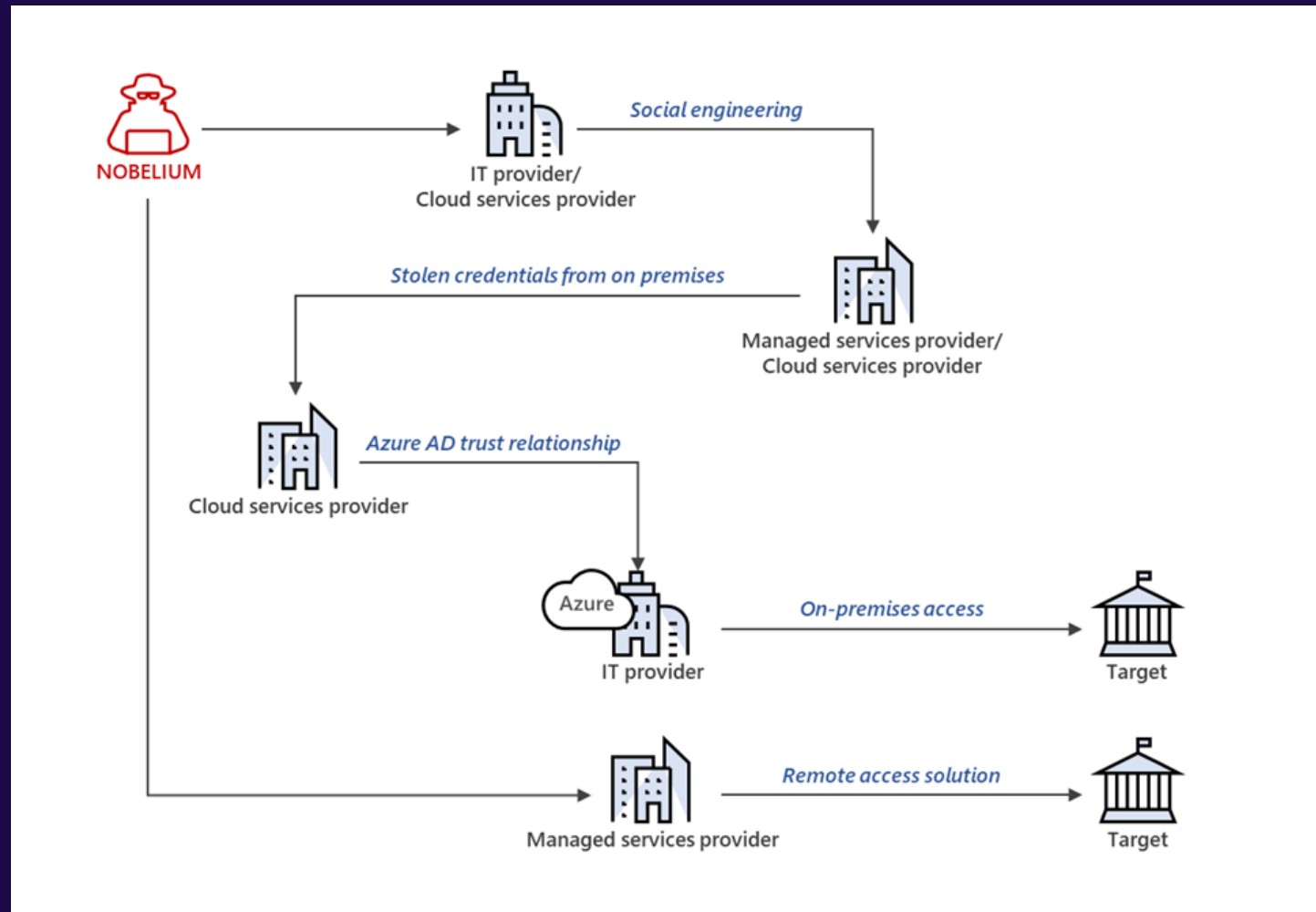
View service provider offers

# RBAC: Azure – DEMO Persistence





# RBAC: Azure - Seen in the Wild



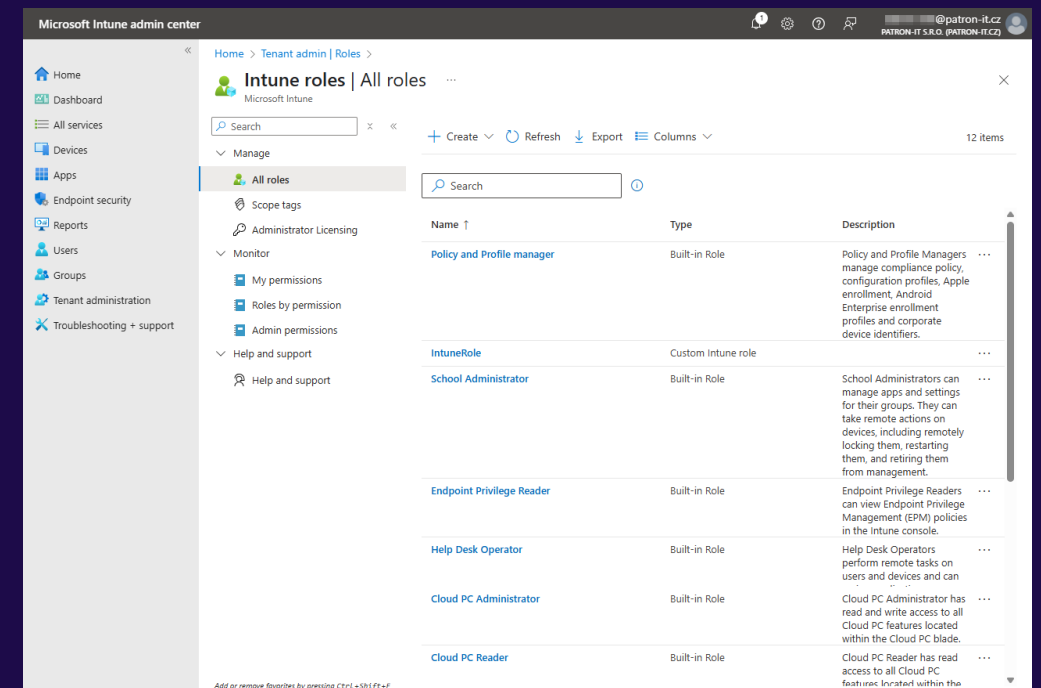
Source: <https://www.microsoft.com/en-us/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/>

# RBAC: Intune

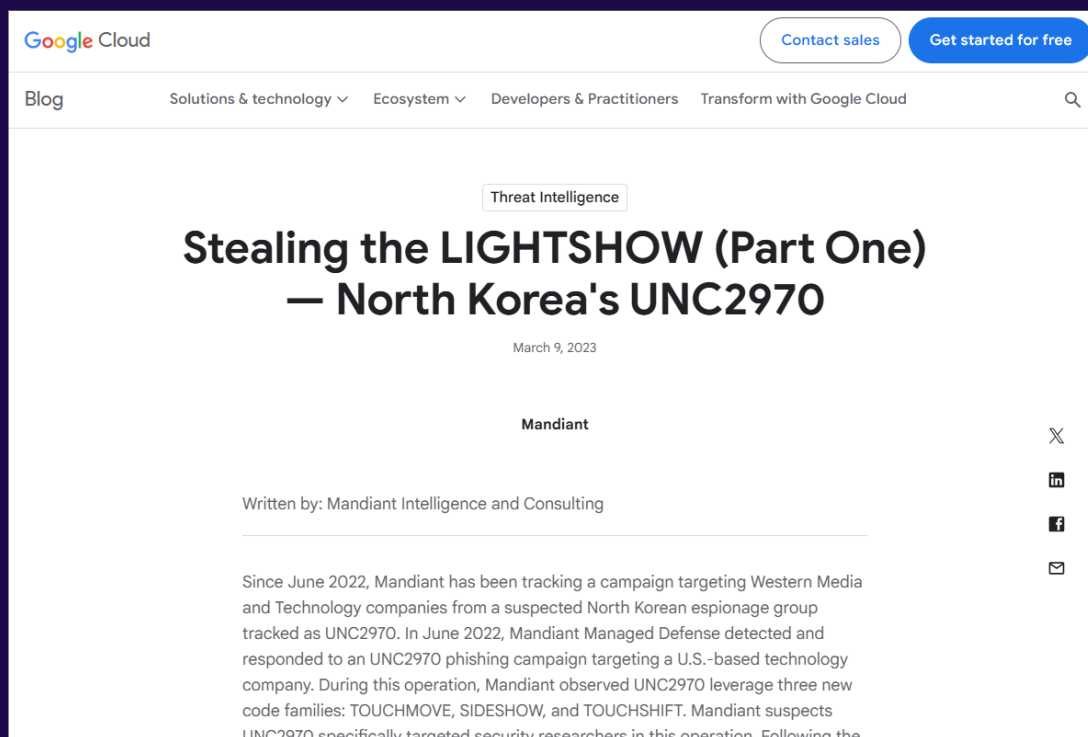


# RBAC: Intune

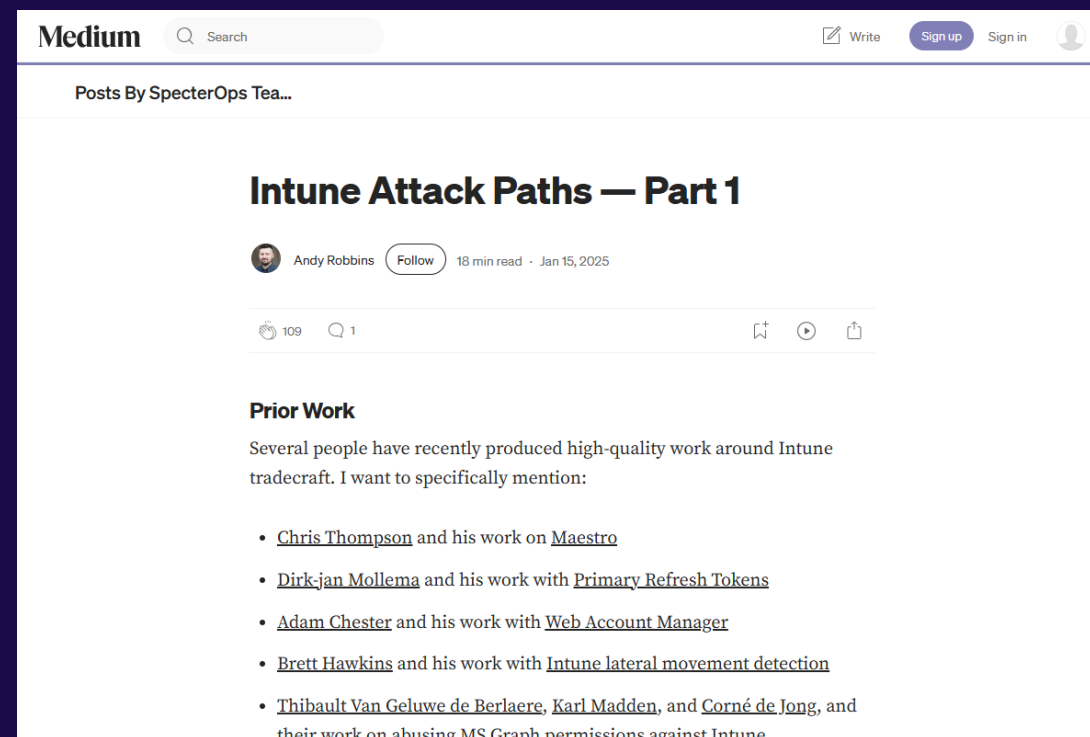
- » Frequently breaks tiering
- » Misconfigurations lead to:
  - » **Lateral movement / privilege escalation:** application deployment, remediations and scripts
  - » **Unauthorized Data Access:** application deployment, remediations and scripts
  - » **Mobile device compromise:** app deployment, custom CA+VPN
  - » **Security alteration:** disable endpoint protection
  - » **Ransomware / DoS**
- » Privileged persistence



# RBAC: Intune - Seen in the Wild



Source: <https://cloud.google.com/blog/topics/threat-intelligence/lightshow-north-korea-unc2970>



Source: <https://posts.specterops.io/intune-attack-paths-part-1-4ad1882c1811>



# RBAC: Microsoft Defender



# RBAC: Defender

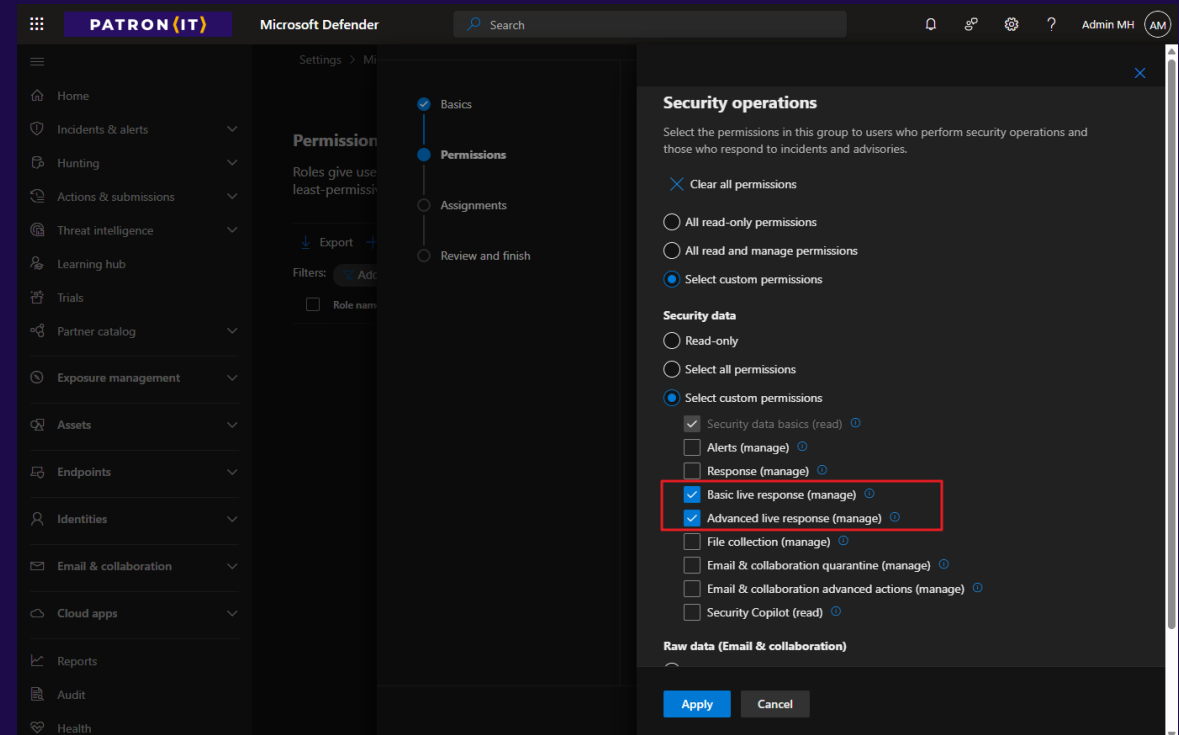
The screenshot shows the Microsoft Defender XDR 'Permissions' page. The left sidebar contains a navigation menu with items like Trials, Partner catalog, Exposure management, Overview, Attack surface, Exposure insights, Secure score, Data connectors, Assets, Devices, Identities, Applications, Endpoints, Vulnerability management, Partners and APIs, Configuration management, Identities, and Dashboard. The main content area is titled 'Permissions' and includes a sub-header 'Try the Microsoft Defender XDR permission model and get more granular control.' Below this, there's a table with columns 'Name' and 'Description'. The table lists several roles and groups, including 'Microsoft Defender XDR (1)', 'Microsoft Entra ID (1)', 'Endpoints roles & groups (2)', 'Cloud Apps (2)', and 'Activity Privacy Permissions'. Each entry has a 'Roles' section with a description of the permissions.

Name	Description
Microsoft Defender XDR (1)	Manage who has access to view tasks and take actions in Microsoft Defender XDR. Assign only the minimum permissions that admins need to get the job done.
Microsoft Entra ID (1)	Manage who has access to view tasks and take actions in the Microsoft Defender portal. Assign them only the permissions needed to perform their duties.
Endpoints roles & groups (2)	Manage endpoint access to view content and perform tasks. Grant only the permissions needed for users to perform their tasks.
Cloud Apps (2)	Manage who has access to view cloud apps content and take actions. Assign them only the permissions needed to perform their duties.
Activity Privacy Permissions	Control which admins can reveal private activities.


The screenshot shows the Microsoft Defender XDR 'Settings' page. The top navigation bar includes 'Settings > Microsoft Defender XDR'. The main content area is titled 'Microsoft Defender XDR'. On the left, there's a sidebar with sections: General (Account, Session details, Email notifications, Preview features, Alert service settings), Rules (Asset rule management, Alert tuning, Critical asset management, Service accounts classification), and Automated response (Identities, Devices). The 'Permissions and roles' section is highlighted with a red box. On the right, there's a 'Workloads' section with sub-sections: 'Endpoints & Vulnerability Management' (Active), 'Email & Collaboration' (Active - Defender for Office 365, Active - Exchange Online permissions), and 'Cloud Apps' (Active). A link 'Go to Permissions and roles' is at the bottom.

# RBAC: Defender

- » Frequently breaks tiering
- » Misconfigurations lead to:
  - » **Lateral movement / privilege escalation:** live response custom scripts
  - » **Unauthorized Data Access:** live response data download
  - » **Security alteration:** alert suppression
- » Privileged persistence



# RBAC: Defender - Seen in the Wild

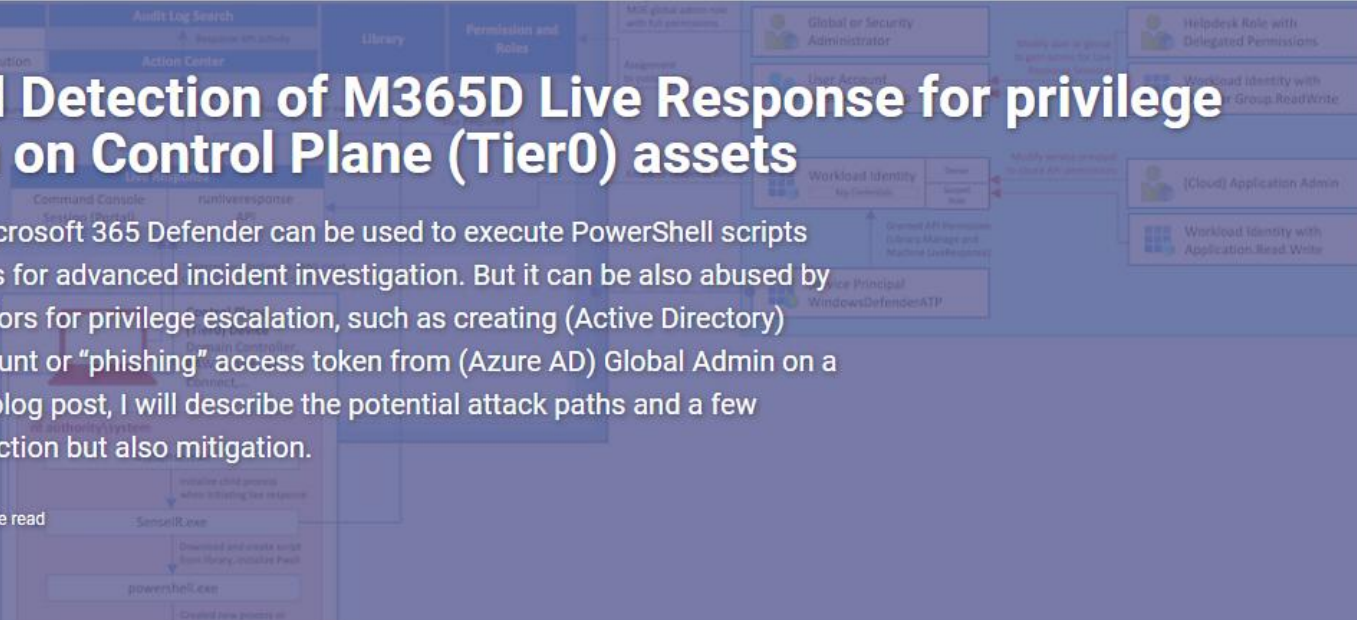
 Thomas Naunheim

AboutBlogCategoriesEntraOpsSpeakingPublicationsLinksDisclosurePrivacy

## Abuse and Detection of M365D Live Response for privilege escalation on Control Plane (Tier0) assets

Live Response in Microsoft 365 Defender can be used to execute PowerShell scripts on protected devices for advanced incident investigation. But it can be also abused by Security Administrators for privilege escalation, such as creating (Active Directory) Domain Admin account or “phishing” access token from (Azure AD) Global Admin on a PAW device. In this blog post, I will describe the potential attack paths and a few approaches for detection but also mitigation.

📅 March 20, 2023 • ⌚ 12 minute read



### Abuse and Detection of M365D Live Response for privilege escalation on Control Plane (Tier0) assets

#### What is Live Response?

#### On this page

- Abuse and Detection of M365D Live Response for privilege escalation on Control Plane (Tier0) assets
- What is Live Response?

Source: <https://www.cloud-architekt.net/abuse-detection-live-response-tier0/>

# RBAC: Purview



## Microsoft Purview



# RBAC: Purview

- » Misconfigurations lead to:
  - » Unauthorized Data Access
  - » Privileged persistence

**Microsoft Purview**

Search

Settings

Account

Roles and scopes

Microsoft Entra ID

Role groups

Compliance Administrator

Organization Management

Purview Administrators

Attack Simulator Administrators

Attack Simulator Payload Auth...

Security Administrator

Audit Manager

Billing Administrator

eDiscovery Manager

Insider Risk Management

Insider Risk Management Adm...

Insider Risk Management Anal...

Insider Risk Management Inve...

Communication Compliance L...

Communication Compliance

Privacy Management

Privacy Management Administ...

Privacy Management Analysts

Privacy Management Investiga...

Subject Rights Request Admini...

Data Security Management

Data Investigator

Communication Compliance A...

Communication Compliance A...

Communication Compliance V...

Compliance Data Administrator

Compliance Manager Adminis...

**Compliance Administrator**

Role group name

Compliance Administrator

Role group description

Roles in the role group

Admin Unit Extension Manager

Case Management

Communication Compliance Admin

Communication Compliance Case Management

Compliance Administrator

Compliance Manager Administration

Compliance Search

Credential Reader

Credential Writer

Data Classification Feedback Provider

Data Classification Feedback Reviewer

Data Connector Admin

Data Investigation Management

Data Map Reader

Device Management

Disposition Management

DLP Compliance Management

Hold

IB Compliance Management

Information Protection Admin

Information Protection Analyst

Information Protection Reader

Insider Risk Management Admin

Insights Reader

Manage Alerts

Organization Configuration

Purview Agent Analysis

Purview Copilot Workspace Contributor

RecordManagement

Retention Management

Scan Reader

Scan Writer

Scope Manager

Source Reader

Source Writer

View-Only Audit Logs

View-Only Case

View-Only Device Management

View-Only DLP Compliance Management

View-Only IB Compliance Management

View-Only Manage Alerts

View-Only Recipients

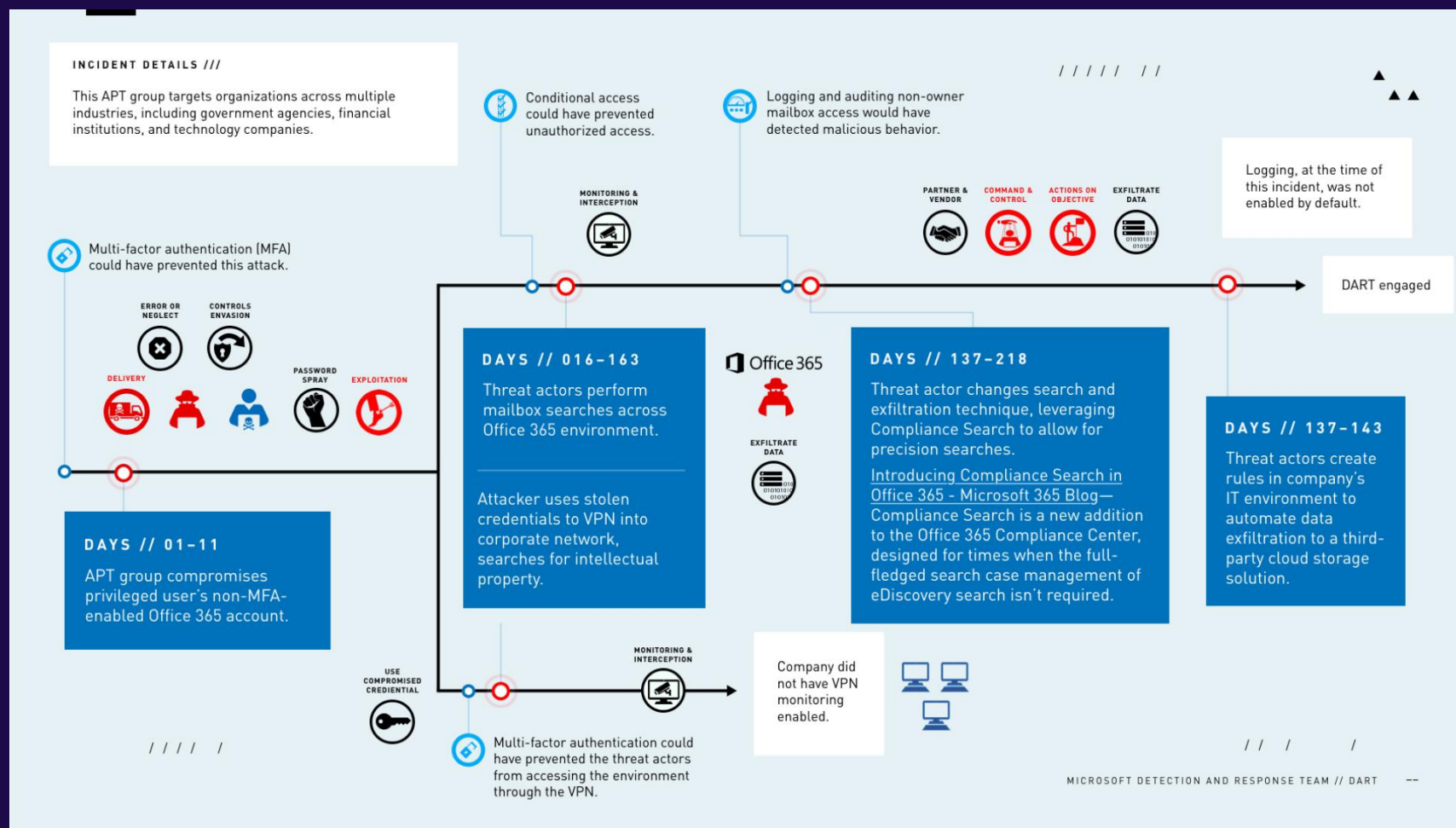
View-Only Record Management

View-Only Retention Management

Members in the role group

Display name	Type	Admin units
Adam Jensen	User	Organization

# RBAC: Purview - Seen in the Wild



Source: <https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2020/03/then-there-were-six.pdf>

# RBAC: SharePoint



Microsoft  
SharePoint

# RBAC: SharePoint

» Frequently messy configuration

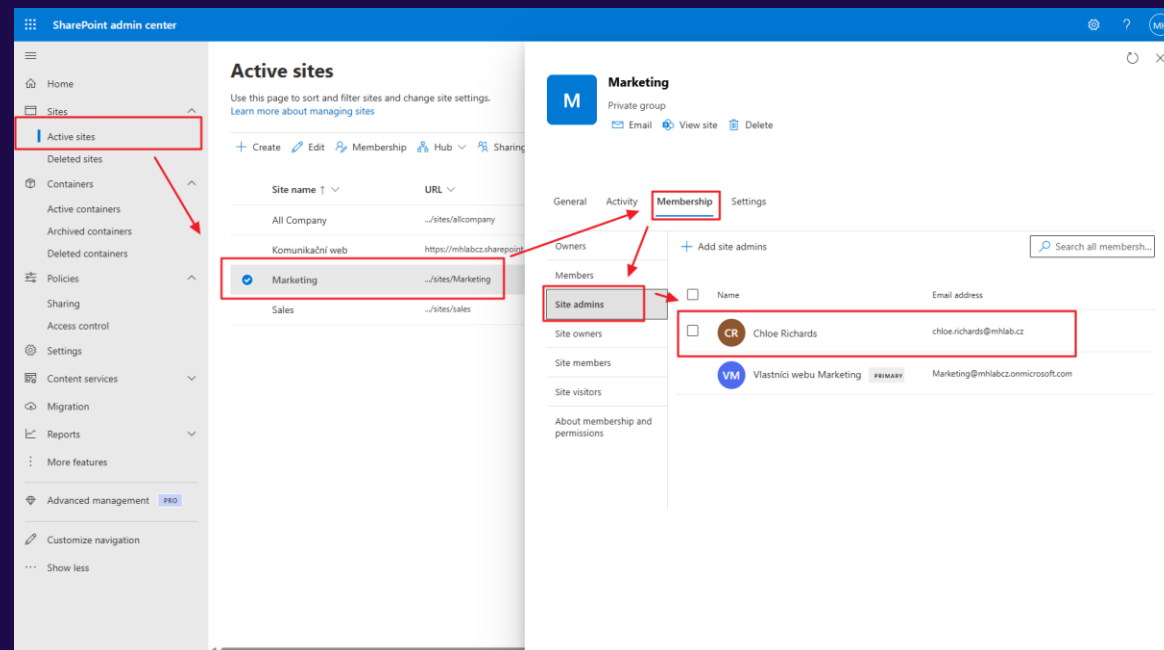
» Misconfigurations lead to:

» **Lateral movement / privilege escalation:** backdooring of stored applications/scripts/macros, searching for stored certificates or password files, or enable users to run/store custom scripts on sites.

» **Unauthorized Data Access**

» **Financial damage:** modification of invoices, agreements...

» Privileged persistence




# RBAC: SharePoint - Seen in the Wild

**RANSOMWARE**

## SaaS Ransomware Attack Hit Sharepoint Online Without Using a Compromised Endpoint

A SaaS ransomware attack against a company's Sharepoint Online was done without using a compromised endpoint.

By **Kevin Townsend** | June 9, 2023 (7:00 AM ET)



Cybersecurity firm Obsidian has observed a successful ransomware attack against Sharepoint Online (Microsoft 365) via a Microsoft Global SaaS admin account rather than the more usual route of a compromised endpoint.

**TRENDING**

- 1 Canadian Airline WestJet Hit by Cyberattack
- 2 Archetyp Dark Web Market Shut Down by Law Enforcement
- 3 High-Severity Vulnerabilities Patched in Tenable Nessus Agent
- 4 Google's \$32 Billion Wiz Deal Draws DOJ Antitrust Scrutiny: Report
- 5 US Insurance Industry Warned of Scattered Spider Attacks
- 6 Industry Reactions to Trump Cybersecurity Executive Order: Feedback Friday
- 7 Critical Vulnerability Exposes Many Mitel MiCollab Instances to Remote Hacking

Anubis Ransomware Packs a

Source: <https://www.securityweek.com/saas-ransomware-attack-hit-sharepoint-online-without-using-a-compromised-endpoint/>



# RBAC: Power Platform



# RBAC: Power Platform

- » Misconfigurations lead to:
  - » Lateral movement / privilege escalation
  - » Unauthorized Data Access
- » Persistence
- » Data exfiltration

Power Platform admin center

Search for settings, pages, and more

Manage

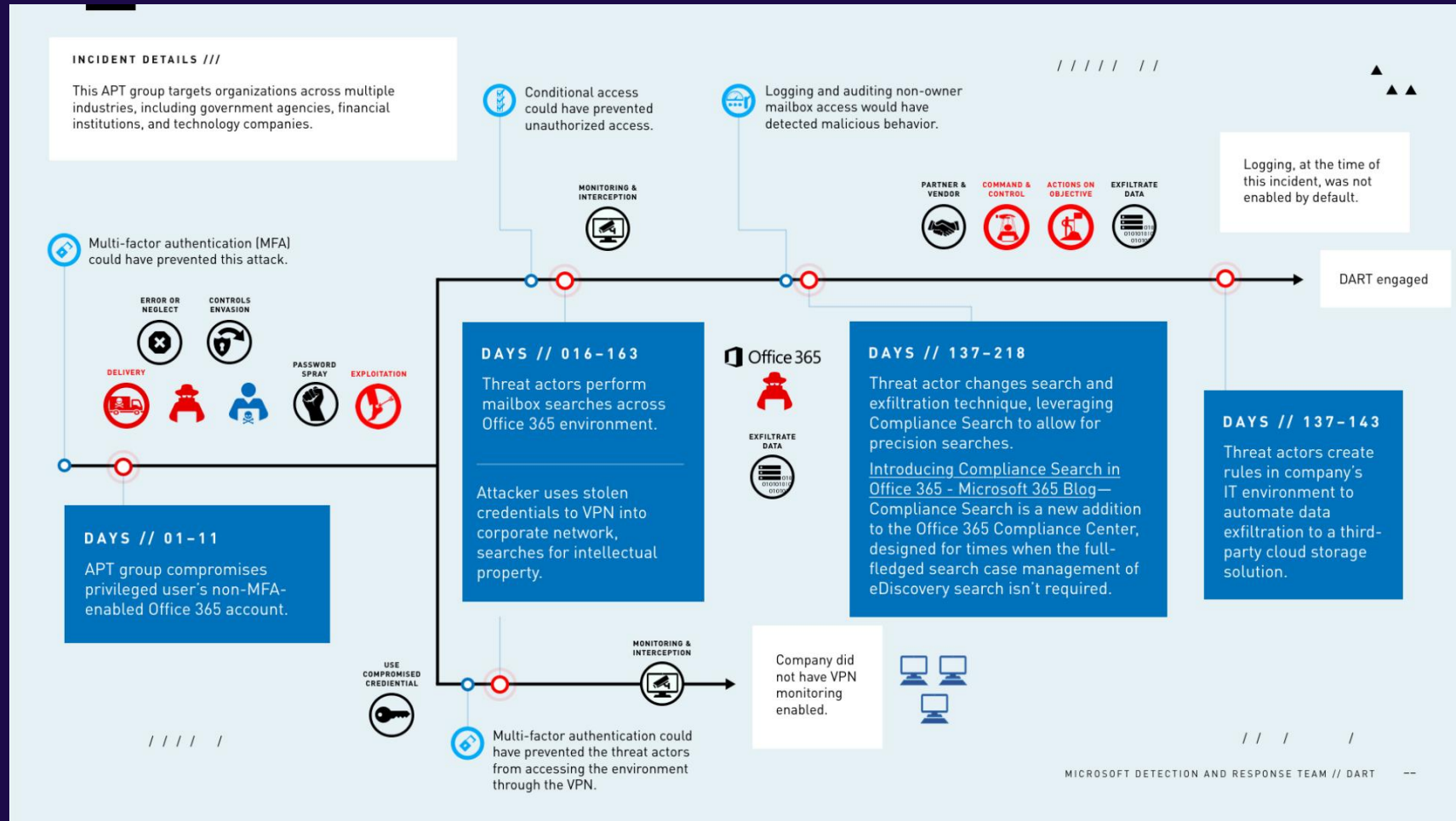
Environments > PATRON-IT s.r.o. (default) > Settings > Security roles > Správce systému > Members

Add or remove people from the Správce systému security role. [Learn more](#)

Business unit  
org6021b4c3

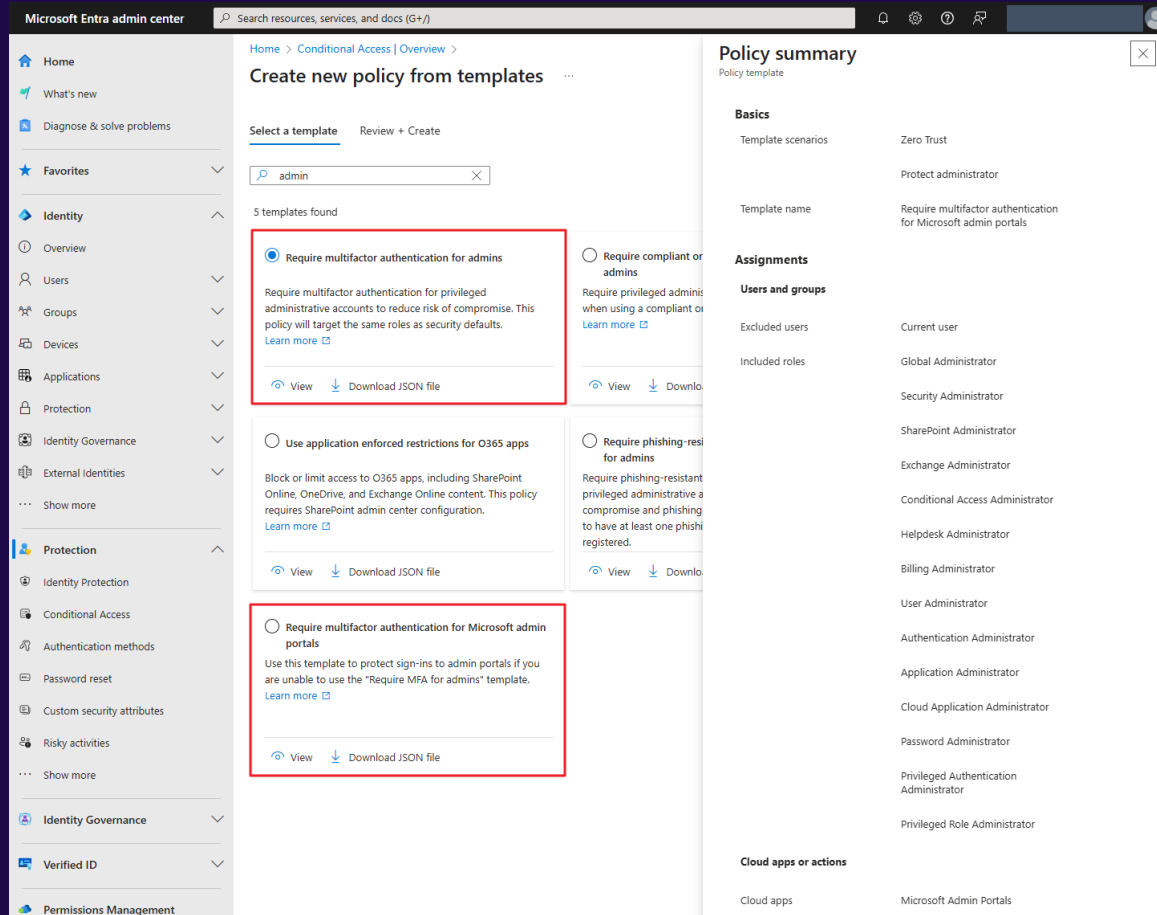
Name ↑	Type	Username
CatalogServiceEur, #	...	CatalogServiceEur@onmicrosoft.com
CCADDataAnalyticsML, #	...	CCADDataAnalyticsML@onmicrosoft.com
CDSUserManagement, #	...	CDSUserManagement@onmicrosoft.com
CDSUserManagementApi, #	...	CDSUserManagementApi@onmicrosoft.com

# RBAC: Power Platform - Seen in the Wild

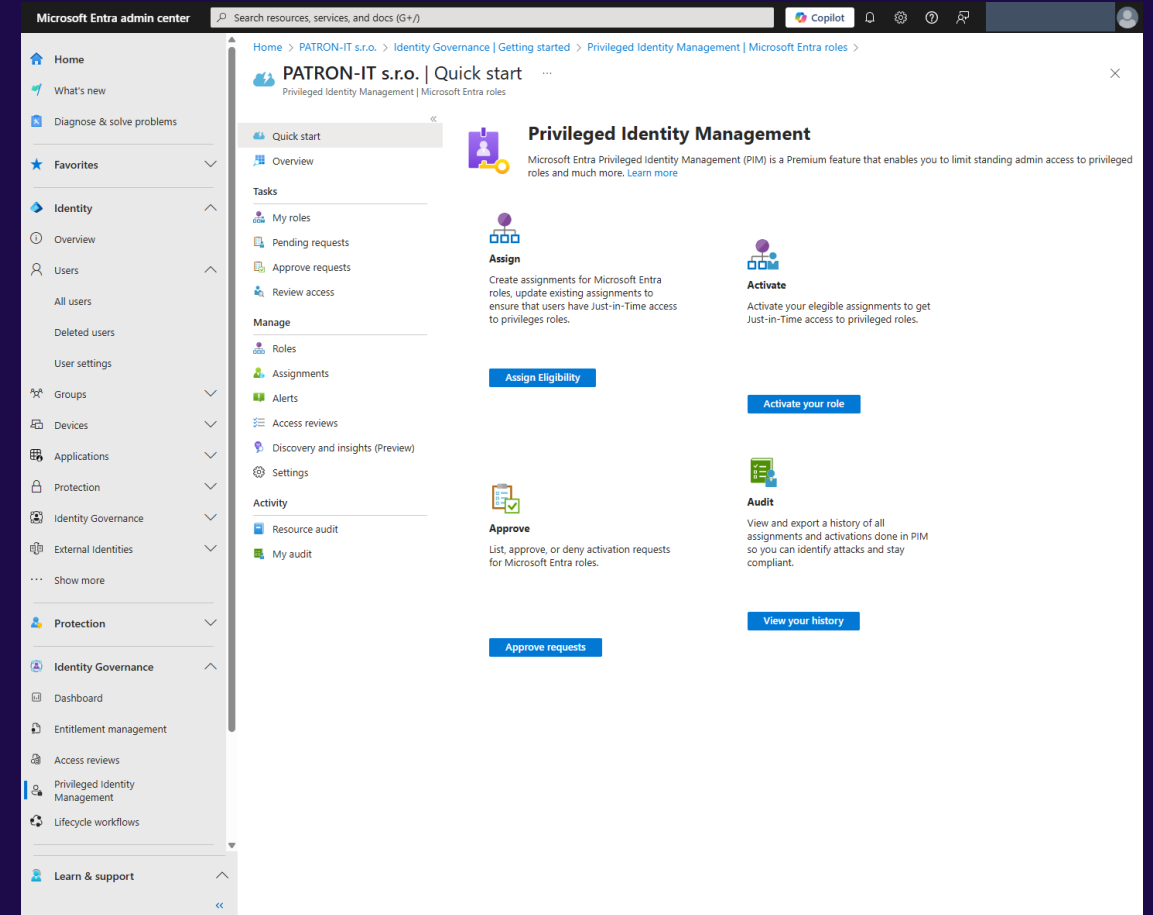


Source: <https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2020/03/then-there-were-six.pdf>

# Entra ID – RBAC – Caveats



Escapes some Conditional Access Policies



Outside of standard PIM for MS Entra Roles

# RBAC: Defense

## STRENGTHENING DEFENSE





# RBAC: Defense

- » Monitoring for changes (Unified Audit Log)
- » Regular reviews
- » New research
- » New tooling
  - » <https://github.com/Cloud-Architekt/EntraOps> (Thomas Naunheim)





**Thank you for  
《your attention》**