Martin Haller

Microsoft Entra ID RBAC: The Shady Place Behind Basic Entra ID Security

TROOPERS

PATRON IT OCHRANA A SPRÁVA SÍTÍ

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

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

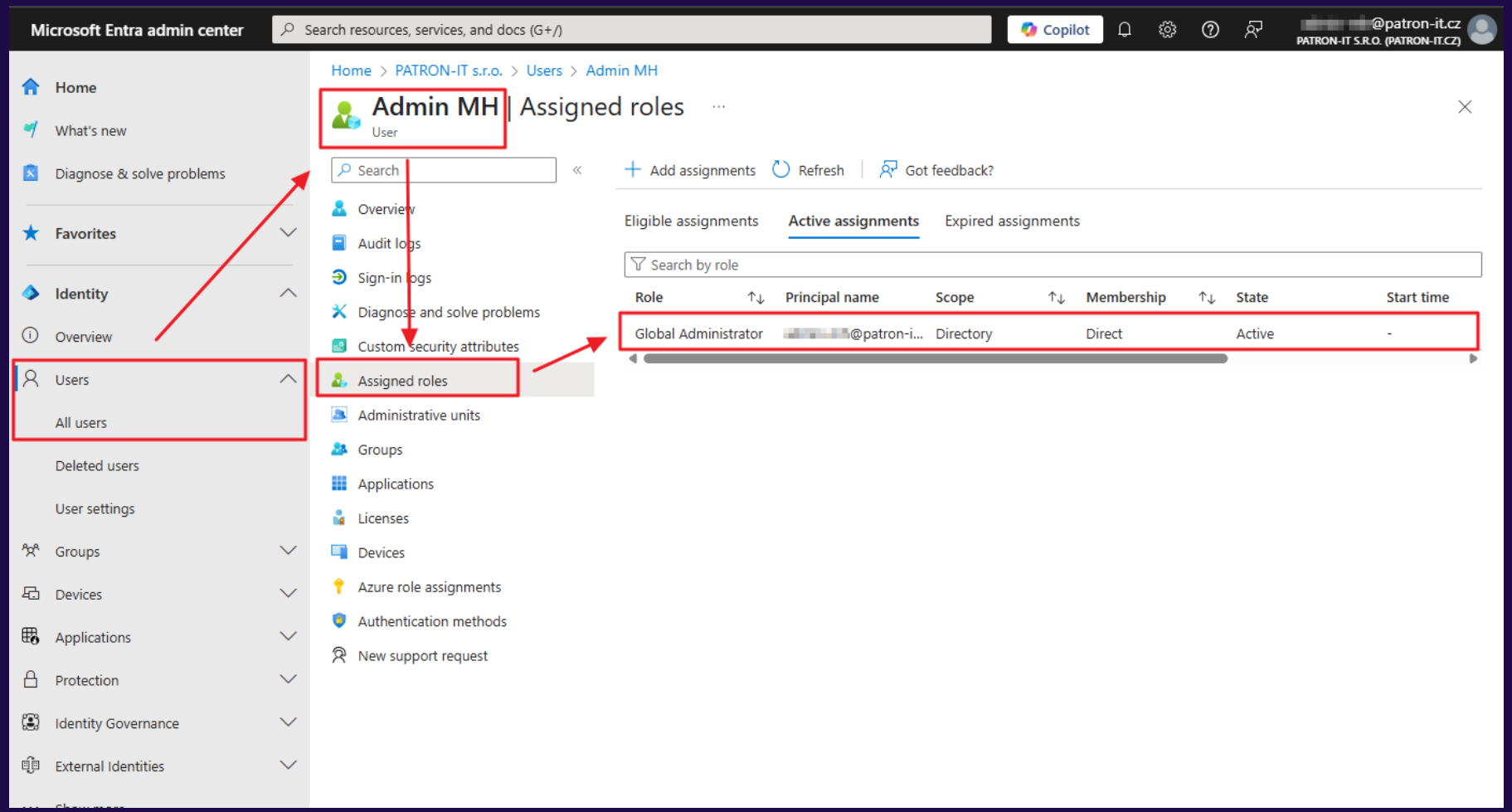
Where We Stand – My point of view

- 🔮 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

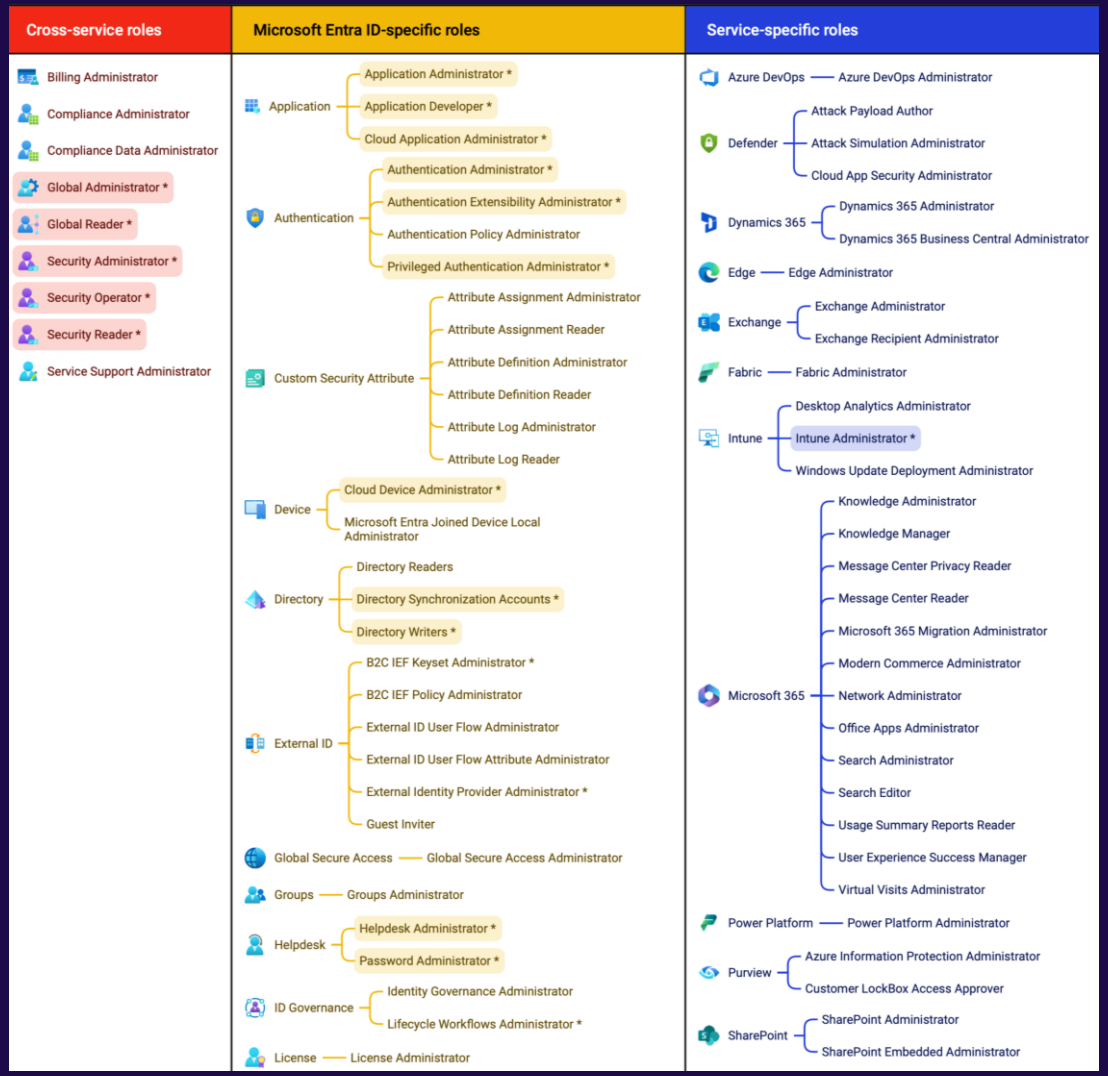
RBAC: Role-Based Access Control

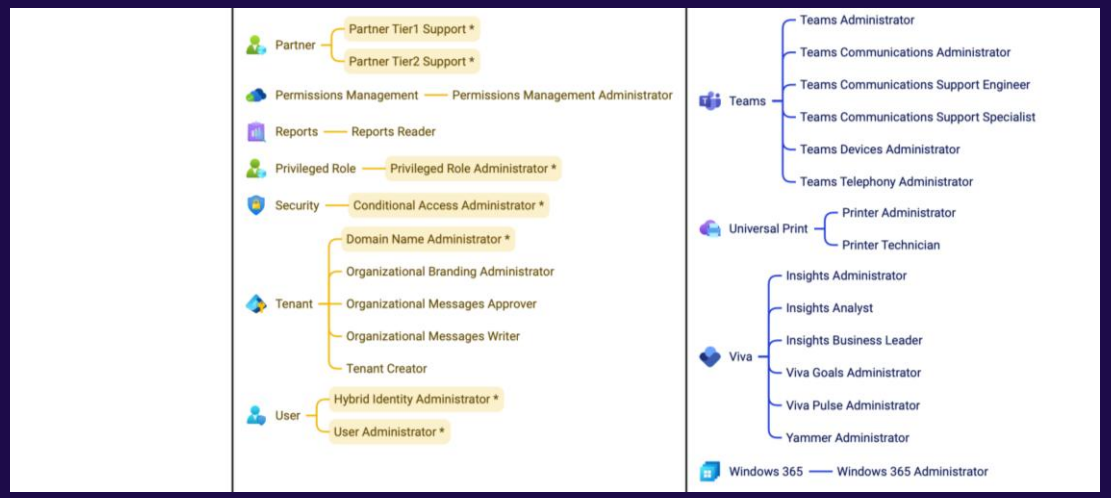
„RBAC is a method of enforcing access controls by assigning users to predefined roles, and associating each role with specific permissions or privileges.“

Entra ID – RBAC – Single pane of glass



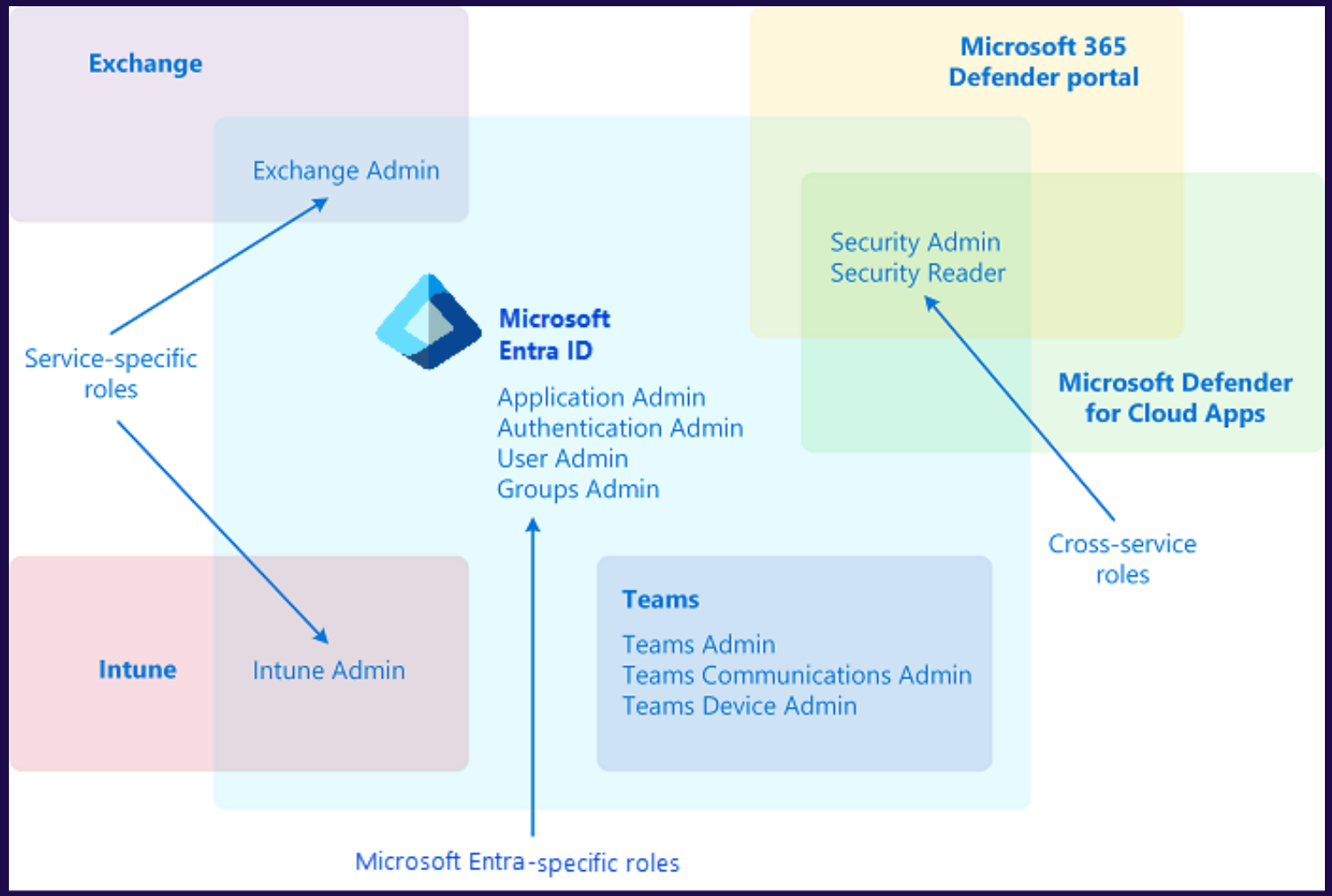
Entra ID – RBAC - Admin Roles





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

Entra ID – RBAC – The reality



Entra ID – RBAC – Auditing tools

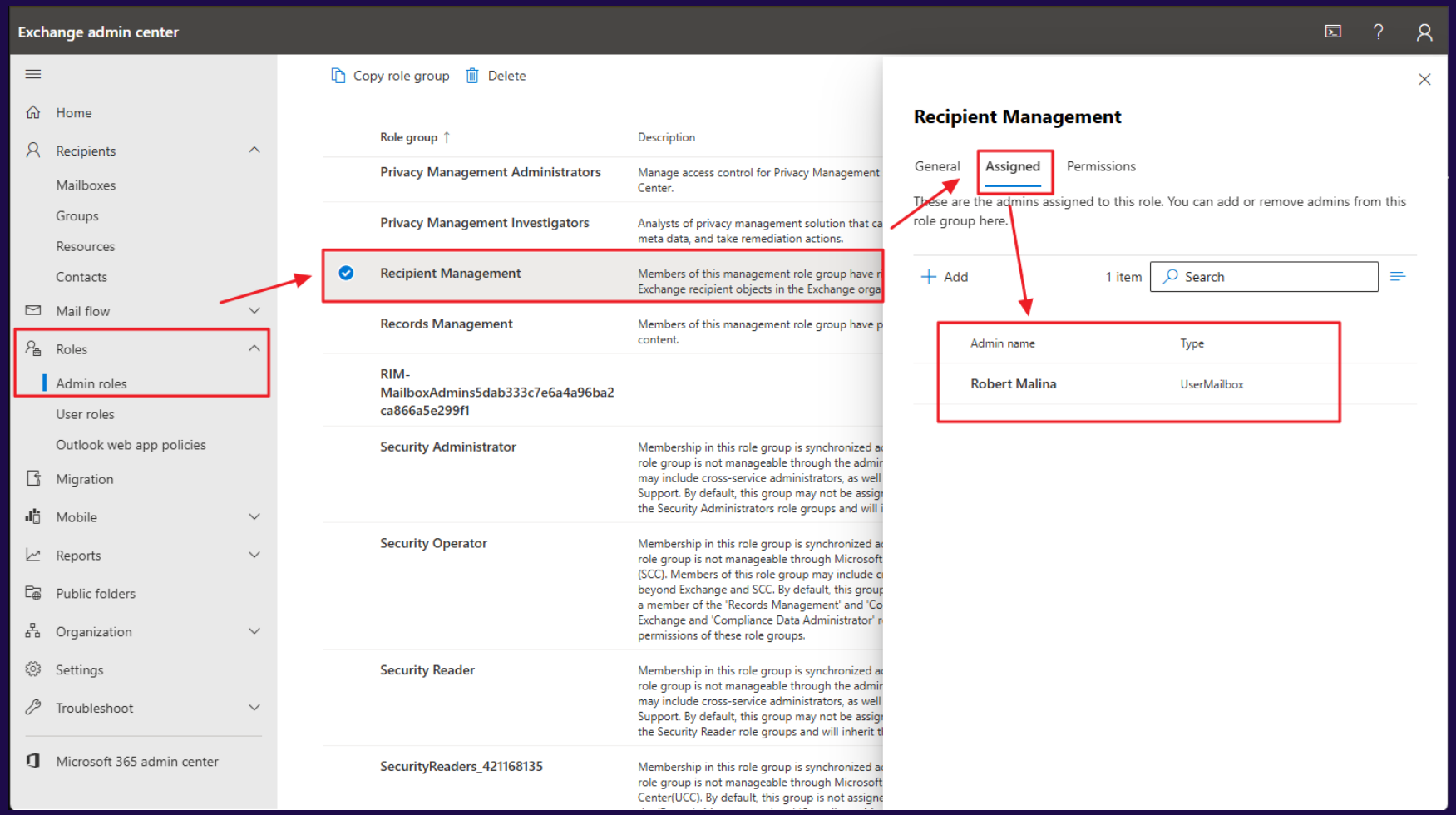
- » ScubaGear (https://github.com/cisagov/ScubaGear)
- » Maester (https://maester.dev/)
- » BloodHound (https://github.com/SpecterOps/BloodHound)
- » PingCastle (https://www.pingcastle.com/)
- » PurpleKnight (https://www.semperis.com/purple-knight/)

😥 APP SPECIFIC RBAC ISN'T COVERED 😥

RBAC: Exchange

RBAC: Exchange

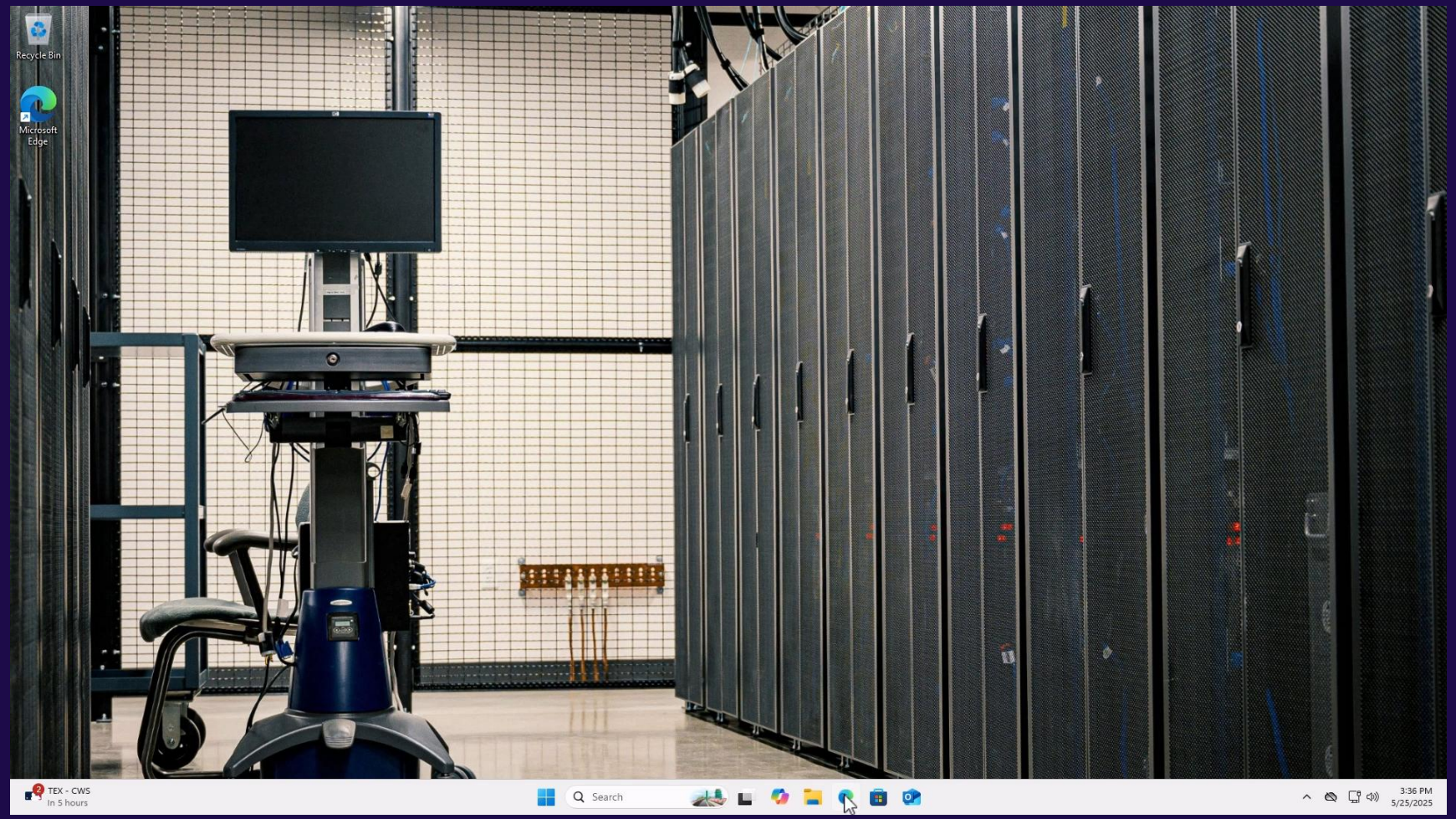
- » The most problematic in audits
- » Often breaks tiering model



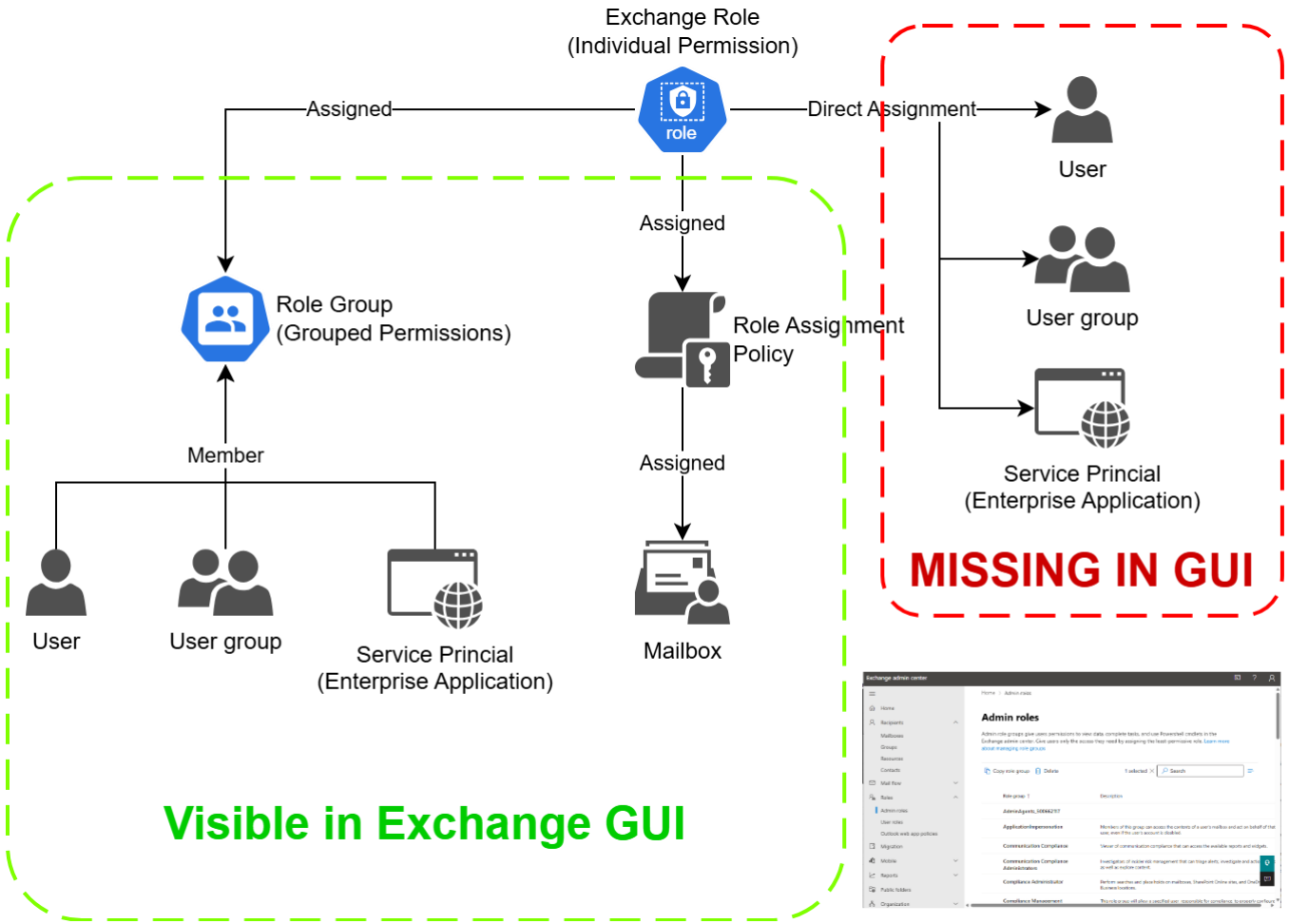
RBAC: Exchange

- **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**

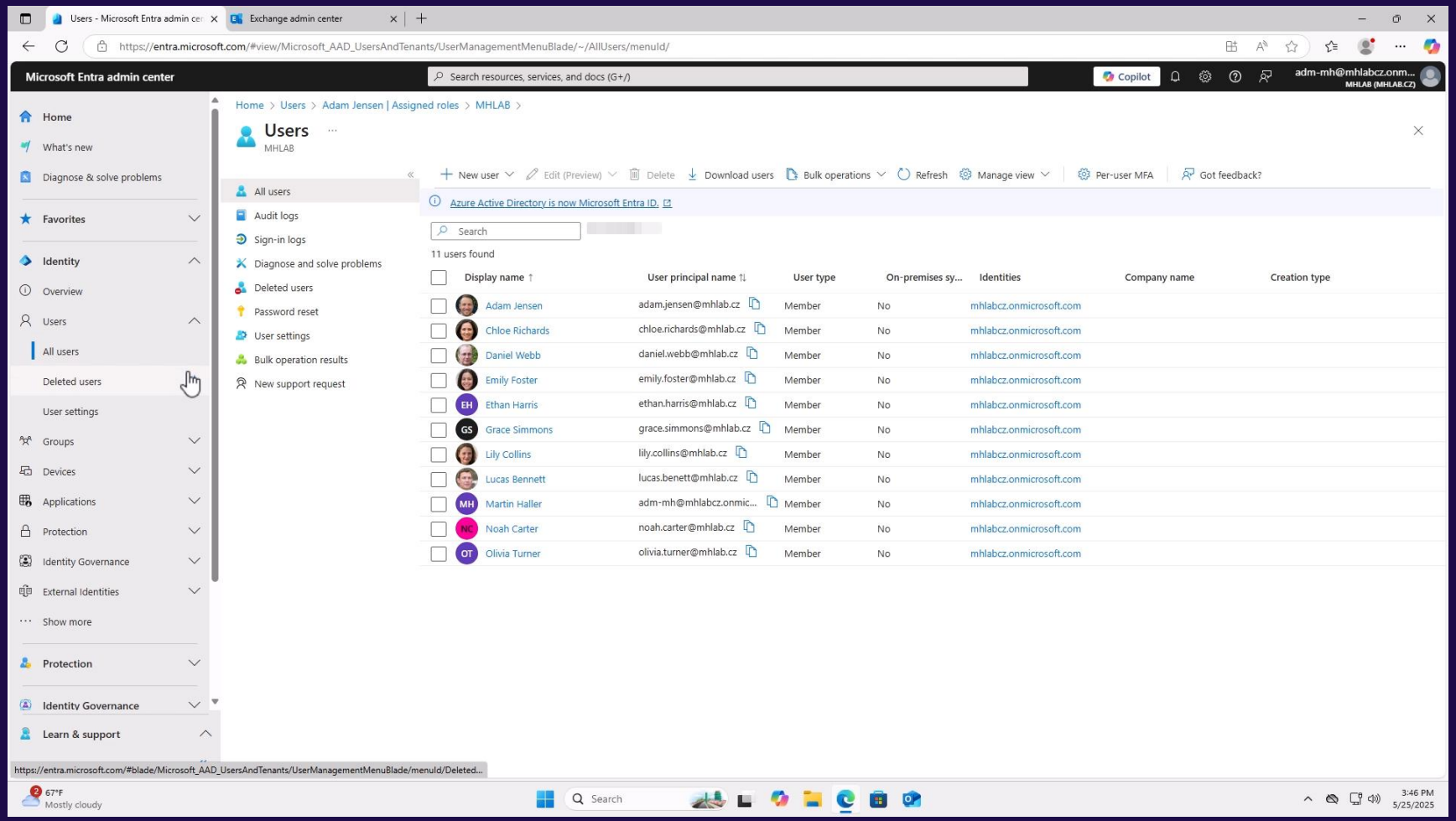
RBAC: Exchange – DEMO Priv. Escalation



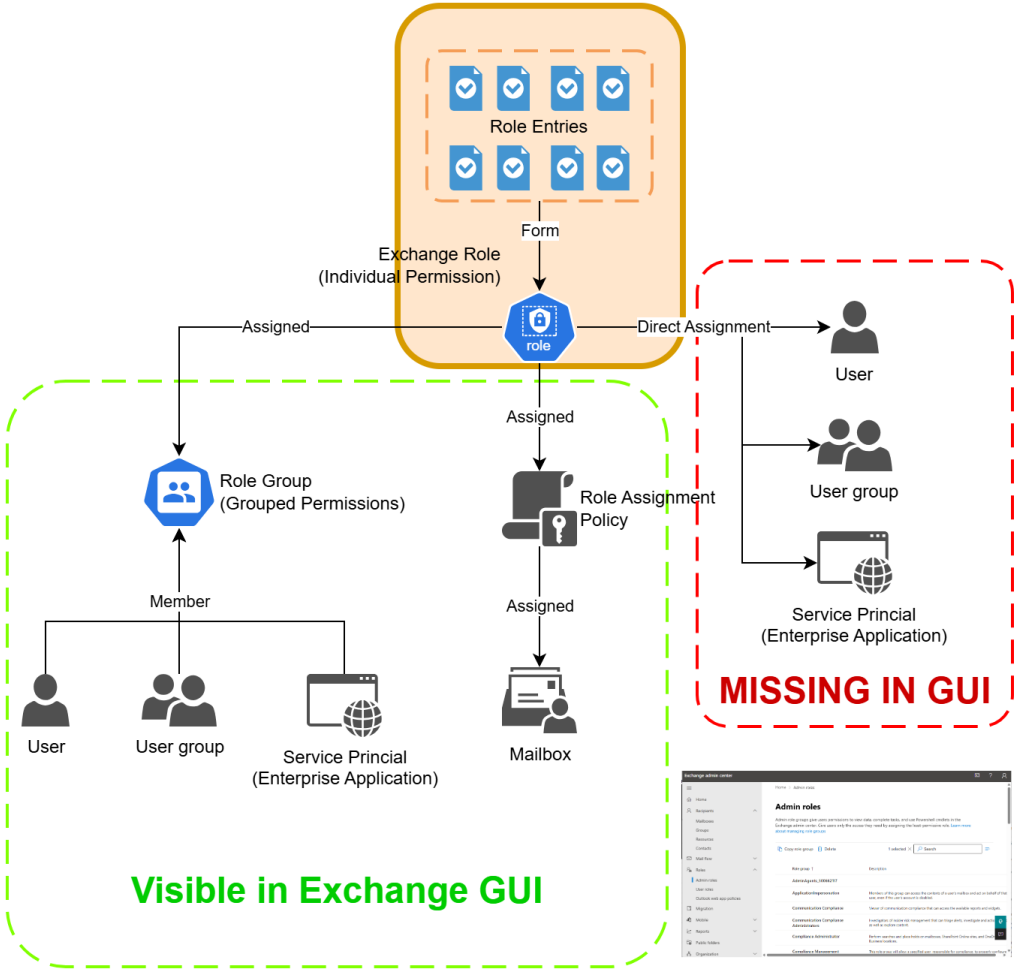
RBAC: Exchange – Assignment possibilities



RBAC: Exchange – DEMO Persistence



RBAC: Exchange – Role isn't atomic



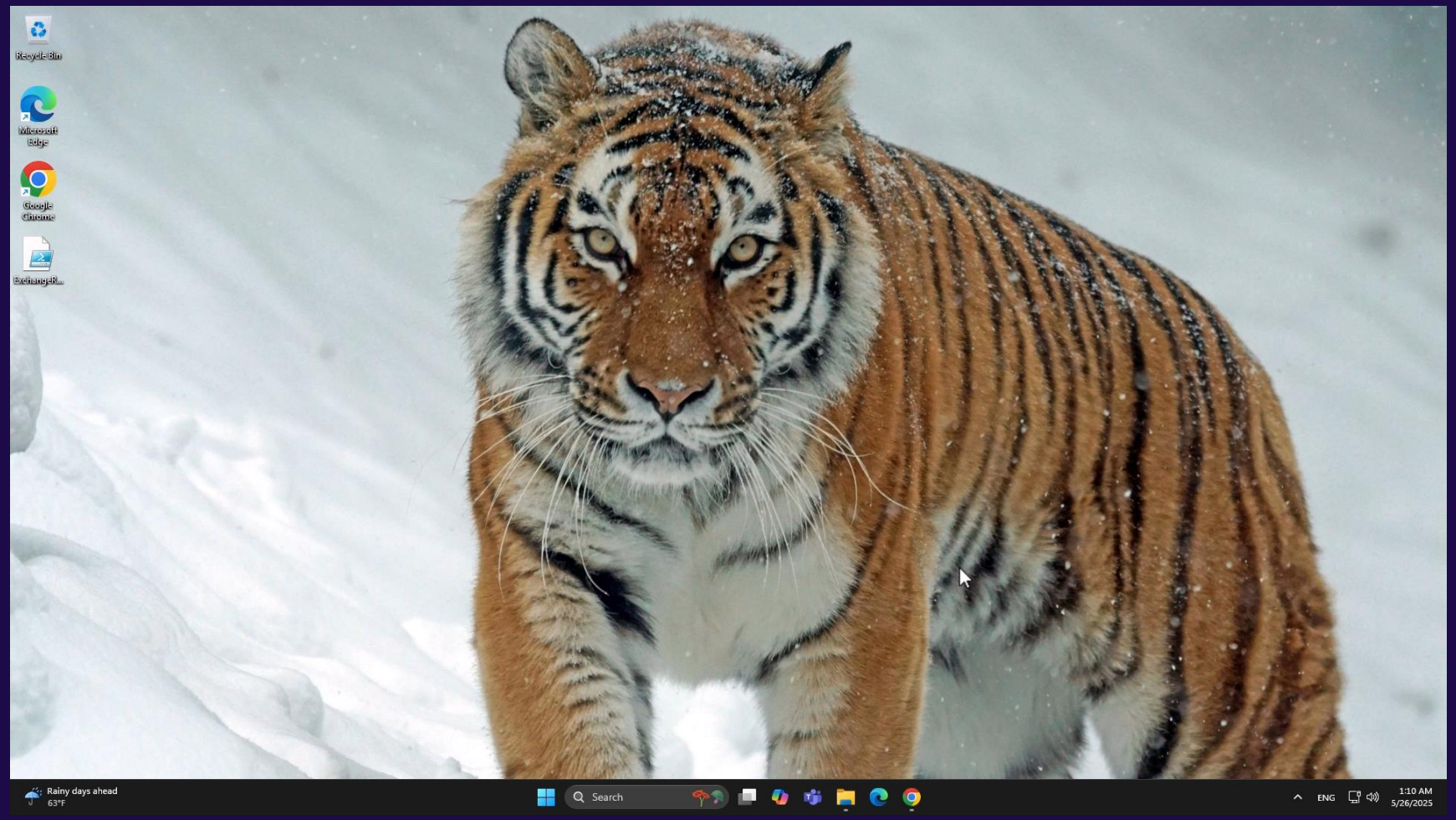
RBAC: Exchange – DEMO Persistence (v2)

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

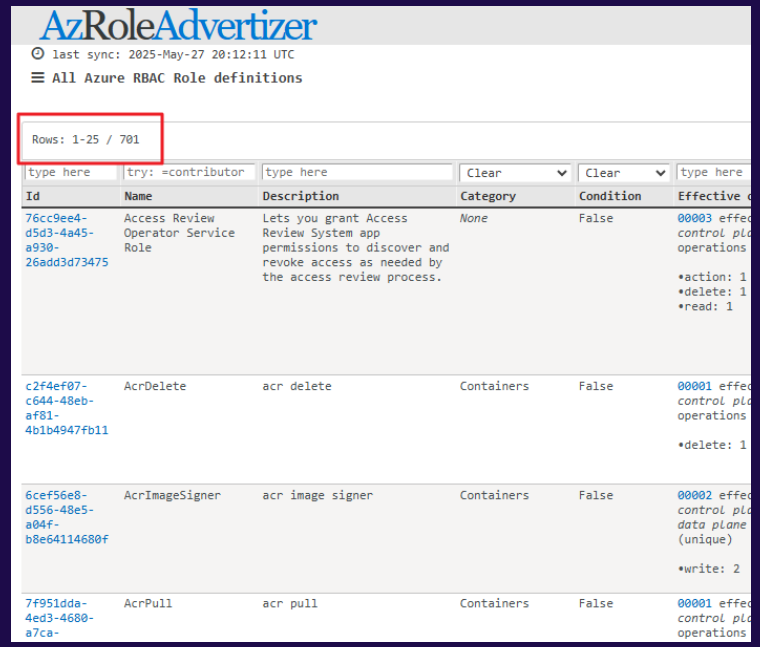
Over the past months, we have provided support to multiple organizations that have fallen victim to Business Email Compromise (BEC) attacks. In this blog we would like to share some of the latest Tactics, Techniques & Procedures (TTPs) we observed during a specific BEC investigation in a Microsoft 365 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**



Source: 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

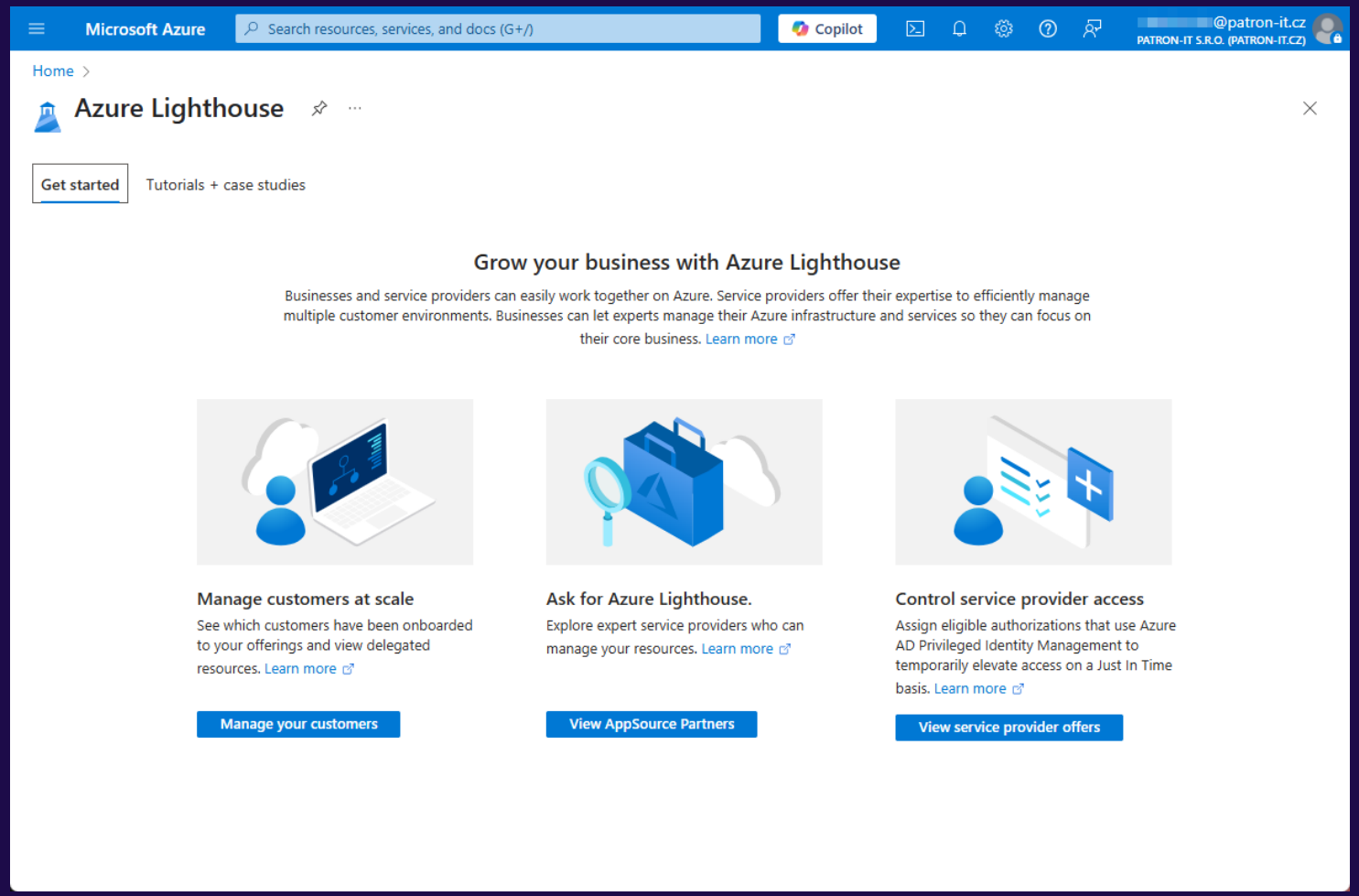
Search by name or email

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

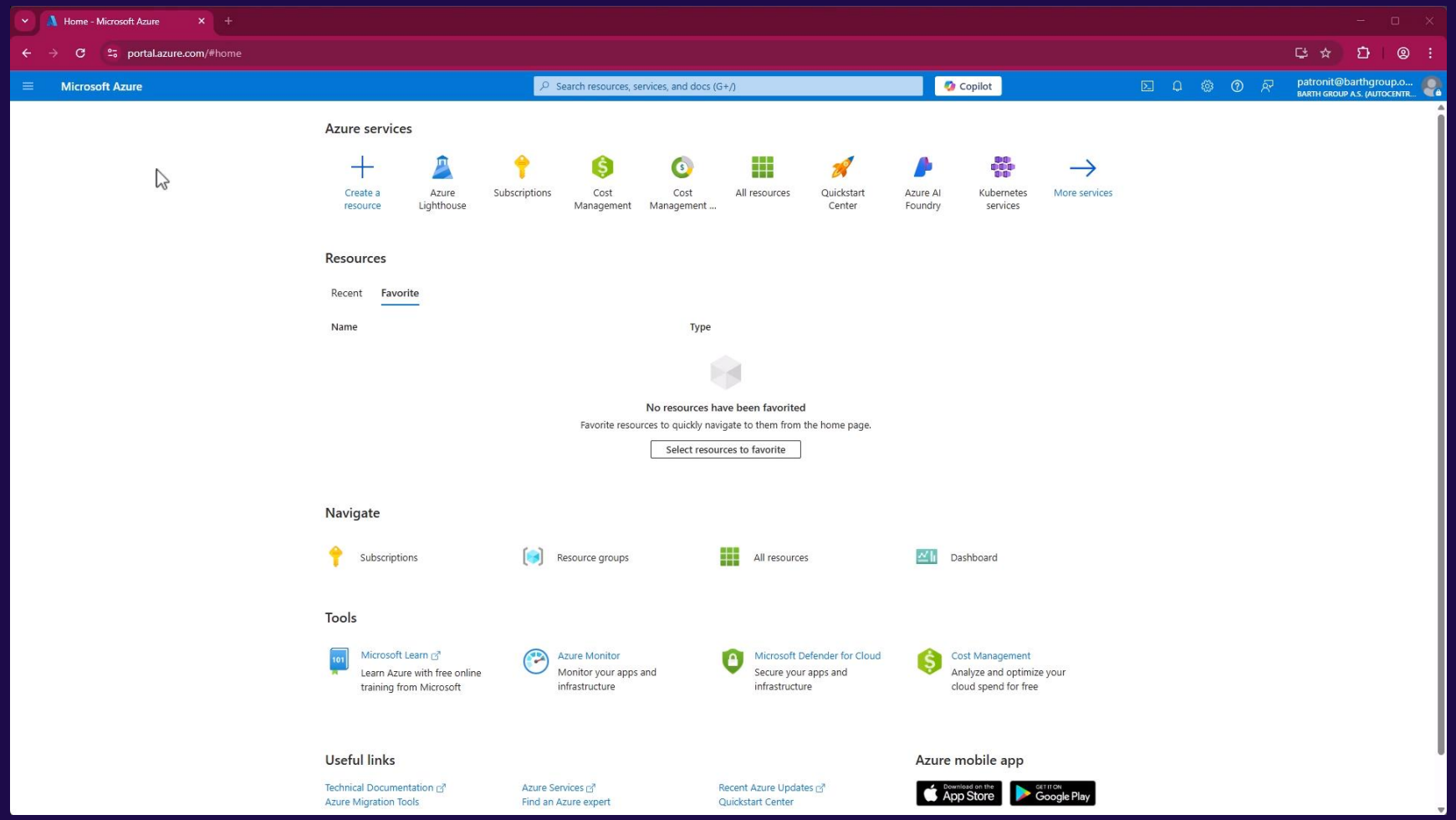
All (29) | Job function roles (13) | Privileged administrator roles (16)

Name	Type	Role	Scope	State	End time	Condition
Owner (5)						
AT [redacted]	User	Owner	This resource	Active Permanent	Permanent	None
AT [redacted]	User	Owner	Management group (Inhe···	Active Permanent	Permanent	None
FP 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
PZ [redacted]	User	Owner	This resource	Active Permanent	Permanent	None

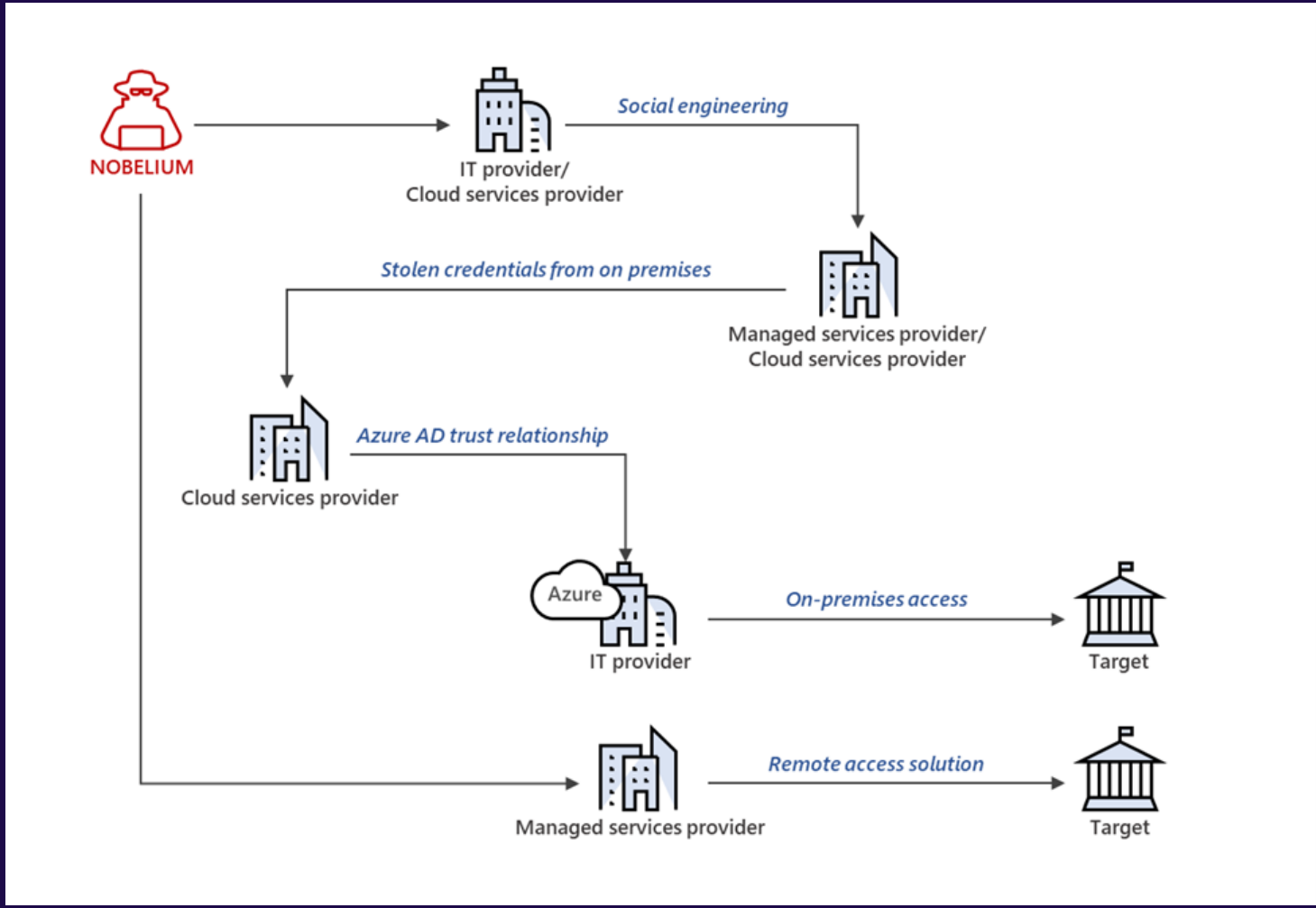
RBAC: Azure - Lighthouse



RBAC: Azure – DEMO Persistence



RBAC: Azure - Seen in the Wild

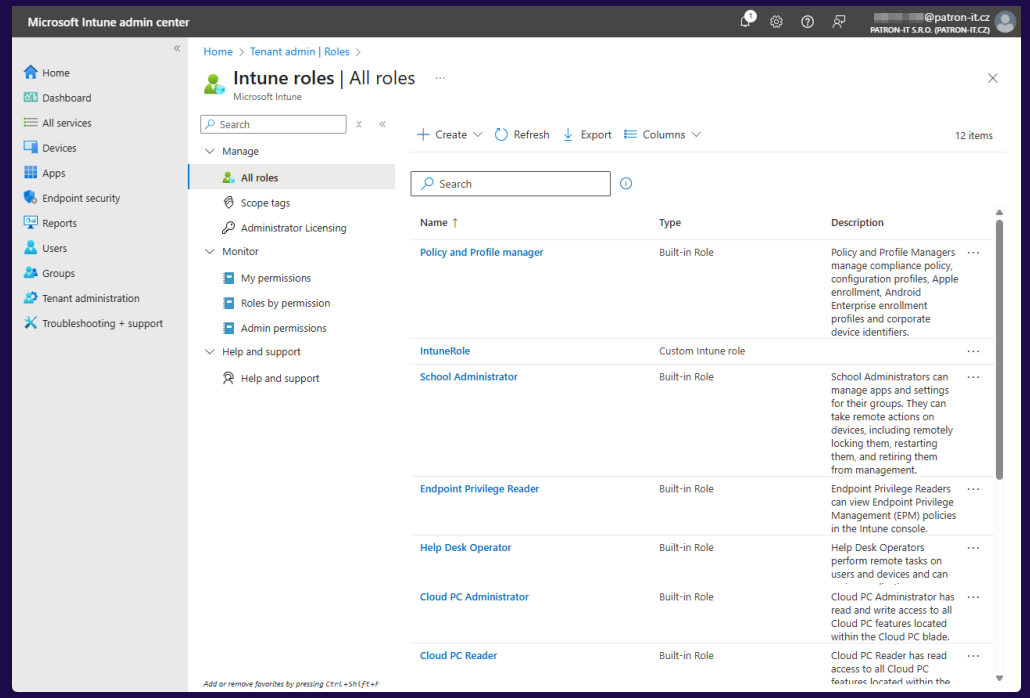


Source: https://www.microsoft.com/en-us/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/

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

Google Cloud | Contact sales | Get started for free

Blog | Solutions & technology | Ecosystem | Developers & Practitioners | Transform with Google Cloud

Threat Intelligence

Stealing the LIGHTSHOW (Part One) — North Korea's UNC2970

March 9, 2023

Mandiant

Written by: Mandiant Intelligence and Consulting

Since June 2022, Mandiant has been tracking a campaign targeting Western Media and Technology companies from a suspected North Korean espionage group tracked as UNC2970. In June 2022, Mandiant Managed Defense detected and responded to an UNC2970 phishing campaign targeting a U.S.-based technology company. During this operation, Mandiant observed UNC2970 leverage three new code families: TOUCHMOVE, SIDESHOW, and TOUCHSHIFT. Mandiant suspects UNC2970 specifically targeted security researchers in this operation. Following the

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

Medium | Search | Write | Sign up | Sign in

Posts By SpecterOps Tea...

Intune Attack Paths — Part 1

Andy Robbins | Follow | 18 min read · Jan 15, 2025

109 | 1

Prior Work

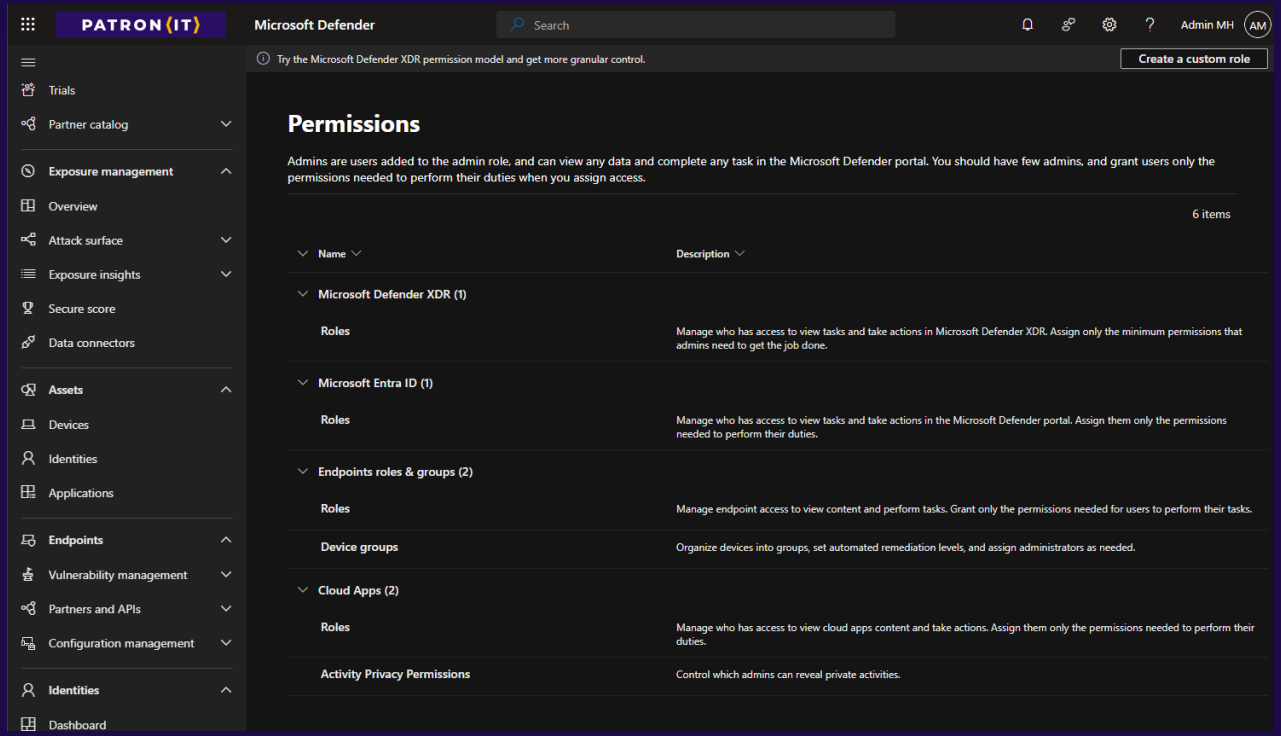
Several people have recently produced high-quality work around Intune tradecraft. I want to specifically mention:

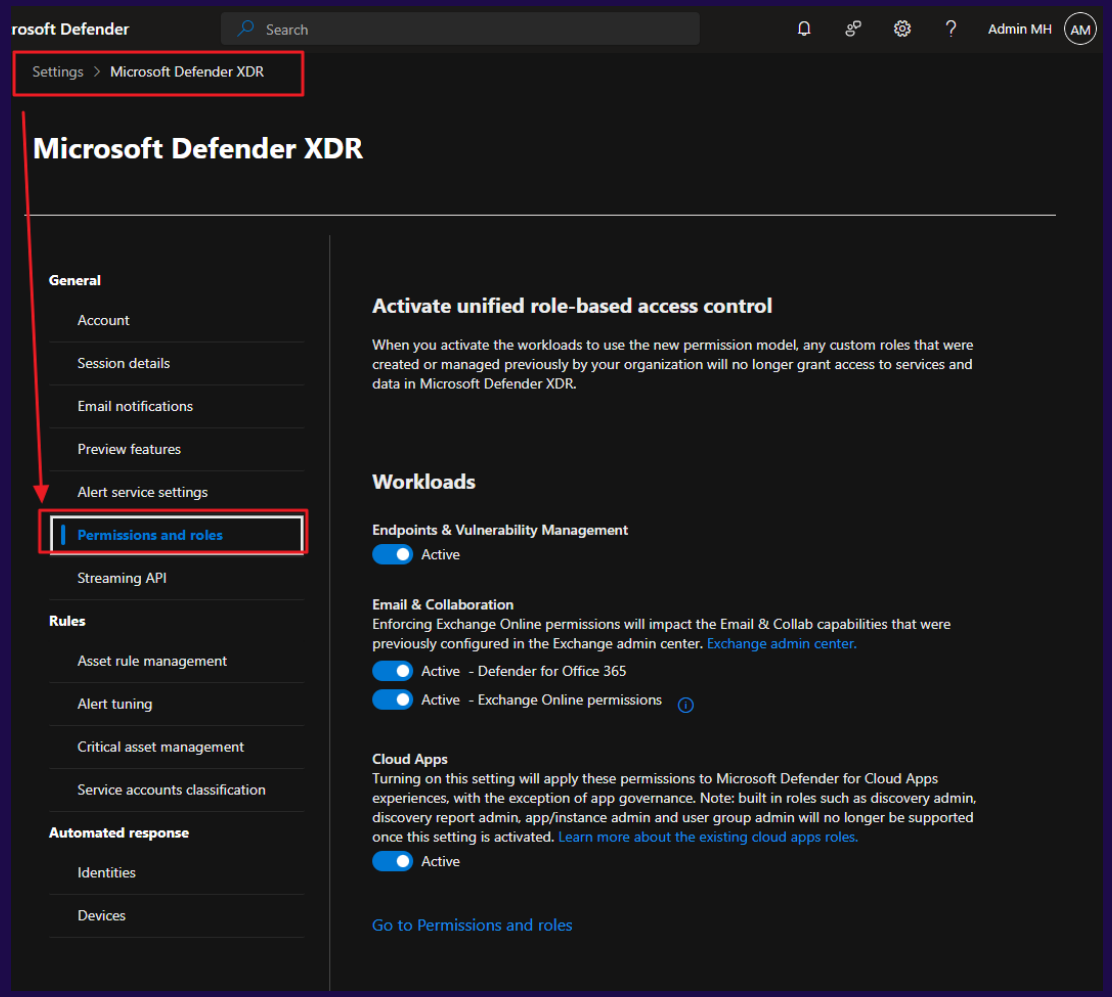
- Chris Thompson and his work on Maestro
- Dirk-jan Mollema and his work with Primary Refresh Tokens
- Adam Chester and his work with Web Account Manager
- Brett Hawkins and his work with Intune lateral movement detection
- Thibault Van Geluwe de Berlaere, Karl Madden, and Corné de Jong, and their work on abusing MS Graph permissions against Intune

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

RBAC: Microsoft Defender

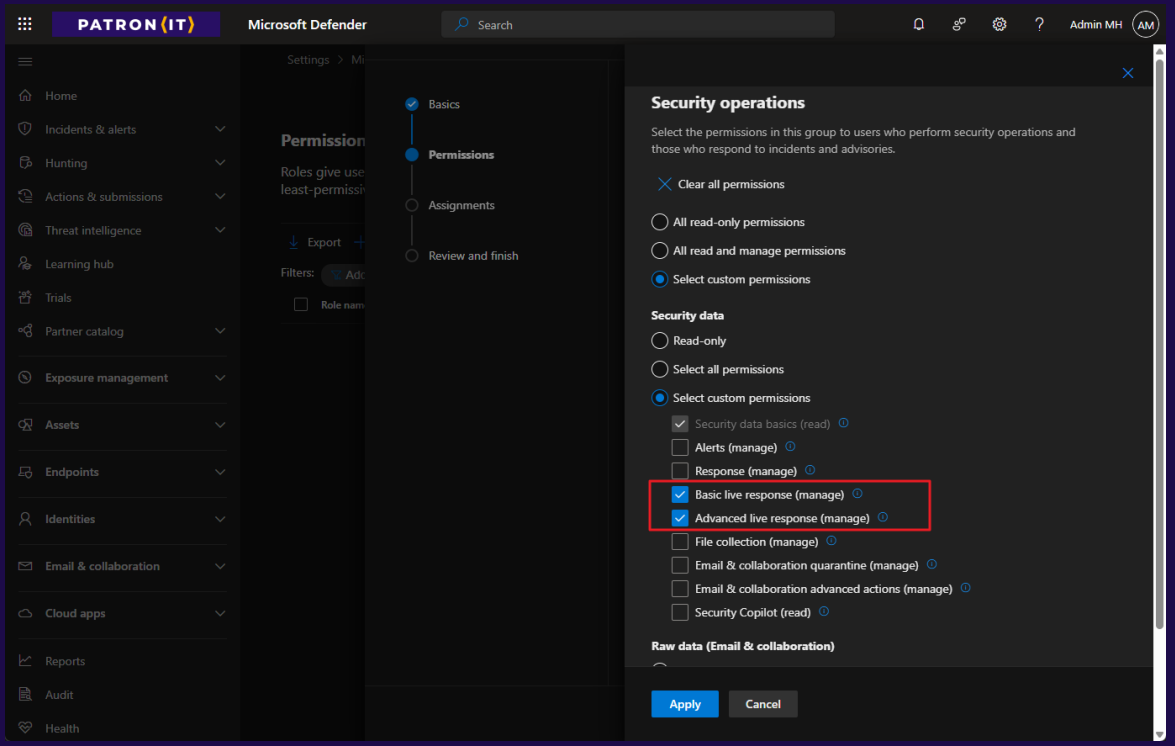
RBAC: Defender



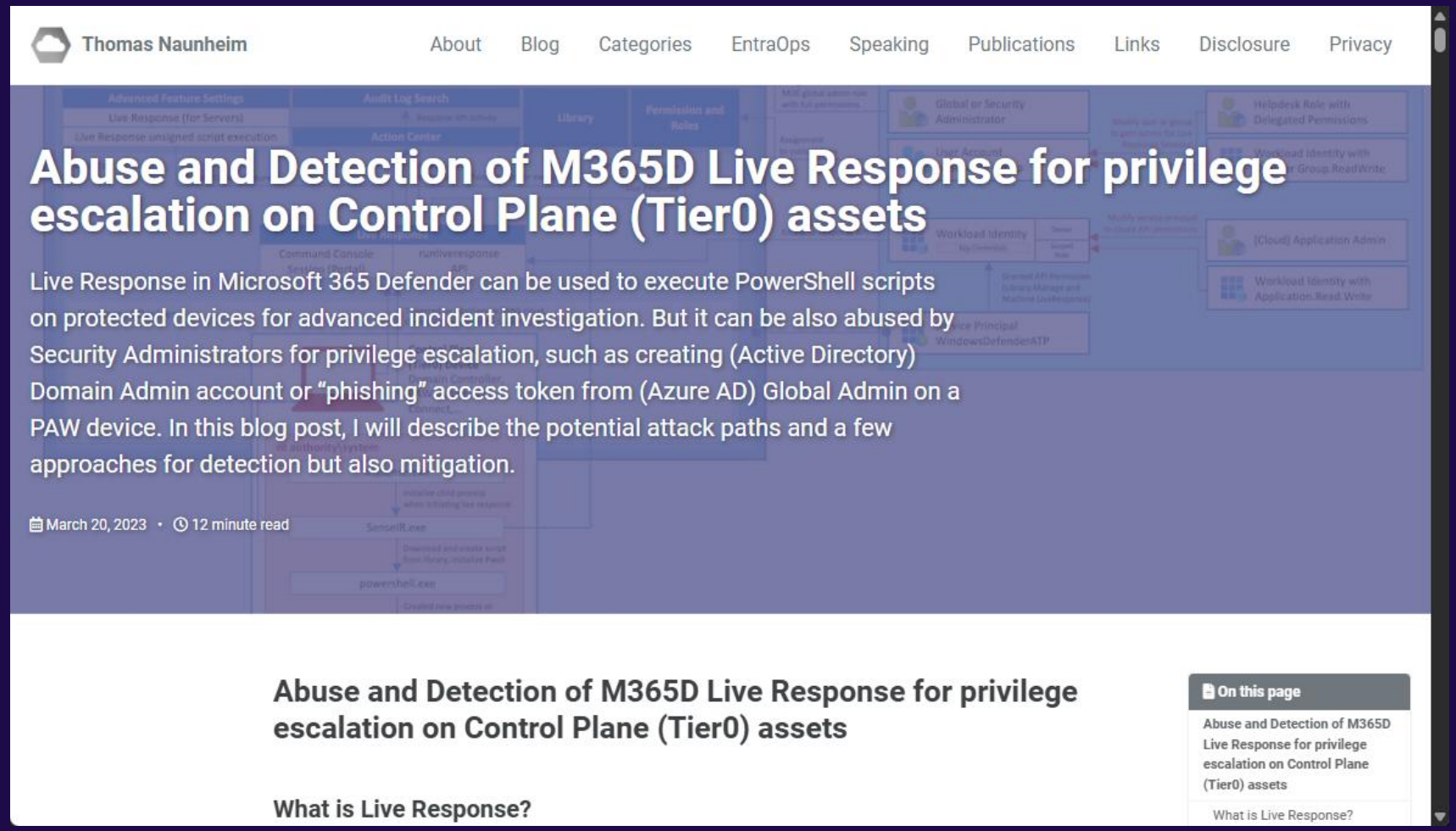


RBAC: Defender

- » **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

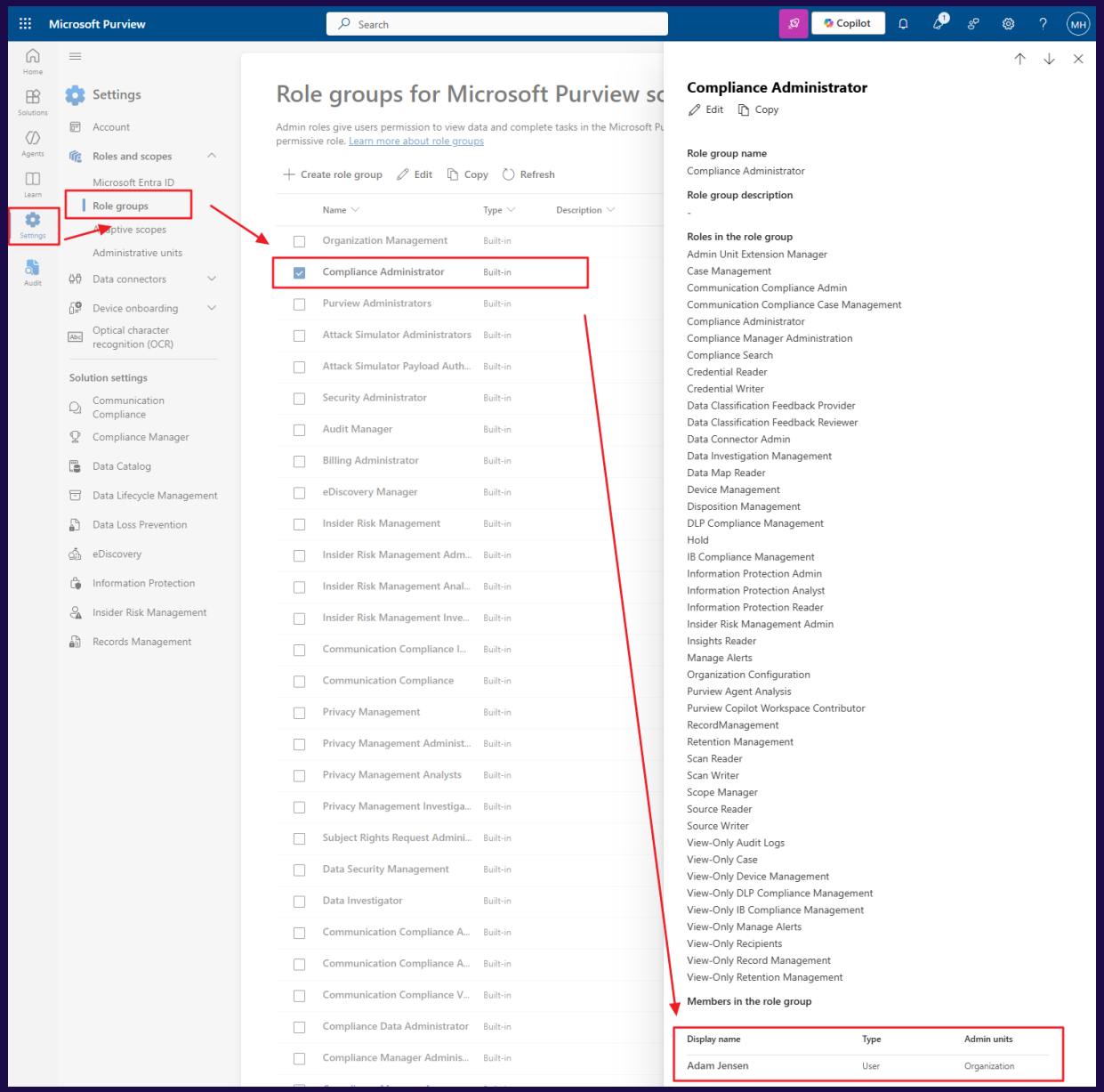


Source: https://www.cloud-architekt.net/abuse-detection-live-response-tier0/

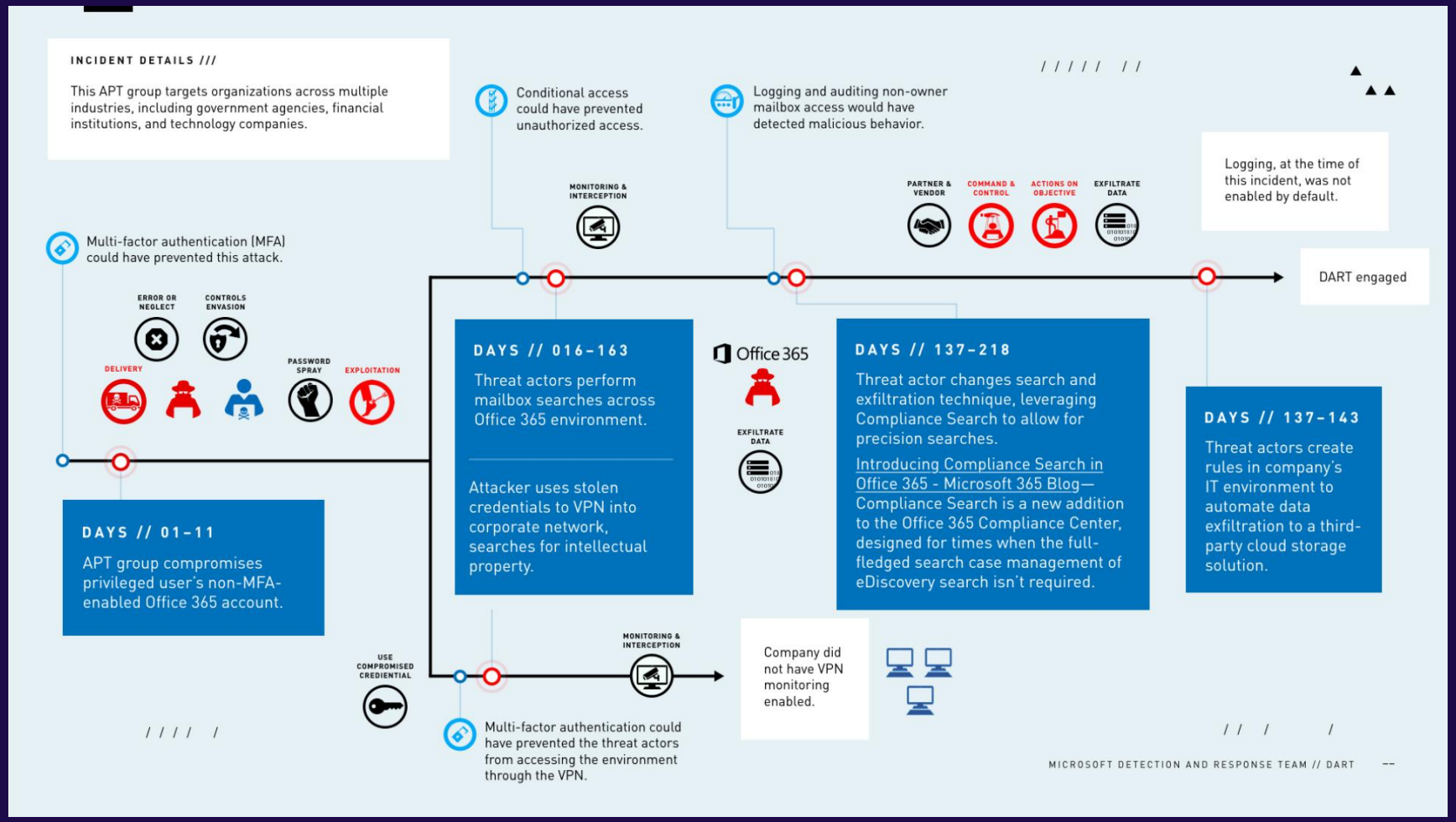
RBAC: Purview

RBAC: Purview

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



RBAC: Purview - Seen in the Wild

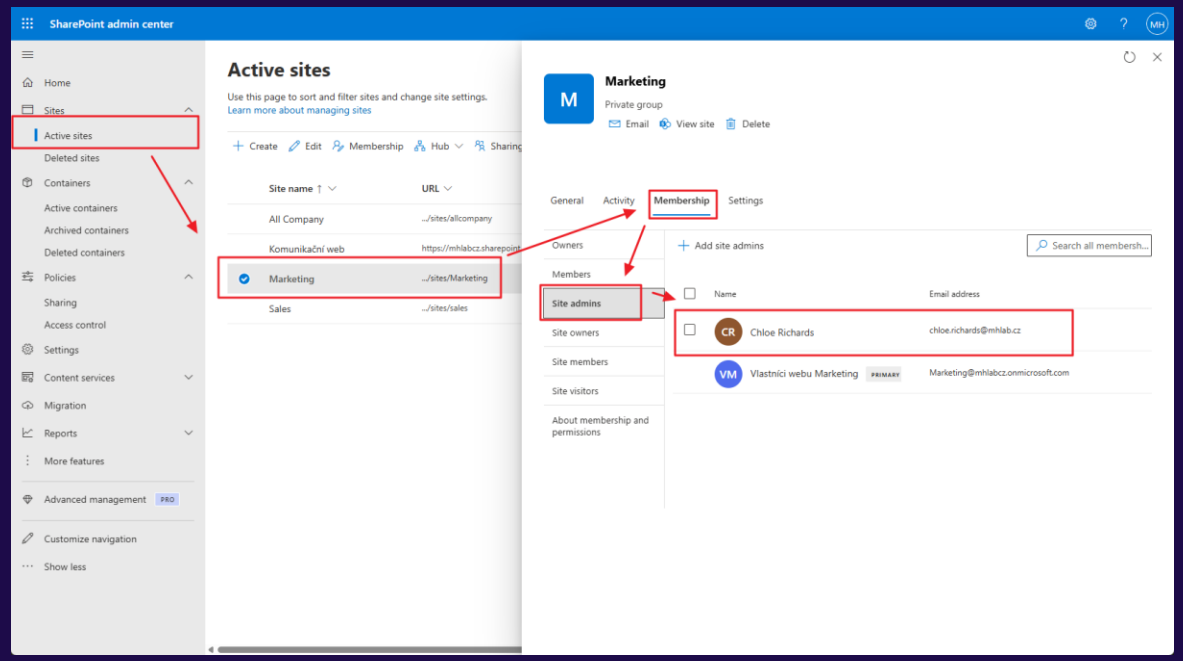


Source: https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2020/03/then-there-were-six.pdf

RBAC: SharePoint

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

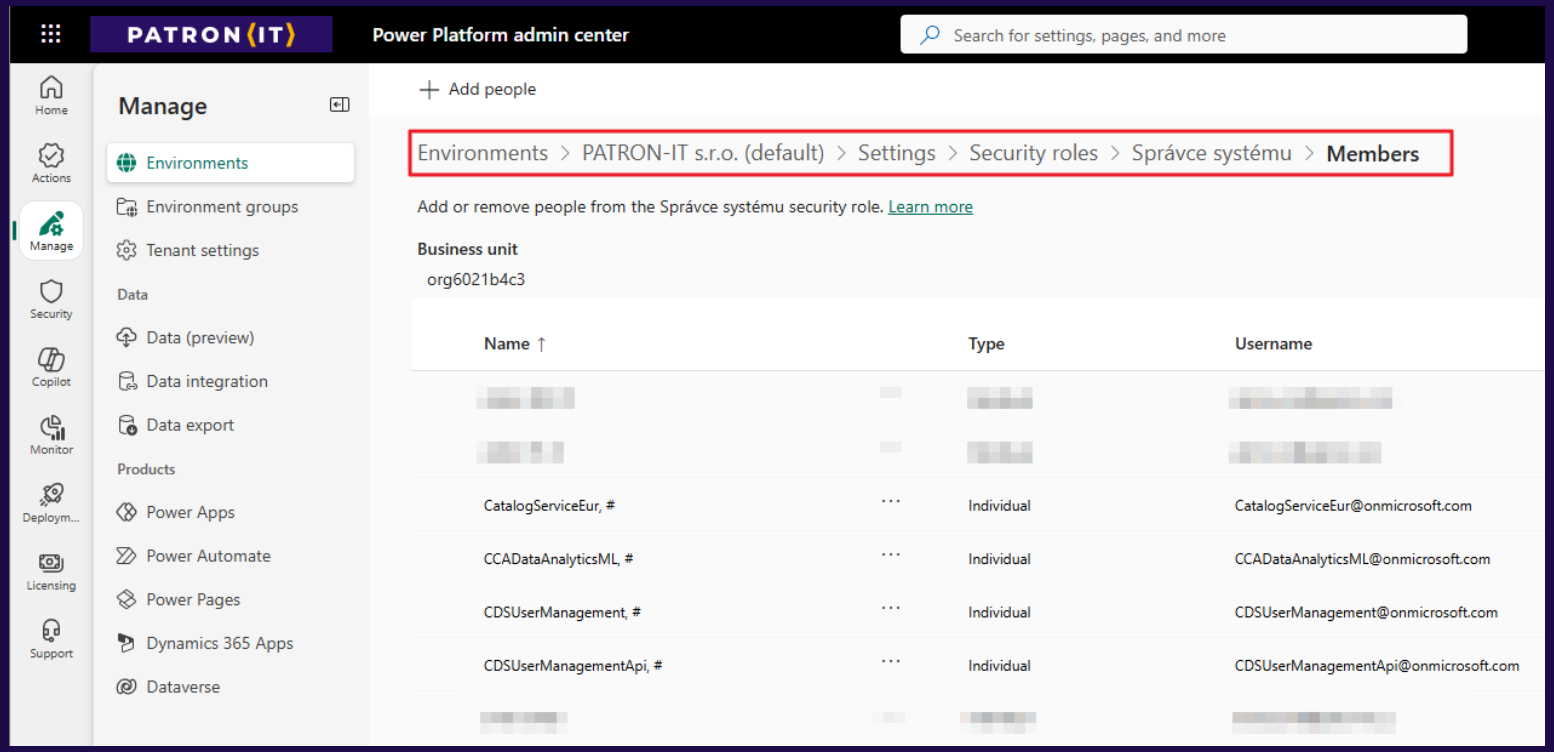
Anubis Ransomware Packs a

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

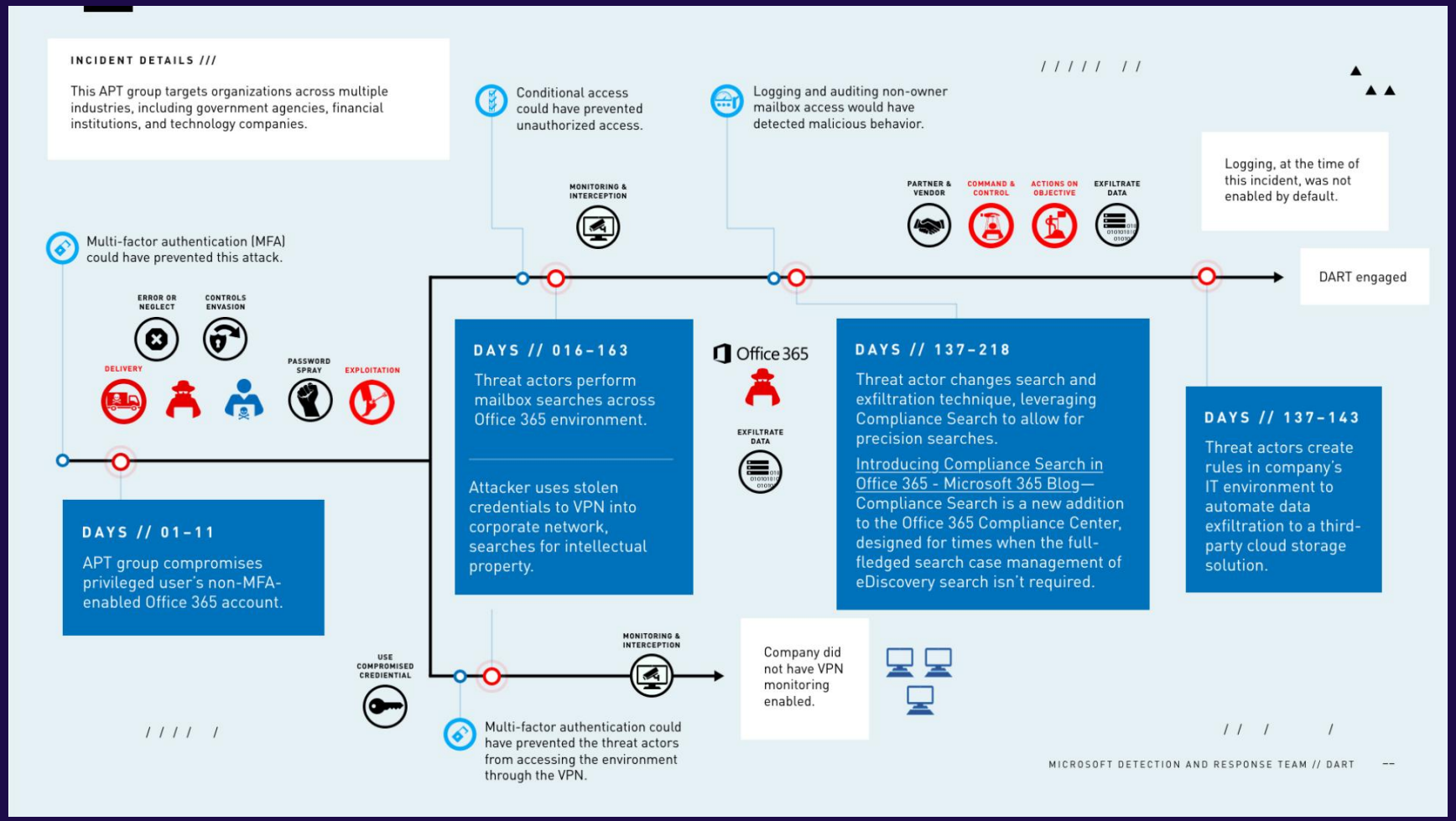
RBAC: Power Platform

RBAC: Power Platform

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

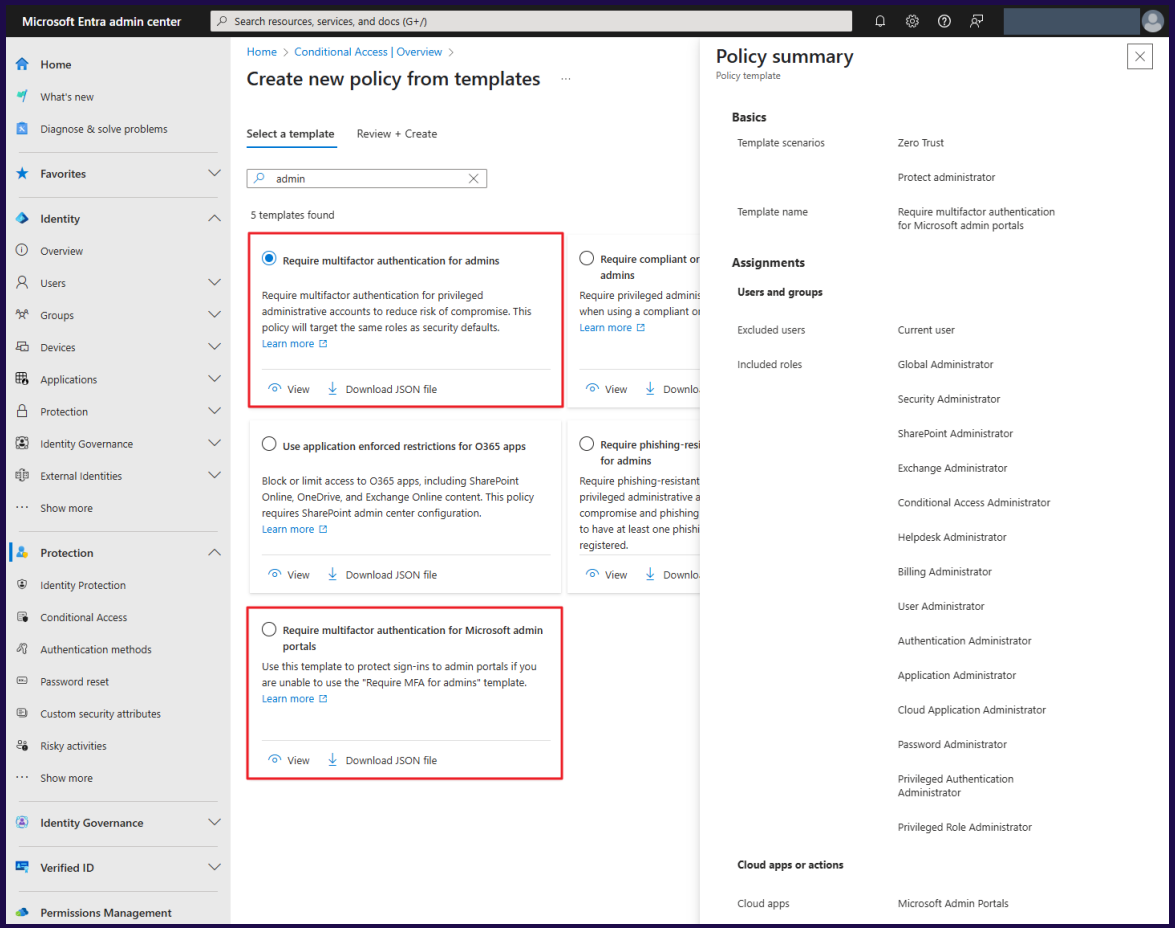


RBAC: Power Platform - Seen in the Wild

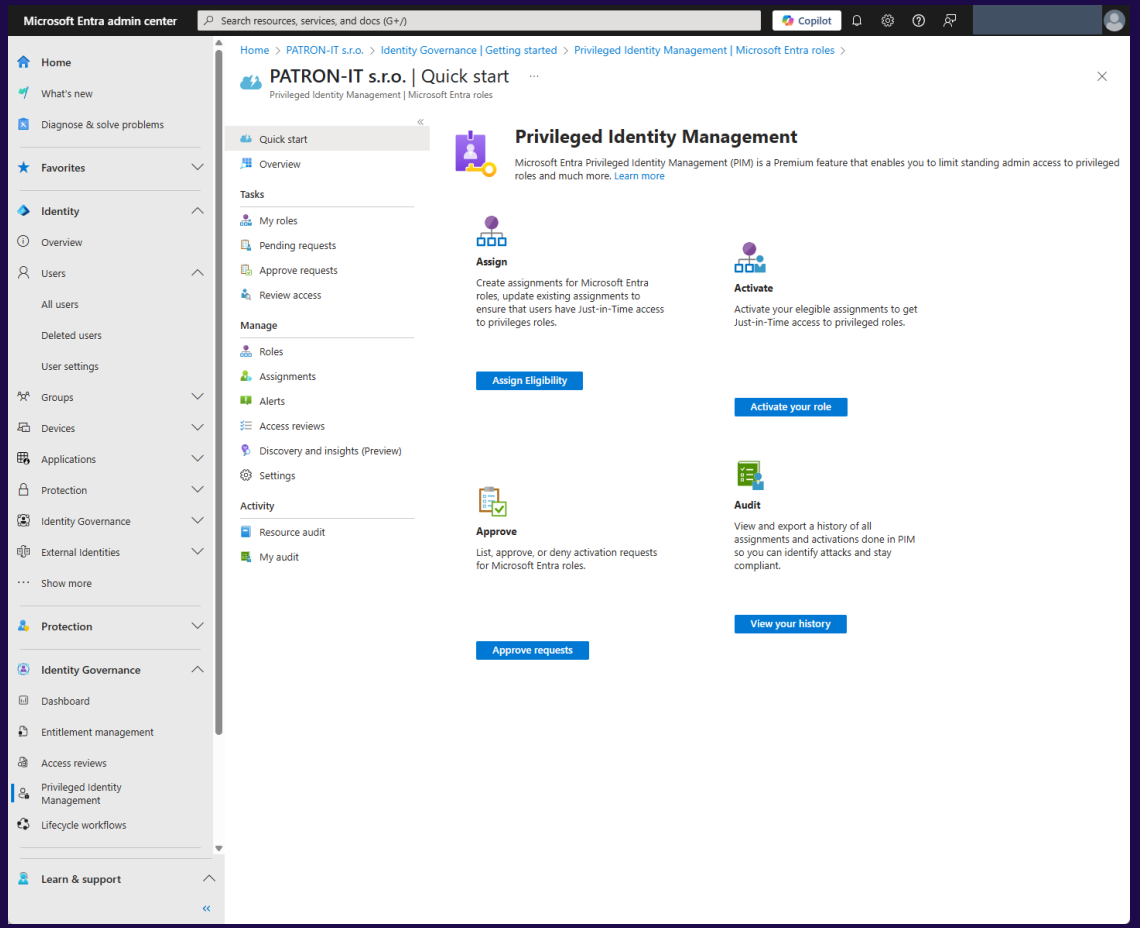


Source: https://www.microsoft.com/en-us/security/blog/wp-content/uploads/2020/03/then-there-were-six.pdf

Entra ID – RBAC – Caveats



Escapes some Conditional Access Policies



Outside of standard PIM for MS Entra Roles

RBAC: Defense

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⟩