SECTOR BRIEFINGS

October 23-24, 2024

METRO TORONTO CONVENTION CENTRE

Guardians of the OAuth Galaxy

Defending Your Organization from OAuth Application Attacks

Microsoft Security

Mangatas Tondang

Security Researcher II

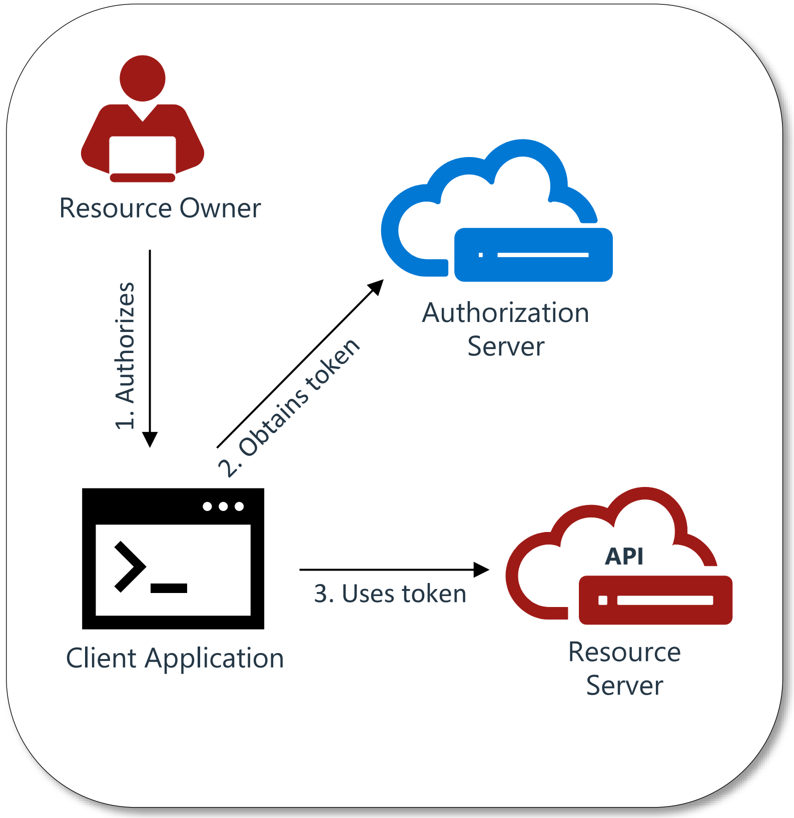
Shruti Ranjit

Senior Security Researcher

Agenda

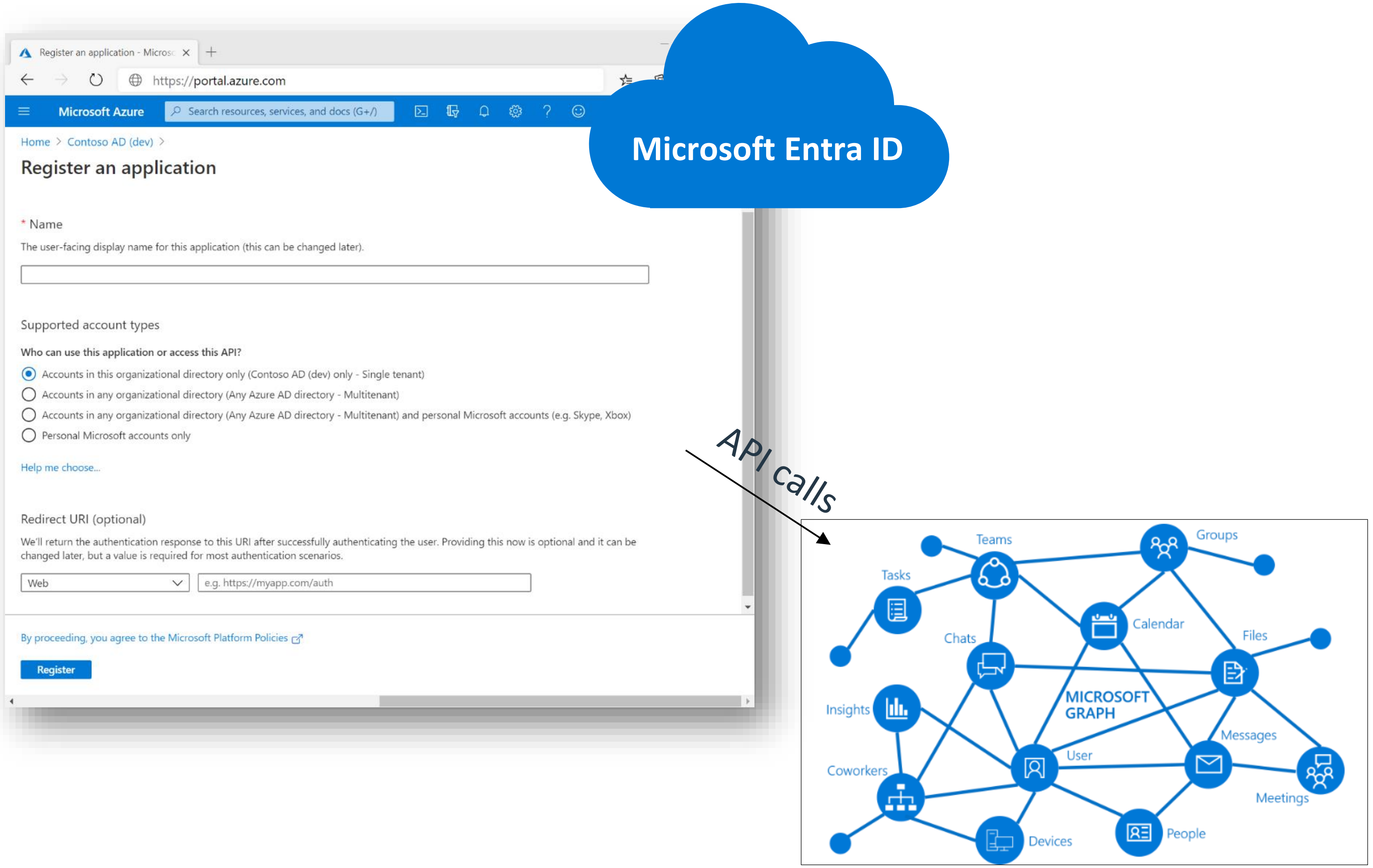
- OAuth & OAuth Application Crash Course
- OAuth Application Abuse
  1. **Consent Phishing**
  2. **Crypto Mining**
  3. **Business Email Compromise (BEC)**
  4. **Spamming Operation**
- Hunting Pointers
- Remediation Strategies
- Mitigation Strategies
- Conclusion (aka SecTor Sound Bytes)

OAuth & OAuth Application Crash Course



Simple OAuth Protocol Flow

OAuth Authorization Code Flow



Register an application

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Contoso AD (dev) only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | e.g. https://myapp.com/auth

By proceeding, you agree to the Microsoft Platform Policies

Register

Accesses user data based on
permissions associated with the application

OAuth Application Characteristics

1. Display name

- Application Display Name

2. Application (client) ID

- Unique Identifier for the Application

3. Directory (tenant) ID

- Unique identifier for the Microsoft Entra ID instance

4. Supported Account types

- Availability to other tenants

5. Redirect URIs

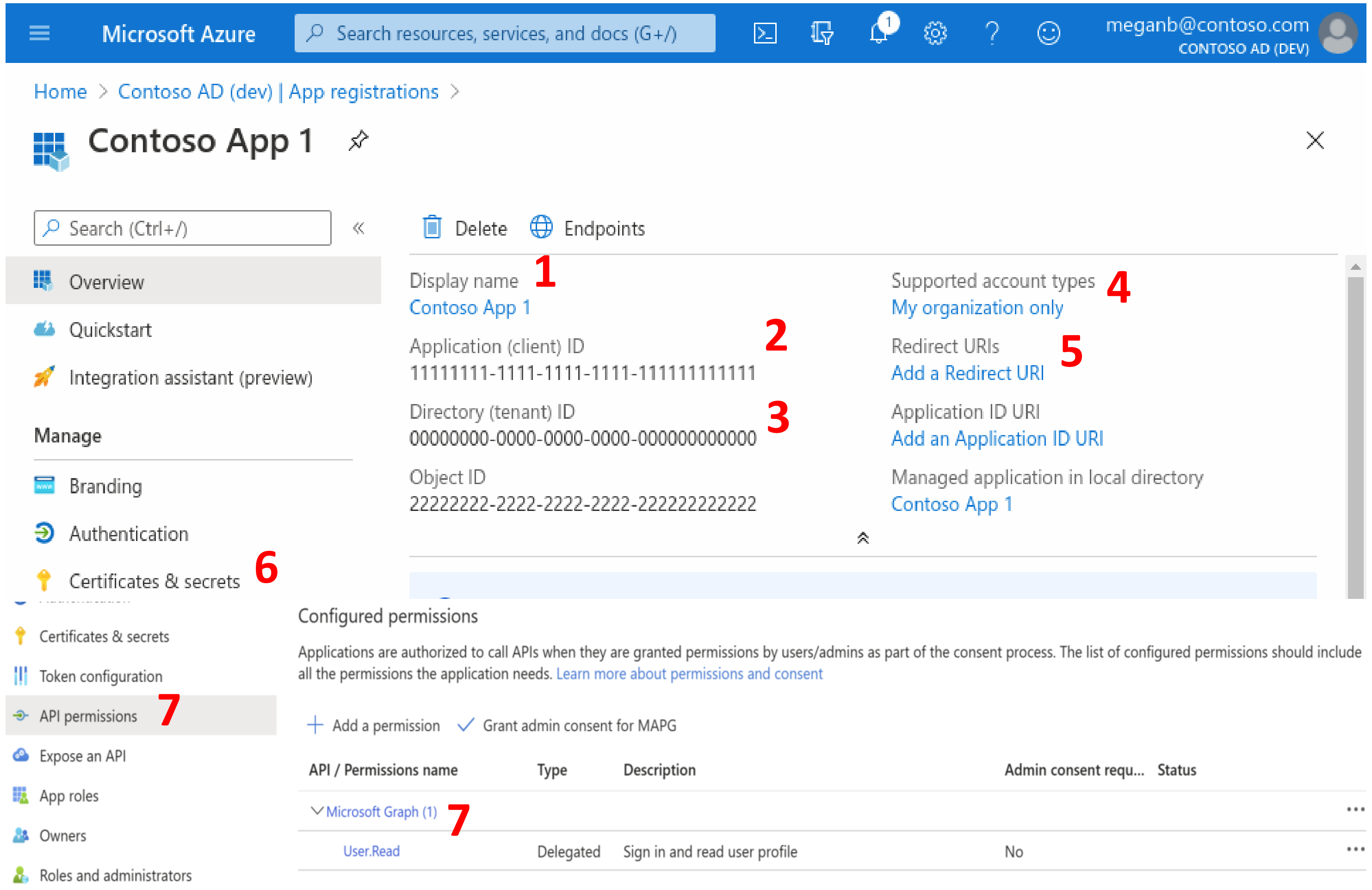
- Location where the authorization server directs the user once the app is authorized and granted necessary tokens

6. Certificates and Secrets

- Credentials that allow your confidential client applications to authenticate as itself, requiring no user interaction at runtime.

7. API permissions

- Permissions-based access to resources for authorized users and client apps accessing APIs.



Display name 1
Contoso App 1

Application (client) ID 2
11111111-1111-1111-1111-111111111111

Directory (tenant) ID 3
00000000-0000-0000-0000-000000000000

Object ID
22222222-2222-2222-2222-222222222222

Supported account types 4
My organization only

Redirect URIs 5
Add a Redirect URI

Application ID URI
Add an Application ID URI

Managed application in local directory
Contoso App 1

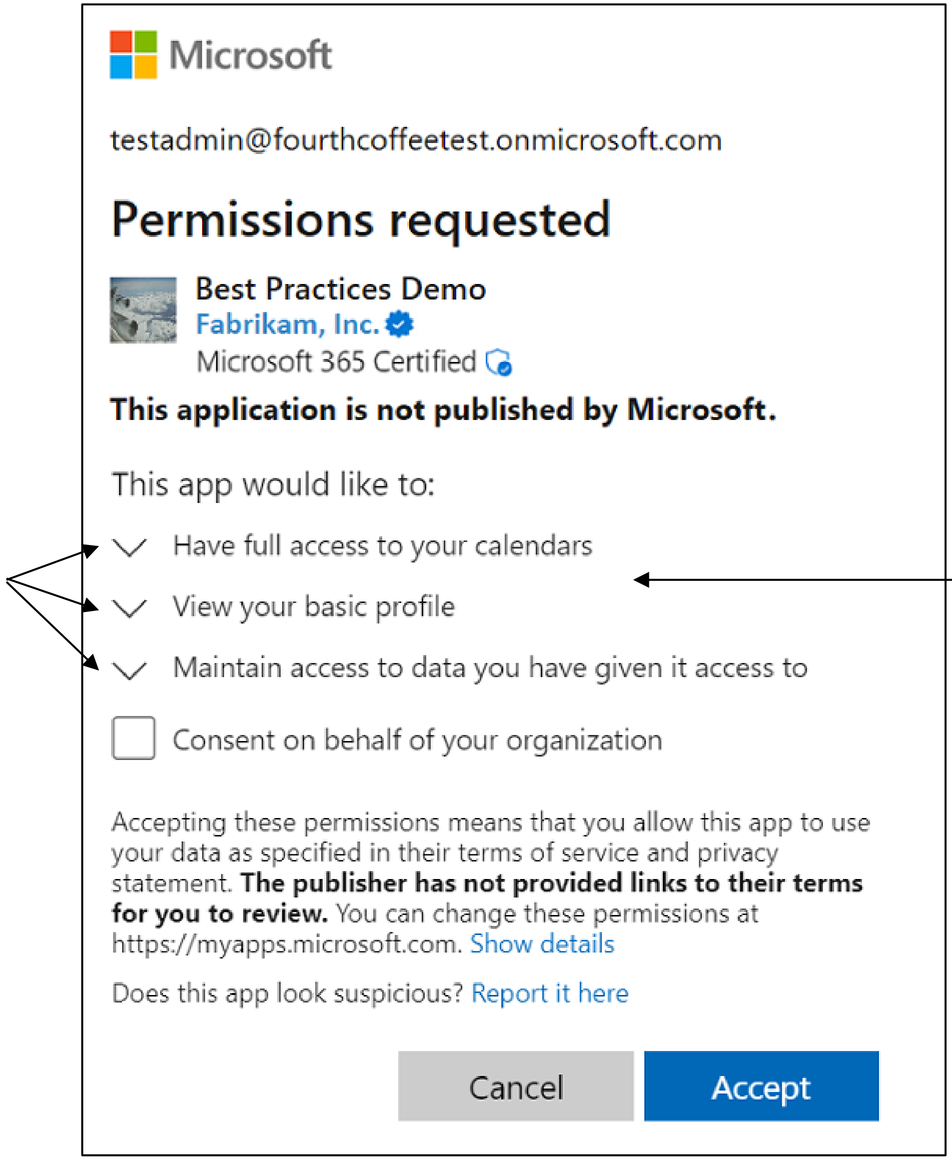
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (1) 7				
User.Read	Delegated	Sign in and read user profile	No	

OAuth Application “Consent” Operation

permissions



Microsoft

testadmin@fourthcoffeetest.onmicrosoft.com

Permissions requested

Best Practices Demo
Fabrikam, Inc.
Microsoft 365 Certified

This application is not published by Microsoft.

This app would like to:

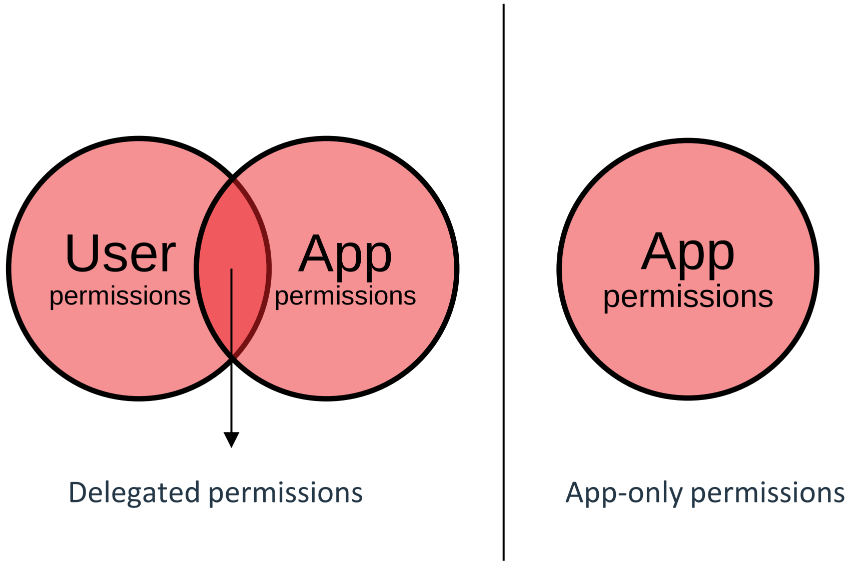
- Have full access to your calendars
- View your basic profile
- Maintain access to data you have given it access to

□ Consent on behalf of your organization

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

Does this app look suspicious? Report it here

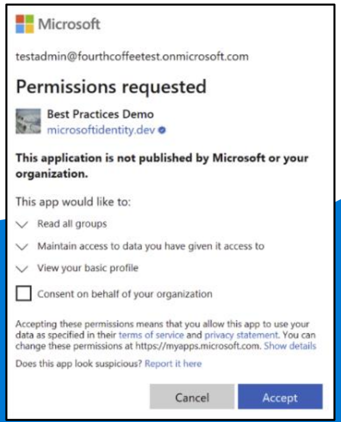
Application consent request page to user



OAuth Application Abuse

Consent Phishing

Consent Phishing Attack



Microsoft

testadmin@fourthcoffeetest.onmicrosoft.com

Permissions requested

Best Practices Demo
microsoftidentity.dev

This application is not published by Microsoft or your organization.

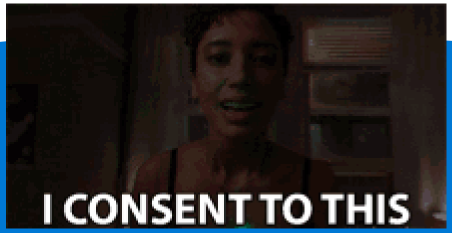
This app would like to:

- Read all groups
- Maintain access to data you have given it access to
- View your basic profile

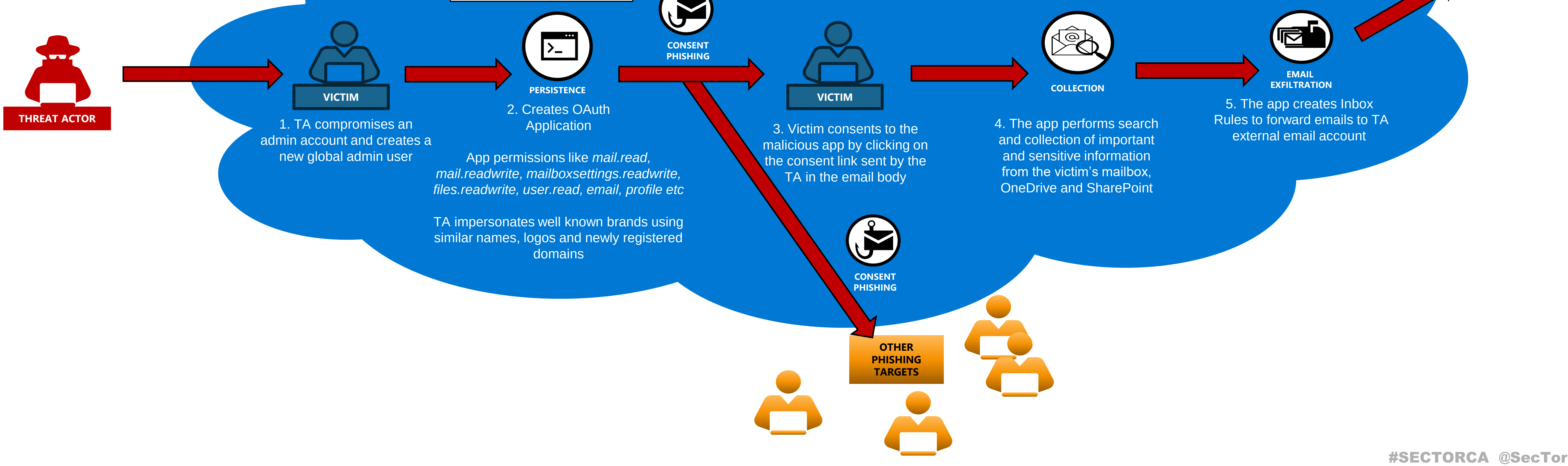
□ Consent on behalf of your organization

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

Does this app look suspicious? Report it here



Targeted Tenant



1. TA compromises an admin account and creates a new global admin user

2. Creates OAuth Application

App permissions like *mail.read, mail.readwrite, mailboxsettings.readwrite, files.readwrite, user.read, email, profile etc*

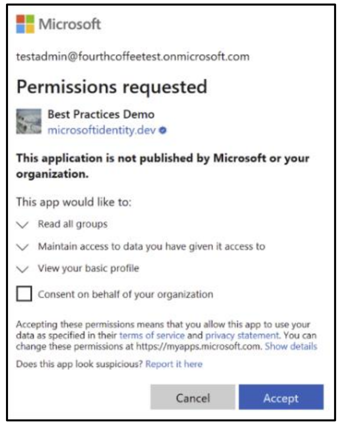
TA impersonates well known brands using similar names, logos and newly registered domains

3. Victim consents to the malicious app by clicking on the consent link sent by the TA in the email body

4. The app performs search and collection of important and sensitive information from the victim's mailbox, OneDrive and SharePoint

5. The app creates Inbox Rules to forward emails to TA external email account

Consent Phishing Attack



Microsoft

testadmin@fourthcoffeetest.onmicrosoft.com

Permissions requested

Best Practices Demo
microsoftidentity.dev

This application is not published by Microsoft or your organization.

This app would like to:

- Read all groups
- Maintain access to data you have given it access to
- View your basic profile

□ Consent on behalf of your organization

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

Does this app look suspicious? Report it here

TA Tenant

PERSISTENCE

1. Creates OAuth Applications

App permissions like: *mail.read, mail.readwrite, mailboxsettings.readwrite, mail.send, user.read, email, profile etc*

TA uses brand impersonation techniques in app used for consenting phishing

TA also creates apps to automate email sending

THREAT ACTOR

CONSENT PHISHING

Targeted Tenant

VICTIM

2. Victim consents to the malicious app through the consent link sent by the TA.

TA hides consents link in attachments such as html files. Also, the TA uses short/redirector links

COLLECTION

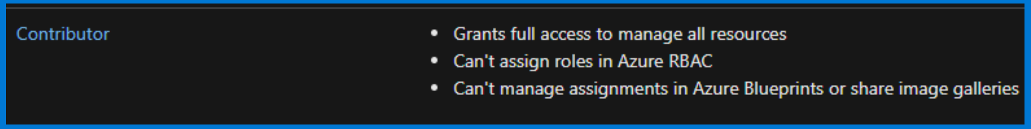
3. TA uses the app to perform collection of important and sensitive information in the victim's mailbox and user directory details

OAuth Application Abuse

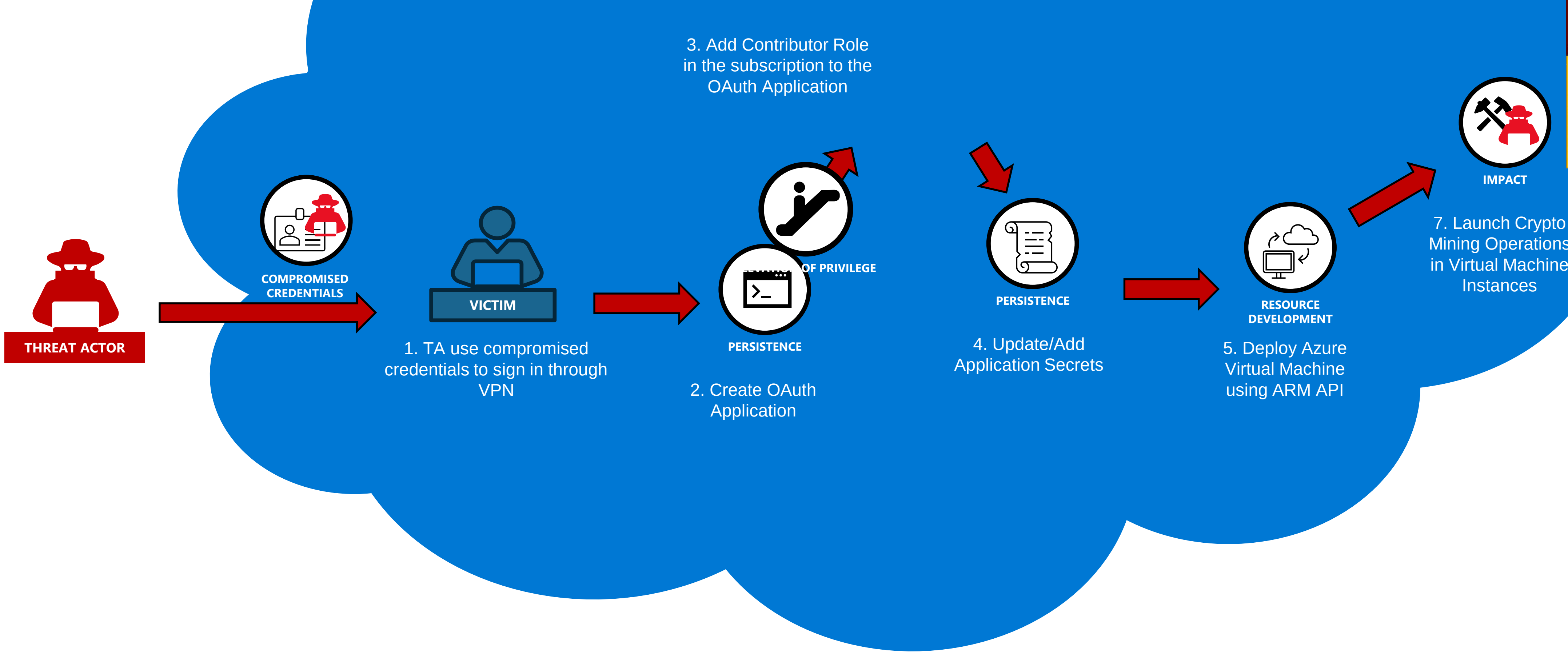
Crypto Mining

OAuth Application deploying Crypto Mining

Targeted Tenant



Contributor	• Grants full access to manage all resources • Can't assign roles in Azure RBAC • Can't manage assignments in Azure Blueprints or share image galleries



3. Add Contributor Role in the subscription to the OAuth Application

1. TA use compromised credentials to sign in through VPN

2. Create OAuth Application

4. Update/Add Application Secrets

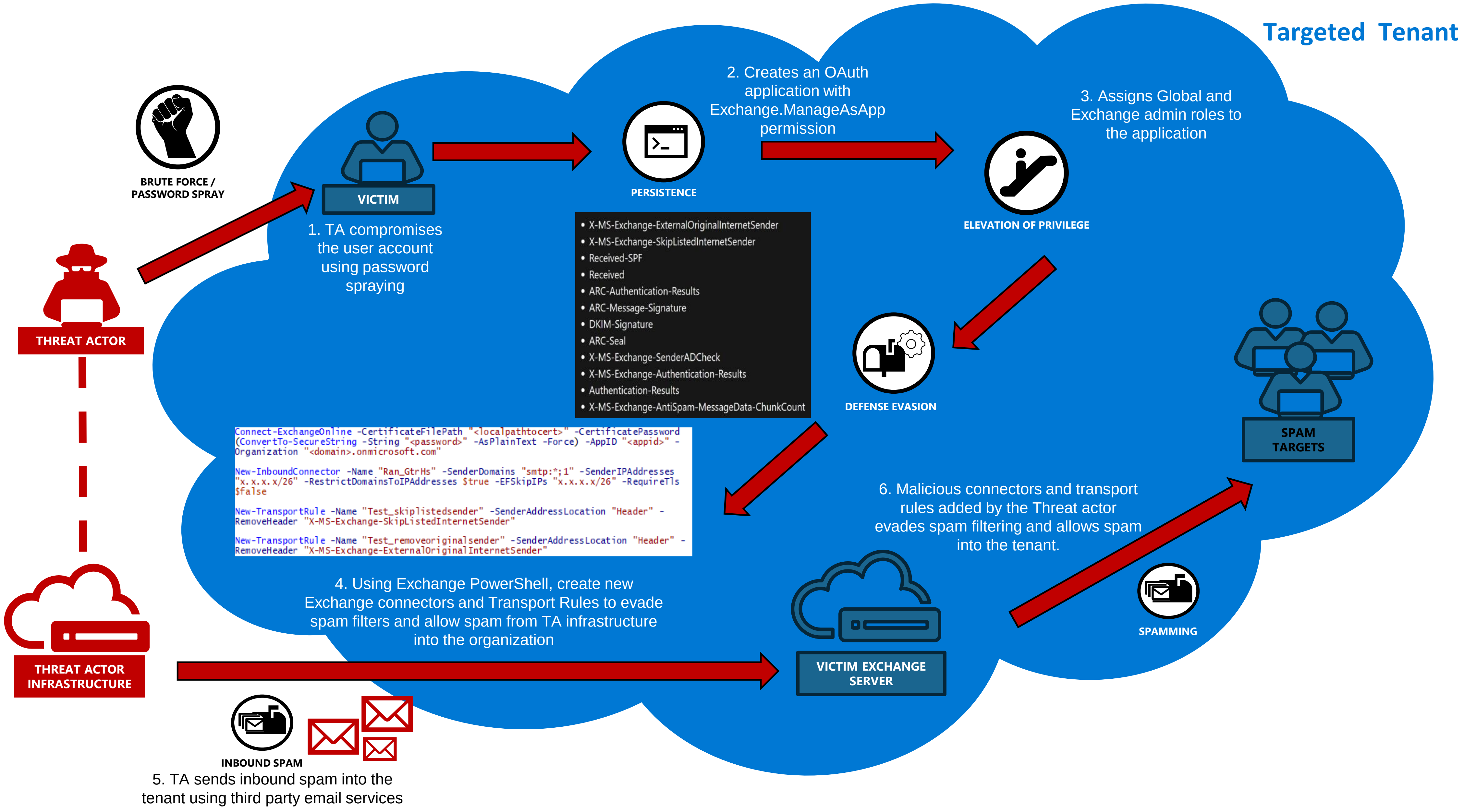
5. Deploy Azure Virtual Machine using ARM API

7. Launch Crypto Mining Operations in Virtual Machine Instances

OAuth Application Abuse

Spam

OAuth Application as Proxy for Spamming



1. TA compromises the user account using password spraying

2. Creates an OAuth application with Exchange.ManageAsApp permission

3. Assigns Global and Exchange admin roles to the application

- X-MS-Exchange-ExternalOriginalInternetSender
- X-MS-Exchange-SkipListedInternetSender
- Received-SPF
- Received
- ARC-Authentication-Results
- ARC-Message-Signature
- DKIM-Signature
- ARC-Seal
- X-MS-Exchange-SenderADCheck
- X-MS-Exchange-Authentication-Results
- Authentication-Results
- X-MS-Exchange-AntiSpam-MessageData-ChunkCount

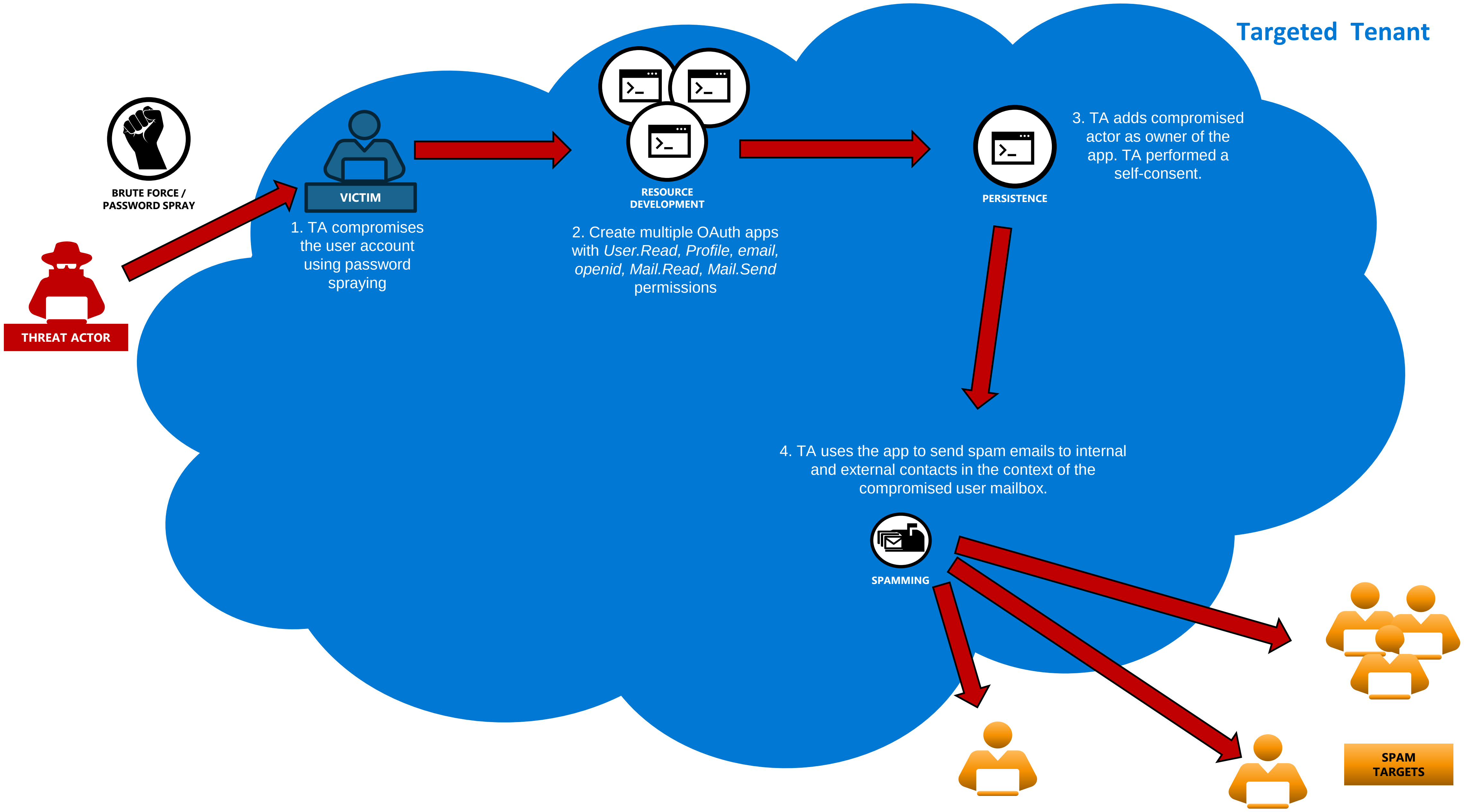
```
Connect-ExchangeOnline -CertificateFilePath "<localpathtocert>" -CertificatePassword
(ConvertTo-SecureString -String "<password>" -AsPlainText -Force) -AppID "<appid>" -
Organization "<domain>.onmicrosoft.com"

New-InboundConnector -Name "Ran_GtrHs" -SenderDomains "smtp:*;1" -SenderIPAddresses
"x.x.x.x/26" -RestrictDomainsToIPAddresses $true -EFSkipIPs "x.x.x.x/26" -RequireTls
$false

New-TransportRule -Name "Test_skiplistedsender" -SenderAddressLocation "Header" -
RemoveHeader "X-MS-Exchange-SkipListedInternetSender"

New-TransportRule -Name "Test_removeoriginalsender" -SenderAddressLocation "Header" -
RemoveHeader "X-MS-Exchange-ExternalOriginalInternetSender"
```

4. Using Exchange PowerShell, create new Exchange connectors and Transport Rules to evade spam filters and allow spam from TA infrastructure into the organization

5. TA sends inbound spam into the tenant using third party email services

6. Malicious connectors and transport rules added by the Threat actor evades spam filtering and allows spam into the tenant.

OAuth Application as Spam Sender



1. TA compromises the user account using password spraying

2. Create multiple OAuth apps with *User.Read, Profile, email, openid, Mail.Read, Mail.Send* permissions

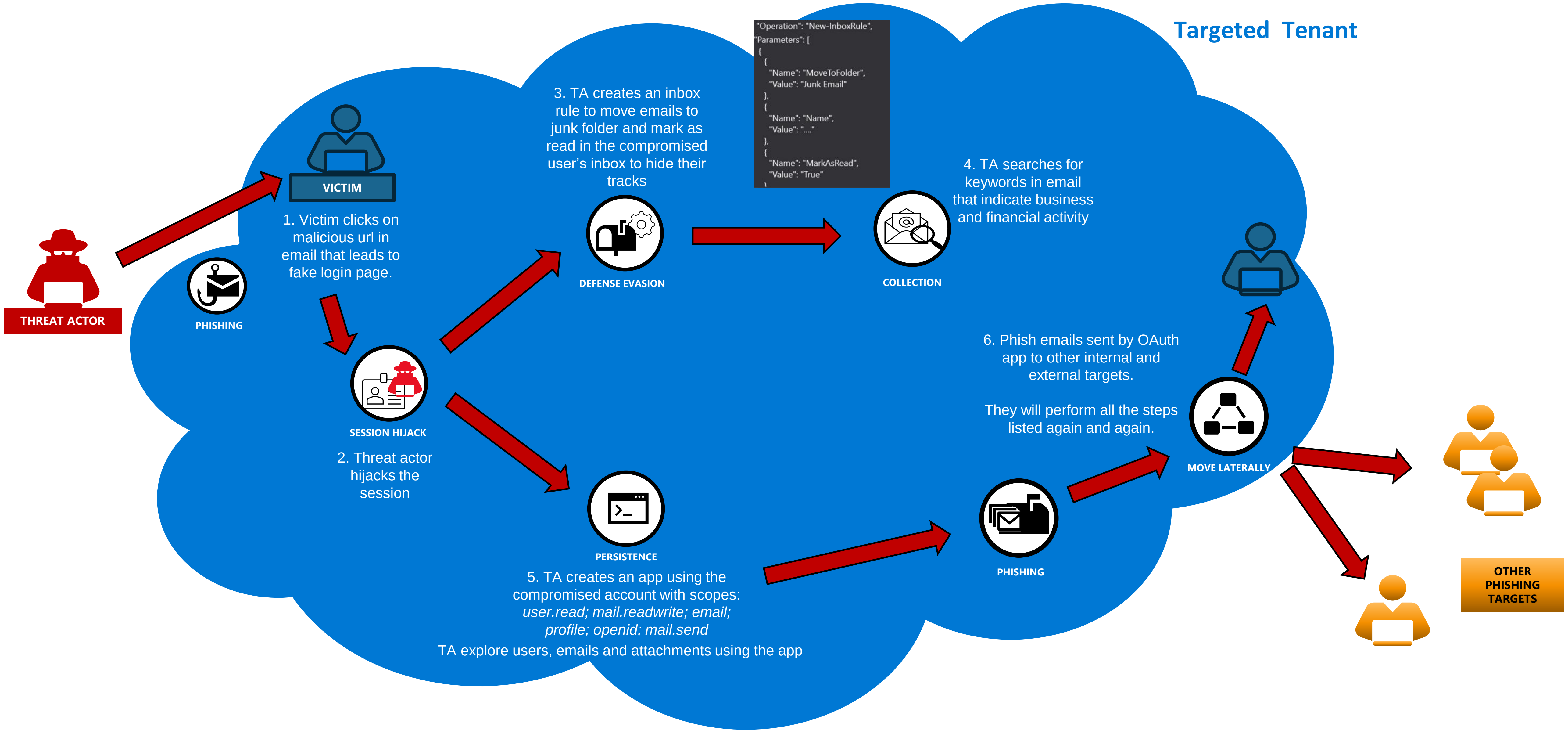
3. TA adds compromised actor as owner of the app. TA performed a self-consent.

4. TA uses the app to send spam emails to internal and external contacts in the context of the compromised user mailbox.

OAuth Application Abuse

BEC & Phishing

OAuth Application in BEC and Phishing



1. Victim clicks on malicious url in email that leads to fake login page.

2. Threat actor hijacks the session

3. TA creates an inbox rule to move emails to junk folder and mark as read in the compromised user's inbox to hide their tracks

```
 "Operation": "New-InboxRule",
"Parameters": [
 {
   {
     "Name": "MoveToFolder",
     "Value": "Junk Email"
   },
   {
     "Name": "Name",
     "Value": "...."
   },
   {
     "Name": "MarkAsRead",
     "Value": "True"
   }
```

4. TA searches for keywords in email that indicate business and financial activity

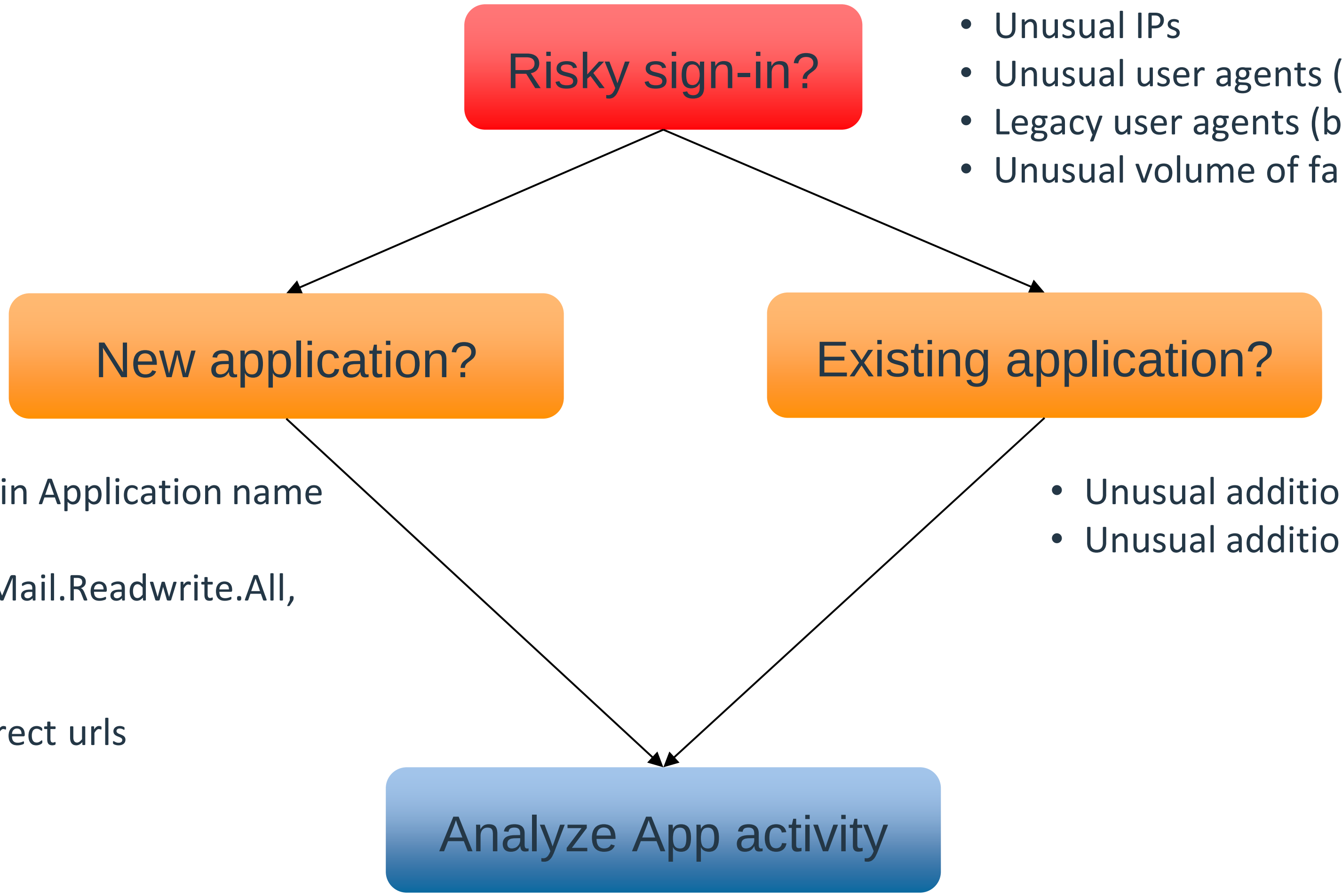
5. TA creates an app using the compromised account with scopes: *user.read; mail.readwrite; email; profile; openid; mail.send*

TA explore users, emails and attachments using the app

6. Phish emails sent by OAuth app to other internal and external targets.

They will perform all the steps listed again and again.

Hunting Pointers



Risky sign-in?

- Unusual location
- Unusual IPs
- Unusual user agents (ExchangeServices, Python,)
- Legacy user agents (bav2ropc)
- Unusual volume of failed sign-in attempts

New application?

- Suspicious naming patterns in Application name
- Brand logo impersonation
- High-level permissions like Mail.Readwrite.All, Mail.Send, Files.ReadWrite, Exchange.ManageAsApp
- Suspicious or malicious redirect urls

Existing application?

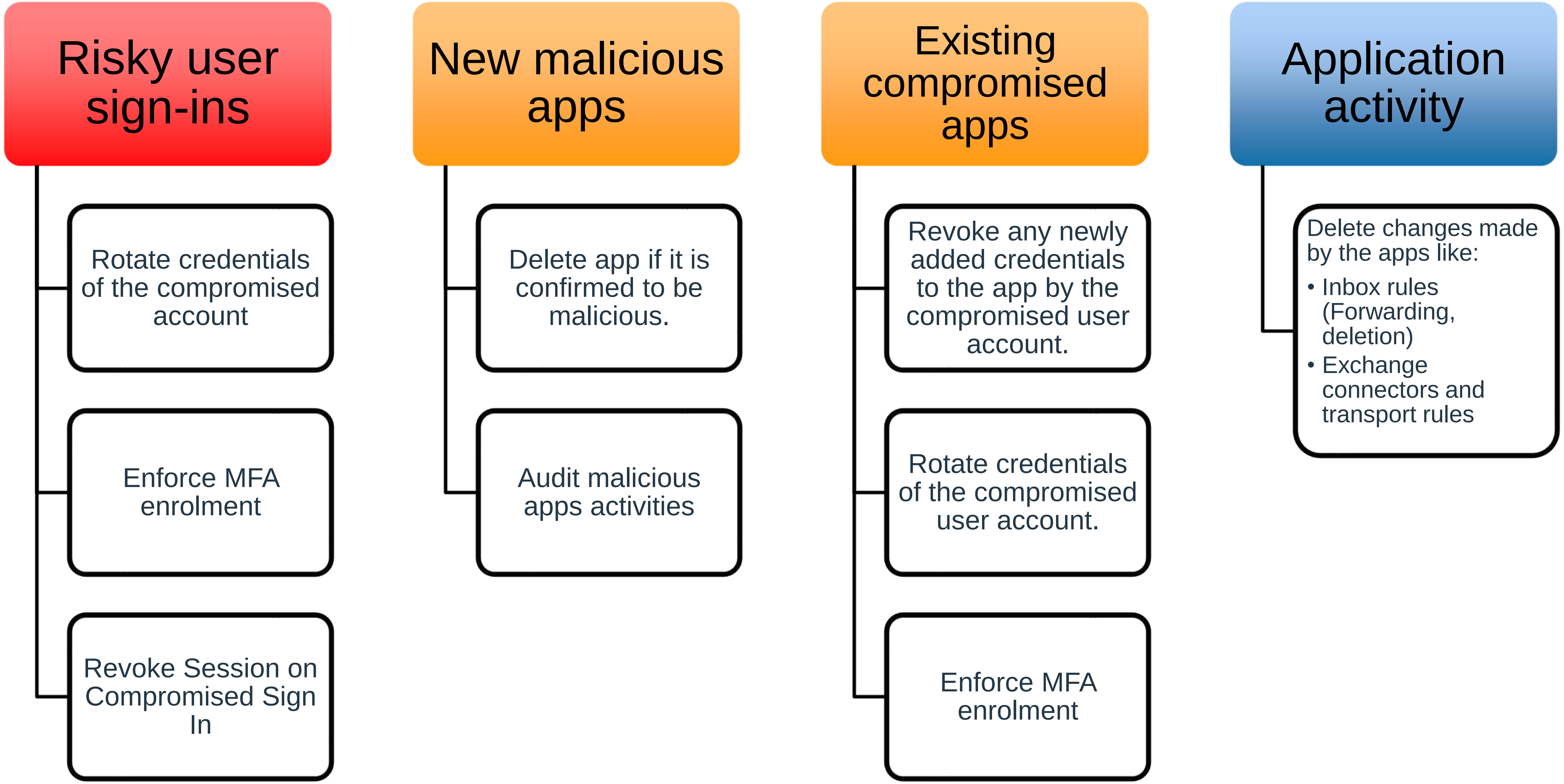
- Unusual addition of new secrets or credentials to app
- Unusual addition of new permissions to an app with admin consent

Analyze App activity

Application activity through workload accesses

- Email reads, sends, inbox rules changes
- File access and downloads
- Cloud assets creation or modification

Remediation Strategies



Risky user sign-ins

- Rotate credentials of the compromised account
- Enforce MFA enrolment
- Revoke Session on Compromised Sign In

New malicious apps

- Delete app if it is confirmed to be malicious.
- Audit malicious apps activities

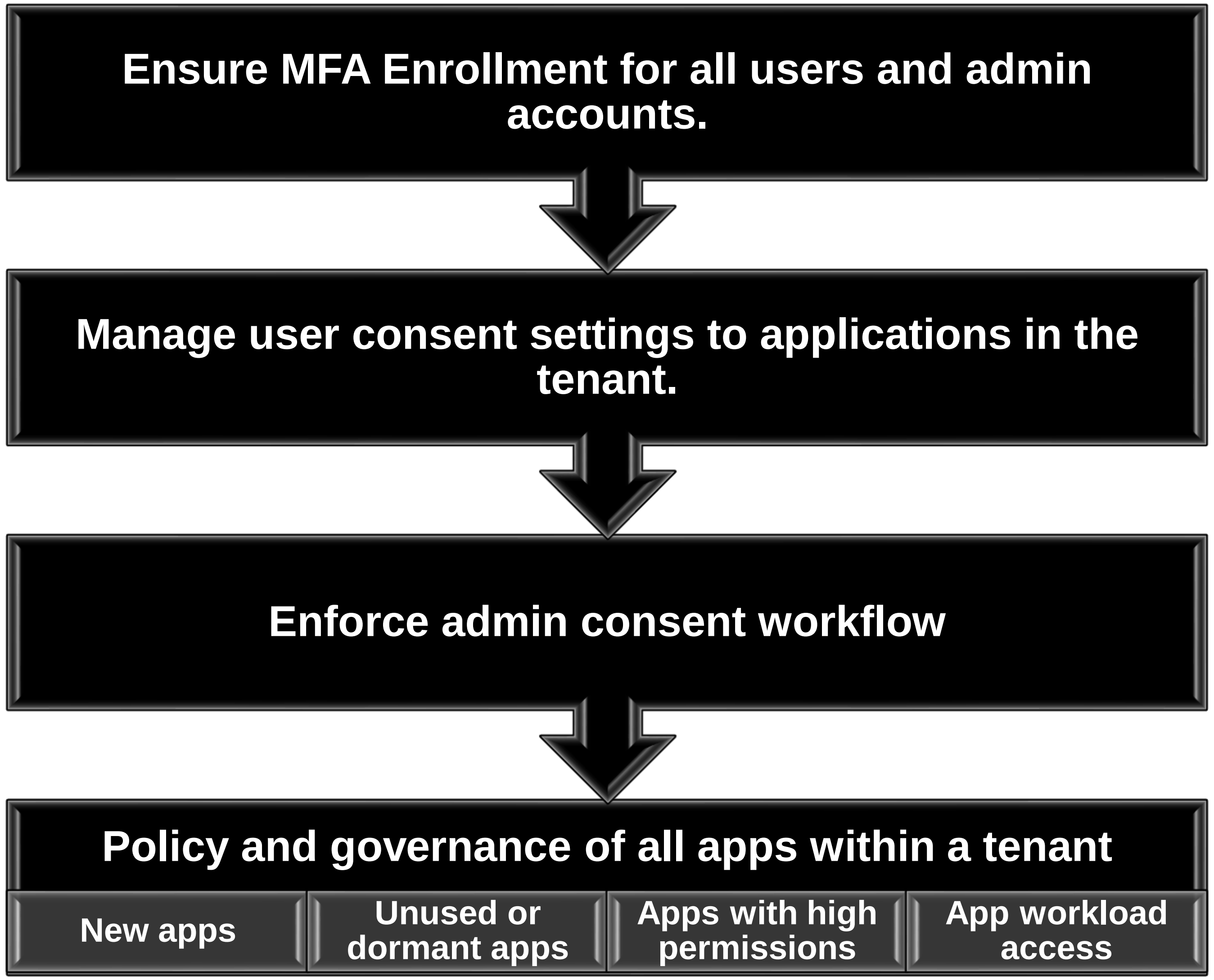
Existing compromised apps

- Revoke any newly added credentials to the app by the compromised user account.
- Rotate credentials of the compromised user account.
- Enforce MFA enrolment

Application activity

- Delete changes made by the apps like:
  - Inbox rules (Forwarding, deletion)
  - Exchange connectors and transport rules

Mitigation Strategies



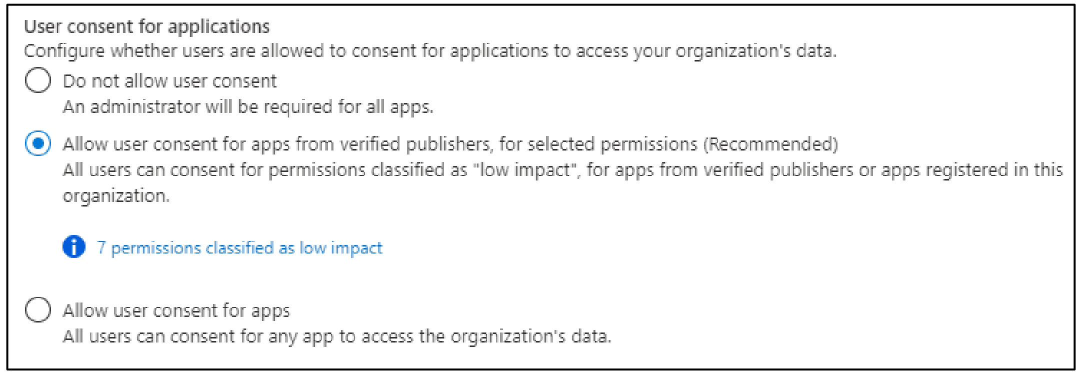
Ensure MFA Enrollment for all users and admin accounts.

Manage user consent settings to applications in the tenant.

Enforce admin consent workflow

Policy and governance of all apps within a tenant

New apps	Unused or dormant apps	Apps with high permissions	App workload access



User consent for applications

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

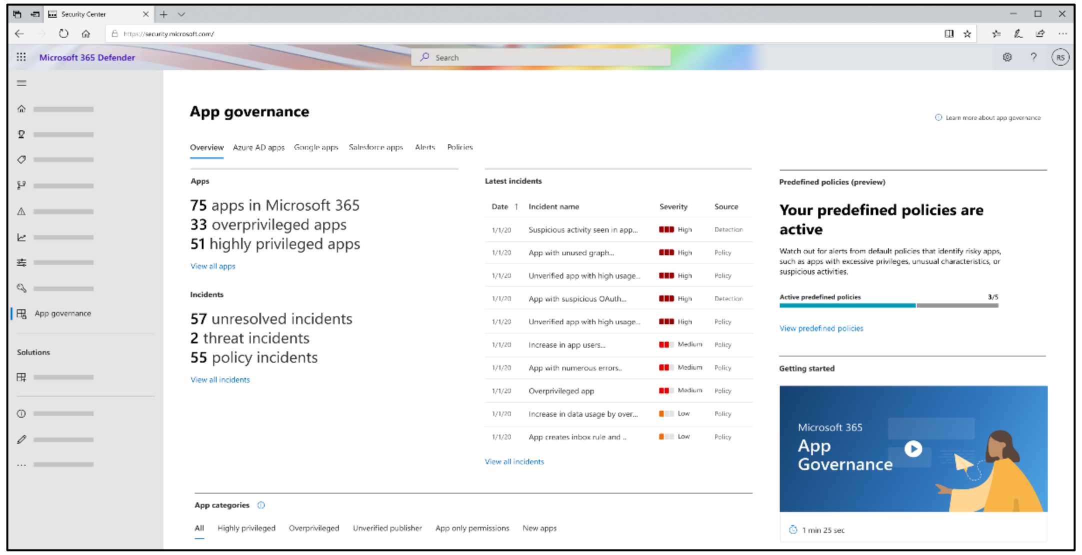
○ Do not allow user consent
An administrator will be required for all apps.

● 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.

7 permissions classified as low impact

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

App consent settings for users and admin in Microsoft Entra ID



App governance

Apps

75 apps in Microsoft 365
33 overprivileged apps
51 highly privileged apps

View all apps

Incidents

57 unresolved incidents
2 threat incidents
55 policy incidents

View all incidents

Latest incidents

Date	Incident name	Severity	Source
1/1/20	Suspicious activity seen in app...	High	Detection
1/1/20	App with unused graph...	High	Policy
1/1/20	Unverified app with high usage...	High	Policy
1/1/20	App with suspicious OAuth...	High	Detection
1/1/20	Unverified app with high usage...	High	Policy
1/1/20	Increase in app users...	Medium	Policy
1/1/20	App with numerous errors..	Medium	Policy
1/1/20	Overprivileged app	Medium	Policy
1/1/20	Increase in data usage by over...	Low	Policy
1/1/20	App creates inbox rule and ..	Low	Policy

View all incidents

Predefined policies (preview)

Your predefined policies are active

Watch out for alerts from default policies that identify risky apps, such as apps with excessive privileges, unusual characteristics, or suspicious activities.

Active predefined policies 3/5

View predefined policies

Getting started

Microsoft 365 App Governance

1 min 25 sec

App categories

All · Highly privileged · Overprivileged · Unverified publisher · App only permissions · New apps

Microsoft Defender for Cloud Apps supports application threat detections and policy governance in the tenant.

SecTor Sound Bytes

REMEMBER TO…

- Familiarize with the OAuth application mechanisms and learn deployment best practices
- Learn about growing threat posed by OAuth application exploitation and their common TTPs
- Prioritize security measures and controls against evolving OAuth application related threats while keep exceling basics security measures such as identity monitoring, MFA implementation and user awareness training

SECTOR
BRIEFINGS
October 23-24, 2024
METRO TORONTO CONVENTION CENTRE

Thank you!

SECTOR BRIEFINGS

Resources

- Threat actors misuse OAuth applications to automate financially driven attacks | Microsoft Security Blog
- Investigate and remediate risky OAuth apps - Microsoft Defender for Cloud Apps | Microsoft Learn
- App governance in Microsoft Defender for Cloud Apps and Microsoft Defender XDR - Microsoft Defender for Cloud Apps | Microsoft Learn