



VIRTUAL SEMINAR

Persisting Unseen: Attacker Methods of Infesting Entra ID

Katie Knowles

Cloud Security Researcher,
Datadog



DATADOG

#RSAC

Purpose

Provide a clear overview of
Entra ID attack techniques
beyond initial compromise.

*Links & recommended
reading at the end!*

Katie Knowles

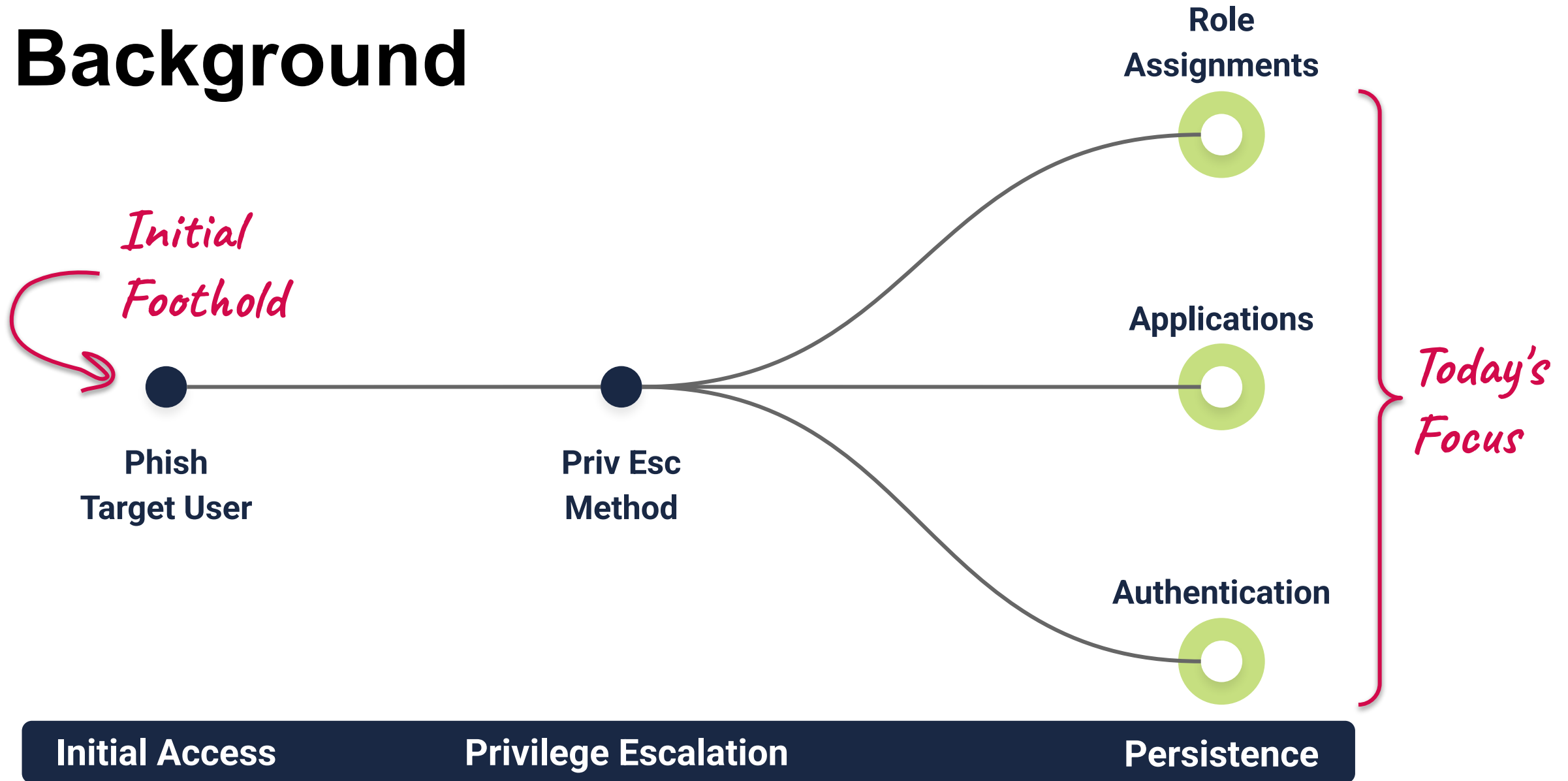
Cloud Security Researcher, Datadog

Previously:

- *Incident response*
- *Security engineering*
- *Penetration testing*

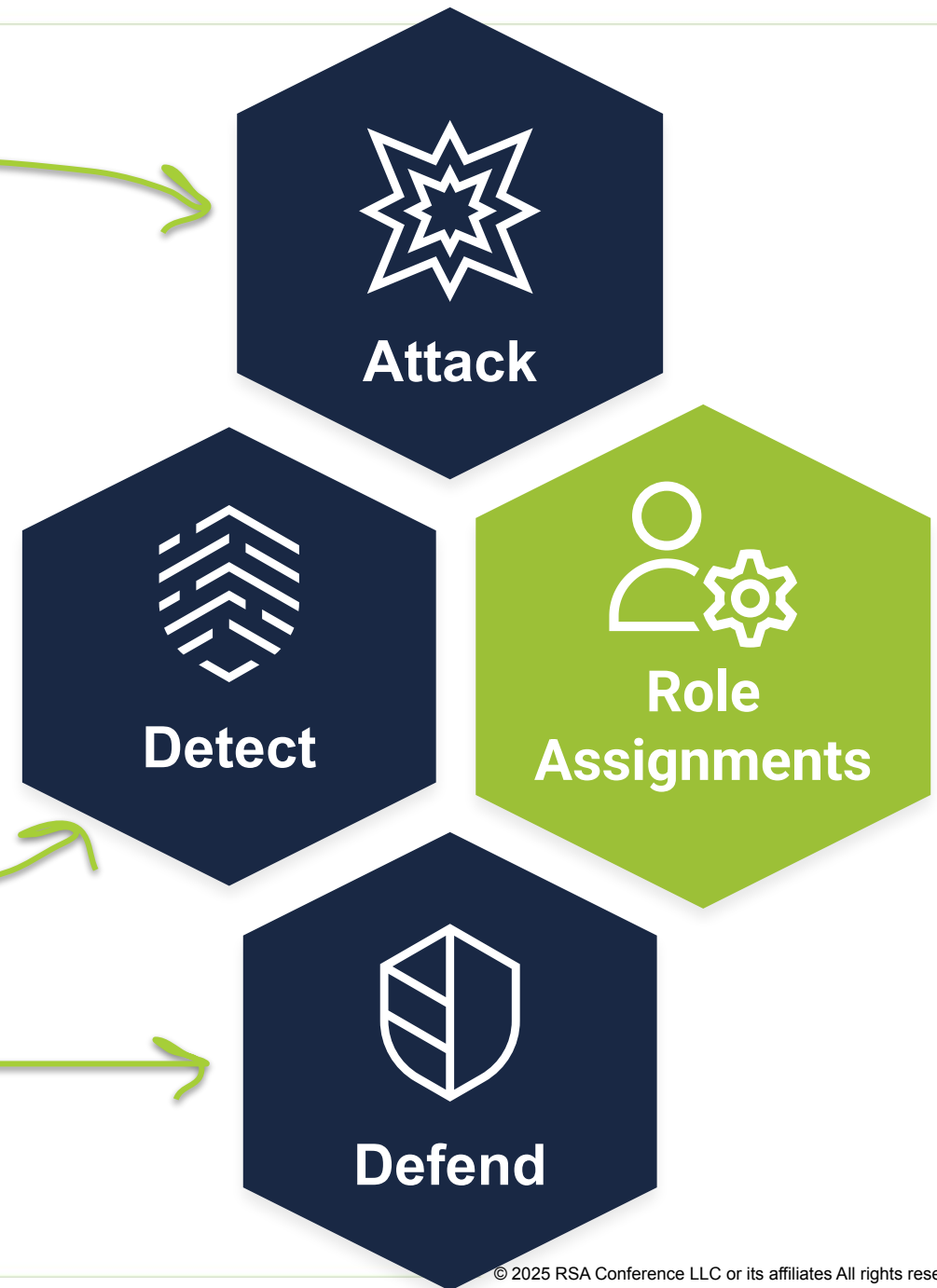


Background



Outcomes

1. Understand Entra ID **attack** methods for persistence:
 - a. **Current** in-the-wild techniques
 - b. **Future** evolution of techniques
2. **Detect** these techniques
3. Actionable steps to **defend** against these techniques



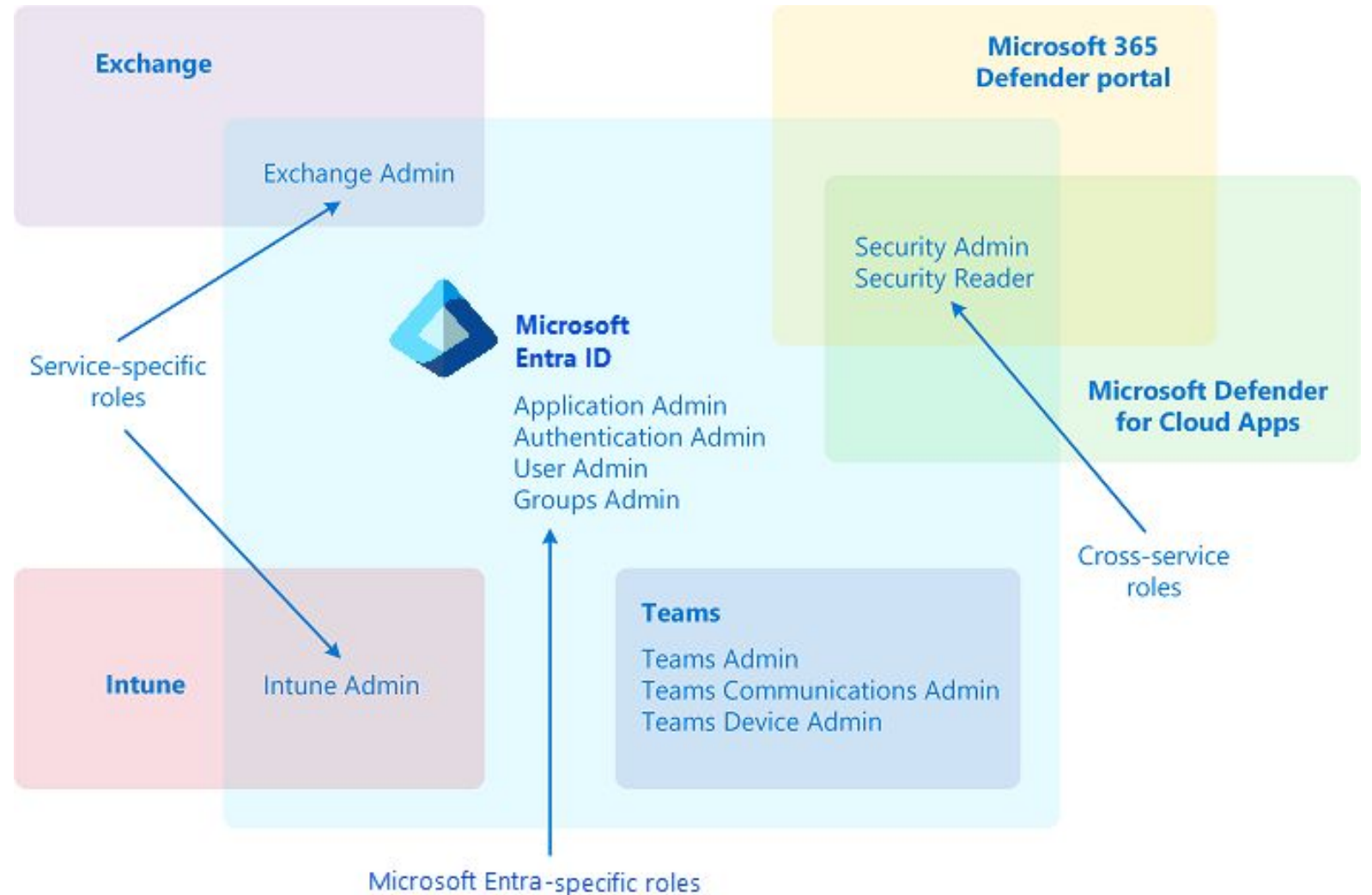


Role Assignments

Entra ID Roles


provide permissions to manage users, as well as settings like trusted domains and authentication.

This makes Entra ID the core of role assignments in Microsoft's cloud, and a powerful target for attackers.



Attack: Privileged Role Assignments

- * Microsoft identifies privileged as:
 - 20+ built-in roles
 - 10+ custom role permissions
- * These manage directory settings, applications, credentials, authentication, and authorization
- * Attackers may:
 - Target users with these roles
 - Assign these roles to evade detection of well-known roles like "Global Administrator"



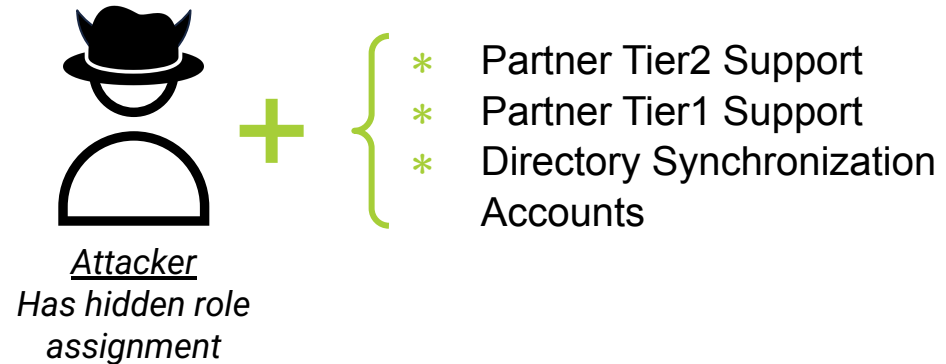
Role	↕	Description	Privileged ↕
<input type="checkbox"/> Application Administrator		Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED
<input type="checkbox"/> Application Developer		Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED
<input type="checkbox"/> Attribute Provisioning Ad...		Read and edit the provisioning configuration of all active custom security attributes for an application.	PRIVILEGED
<input type="checkbox"/> Attribute Provisioning Rea...		Read the provisioning configuration of all active custom security attributes for an application.	PRIVILEGED
<input type="checkbox"/> Authentication Administra...		Can access to view, set and reset authentication method information for any non-admin user.	PRIVILEGED
<input type="checkbox"/> Authentication Extensibilit...		Customize sign in and sign up experiences for users by creating and managing custom authentication extensions.	PRIVILEGED
<input type="checkbox"/> B2C IEF Keyset Administra...		Can manage secrets for federation and encryption in the Identity Experience Framework (IEF).	PRIVILEGED

Attack: Hidden Privileged Roles

Certain privileged roles are hidden from the Azure Portal:

- Partner Tier2 Support
- Partner Tier1 Support
- Directory Synchronization Accounts

Attackers with Global Admin or Privileged Role Admin may assign these roles to conceal their access.



Administrative roles
Administrative roles are used for granting access for privileged actions in Microsoft Entra ID. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Microsoft Entra ID not related to application configuration. [Learn more.](#)

[Learn more about Microsoft Entra ID role-based access control](#)

Search: partner tier [X] [Add filters]

Role	↑↓	Description	Privileged
No roles found			

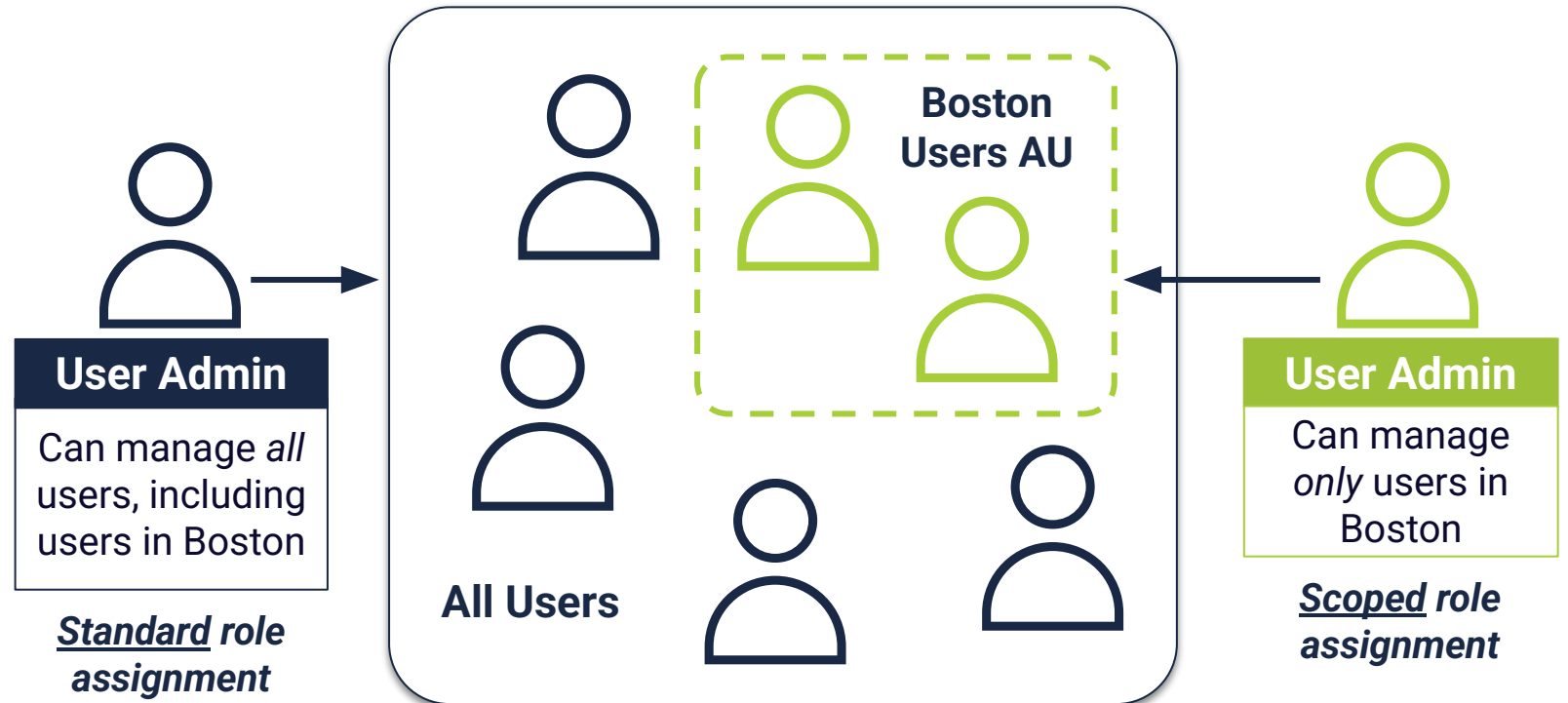
Search: directory sync [X] [Add filters]

Role	↑↓	Description	Privileged
No roles found			

Administrative Units (AUs) make role assignments more flexible by allowing roles to be scoped over a subset of users.

AUs can also be:

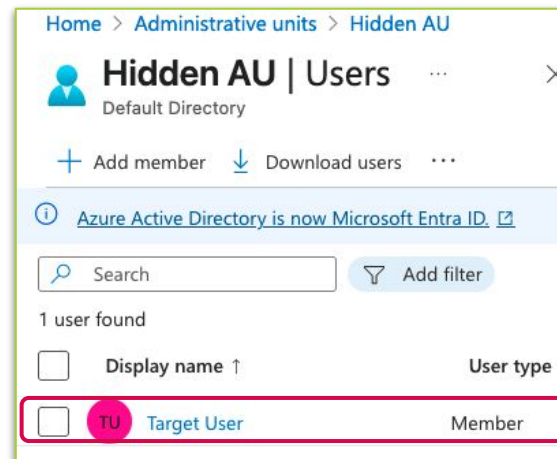
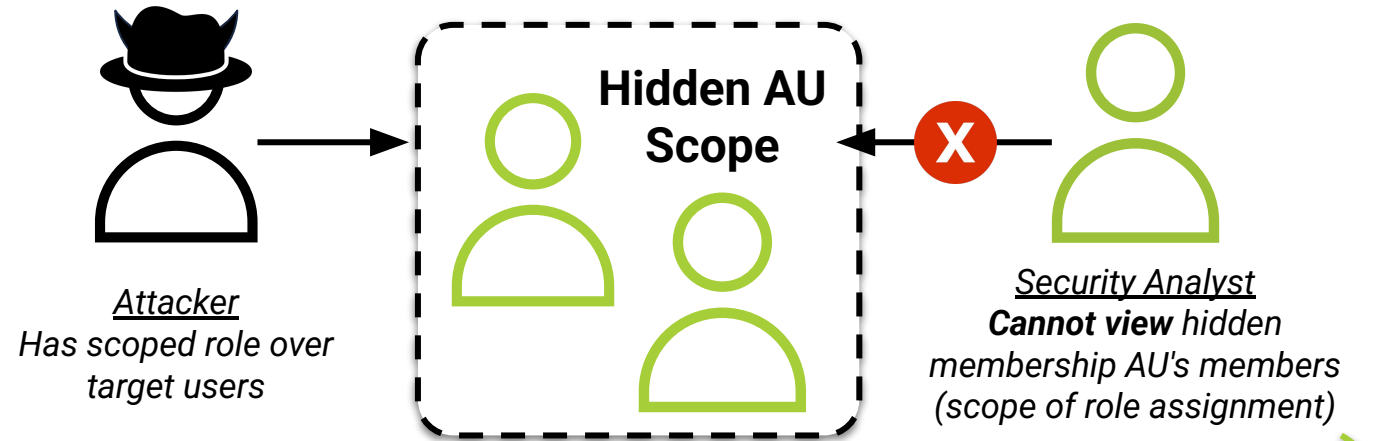
- ***Restricted:***
Protect VIP users
- ***Hidden:***
Hide AU members



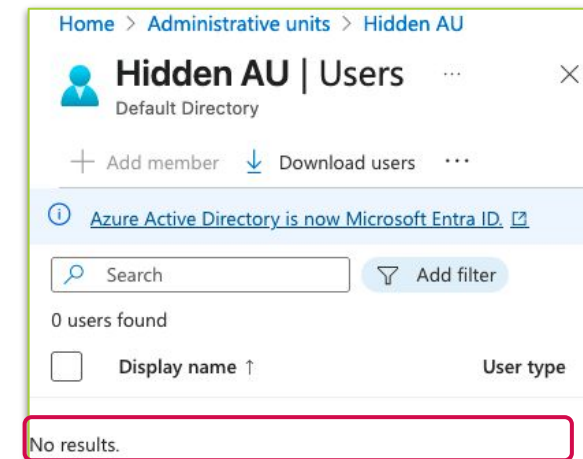
Attack: Hidden AU Members

Administrative Units (AUs) allow scoped role assignments.

Hidden AU members can be used by an attacker with Global Admin or Privileged Role Admin to conceal the scope of a privileged role assignment.



View as Global Administrator



View as Security Administrator



Detect: Suspicious Role Assignments

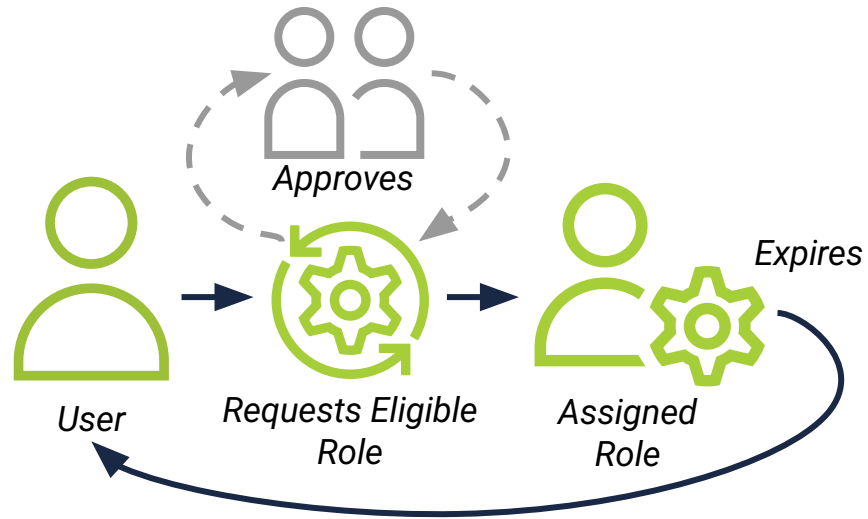
Monitor role assignment event names:

- * "Add member to role"
- * "Add eligible member to role"
- * "Add scoped member to role"
- * "Add member to role scoped over Restricted Management Administrative Unit"
- * "Add member to role completed (PIM activation)"
- * "Update role definition"

Monitor assignments to hidden and privileged roles:

- * Hidden Roles
 - Partner Tier2 Support
 - Partner Tier1 Support
 - Directory Synchronization Accounts
- * Privileged Roles
 - Privileged role assignments as classified by Microsoft

Defend: Manage Role Assignments



Consider Privileged Identity Management (PIM) for Just-in-Time (JIT) role assignment. Require approval or justification for privileged role activation.

Implement PIM



Review role membership periodically, especially for role membership hidden from the Azure Portal (*see script in links*). Hidden roles are not typically used.

Review Role Membership



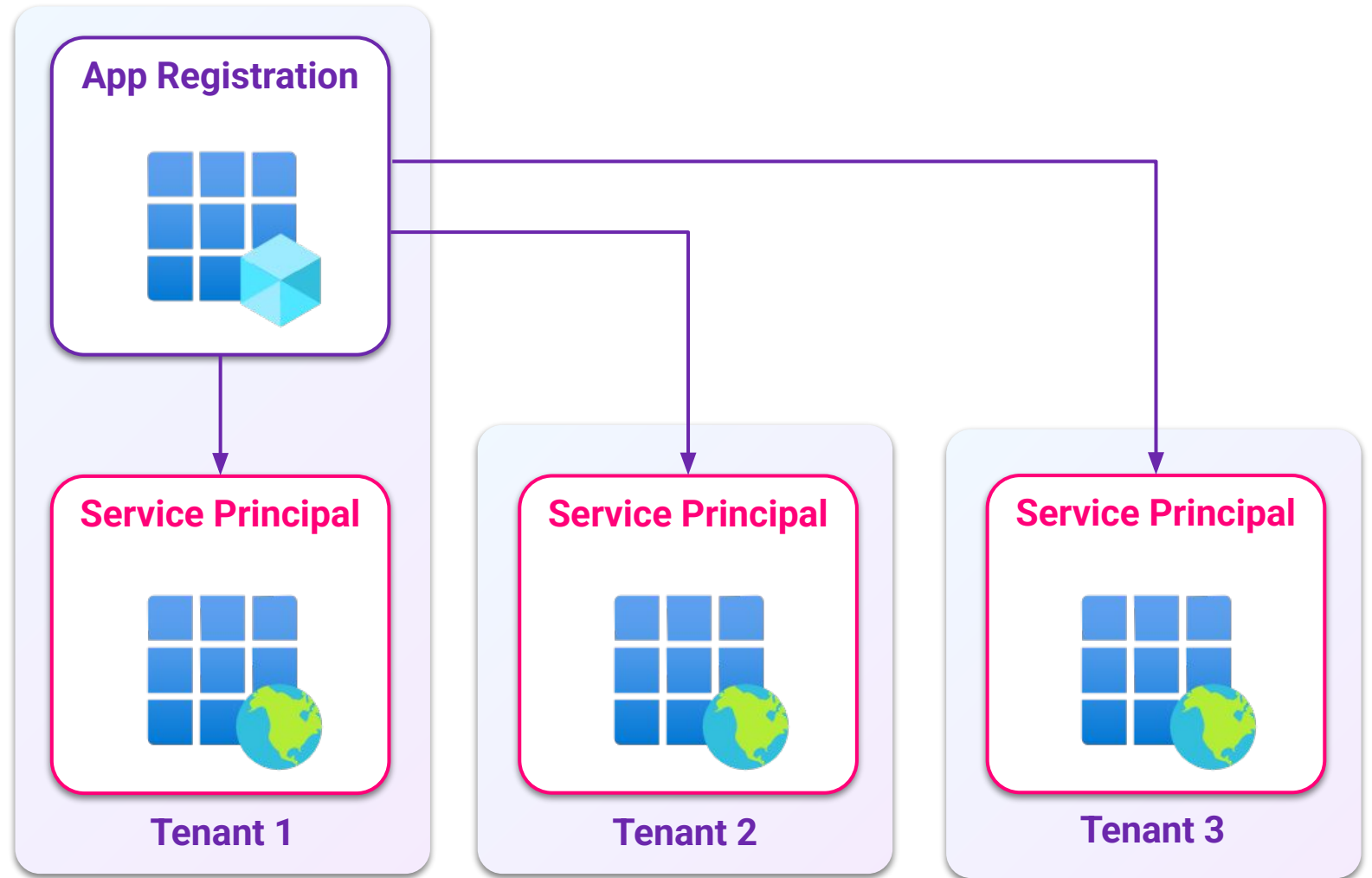
Applications

Entra ID Applications

use an app registration to define an app's configuration.

The app registration is then used to create a service principal (SP) in tenant(s) where the app is used.

Either object can authenticate as the app with a secret. Apps are often highly privileged.

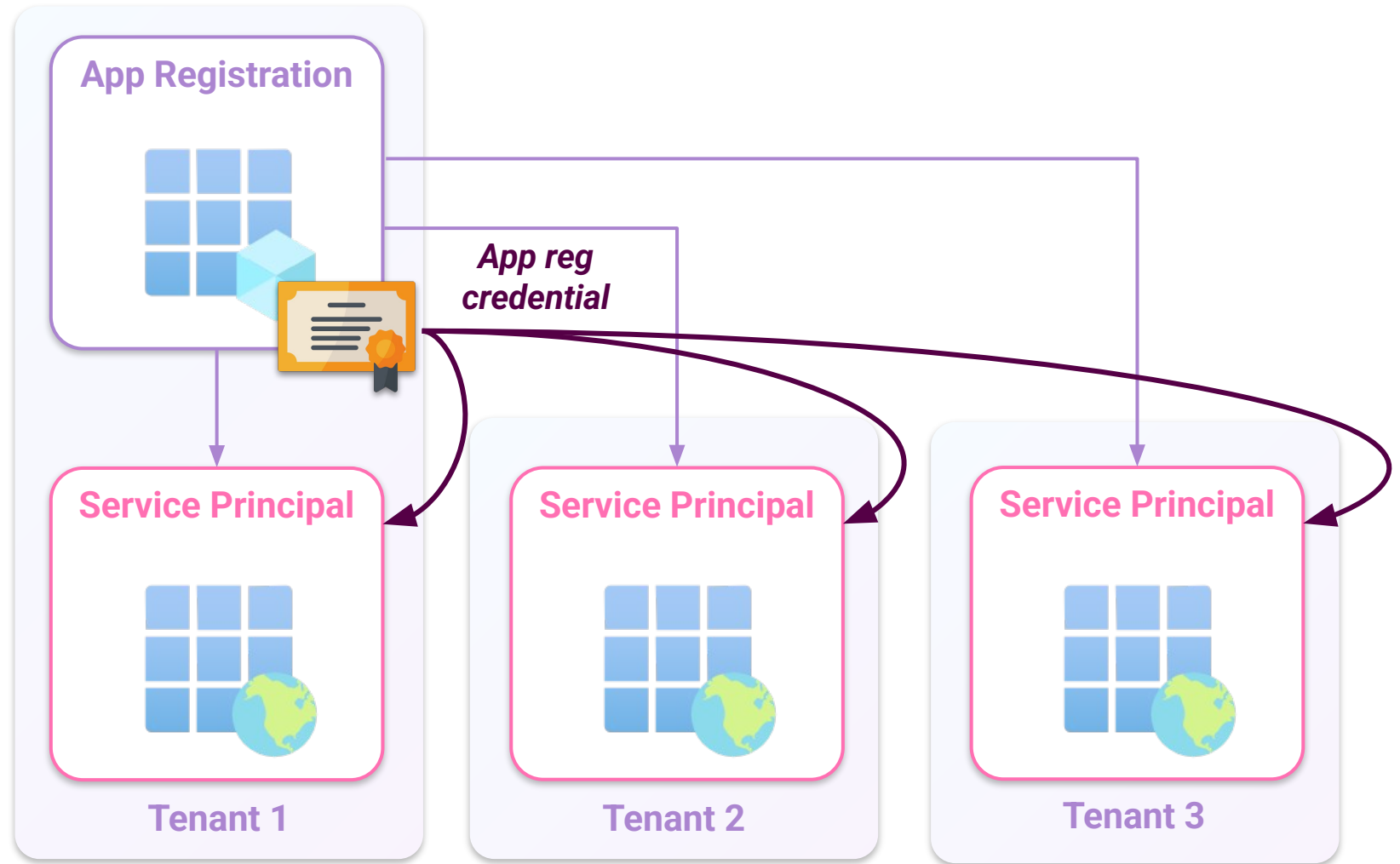


Entra ID Applications

use an app registration to define an app's configuration.

The app registration is then used to create a service principal (SP) in tenant(s) where the app is used.

Either object can authenticate as the app with a secret. Apps are often highly privileged.

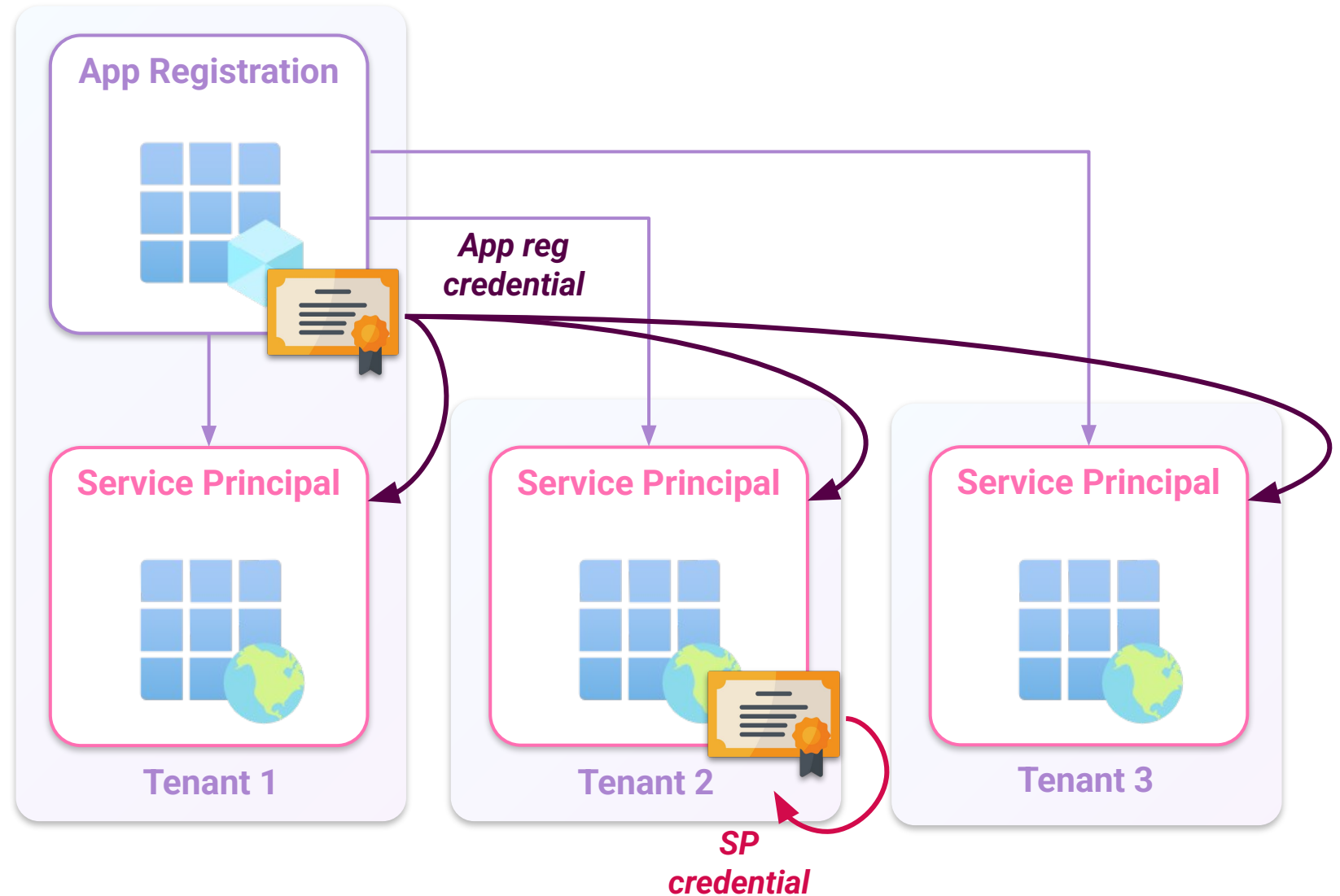


Entra ID Applications

use an app registration to define an app's configuration.

The app registration is then used to create a service principal (SP) in tenant(s) where the app is used.

Either object can authenticate as the app with a secret. Apps are often highly privileged.



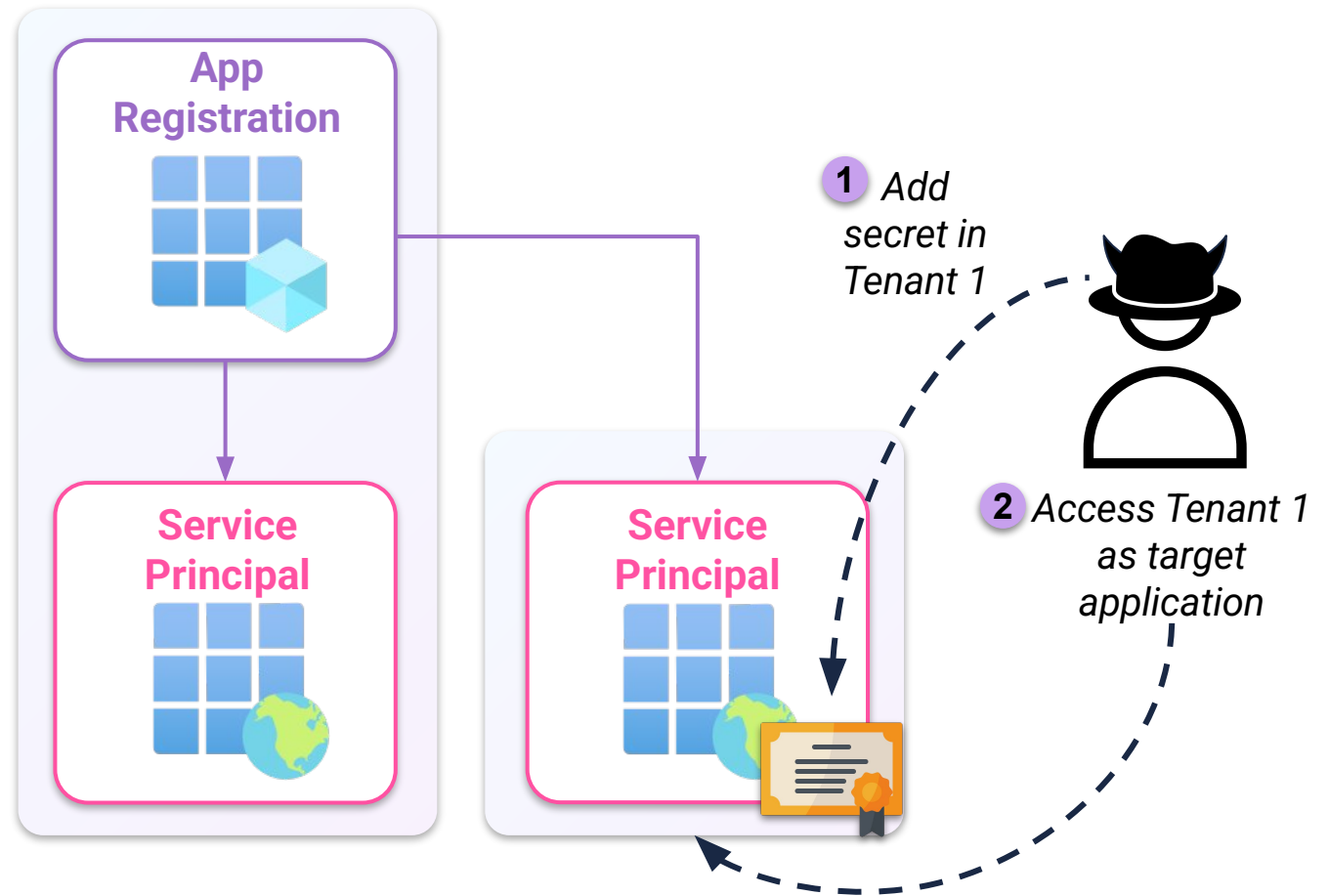
Attack: Credentials on SPs

An attacker with the following roles can add credentials to SPs:

- * Application Admin.
- * Cloud Application Admin.
- * Owner

SP credentials are not shown in the Azure Portal.

Application permissions assigned to apps are used without user interaction.

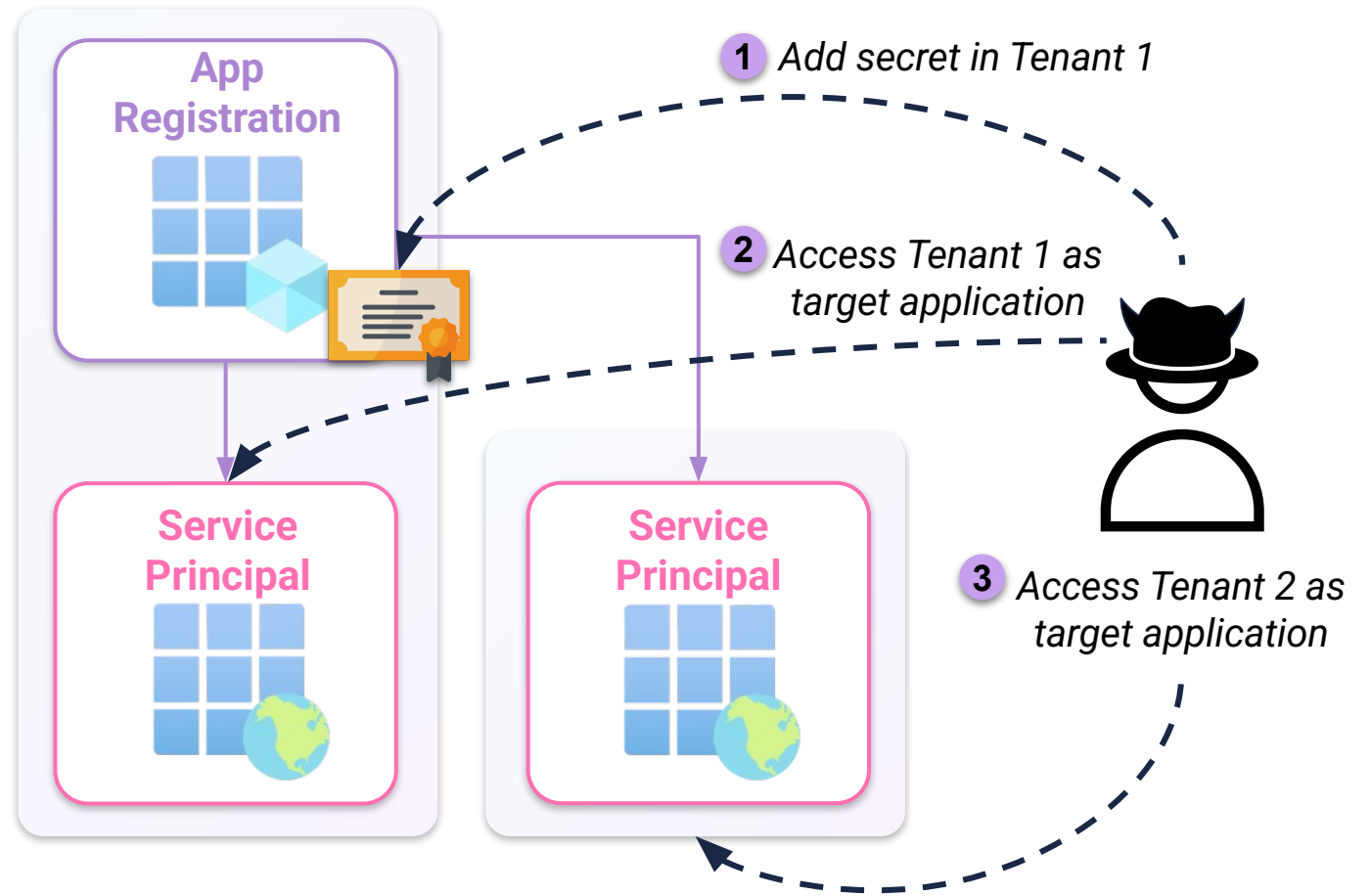


Attack: Credentials on App Registrations

An attacker with the below roles can also add credentials to app registrations:

- * Application Admin.
- * Cloud Application Admin.
- * Owner

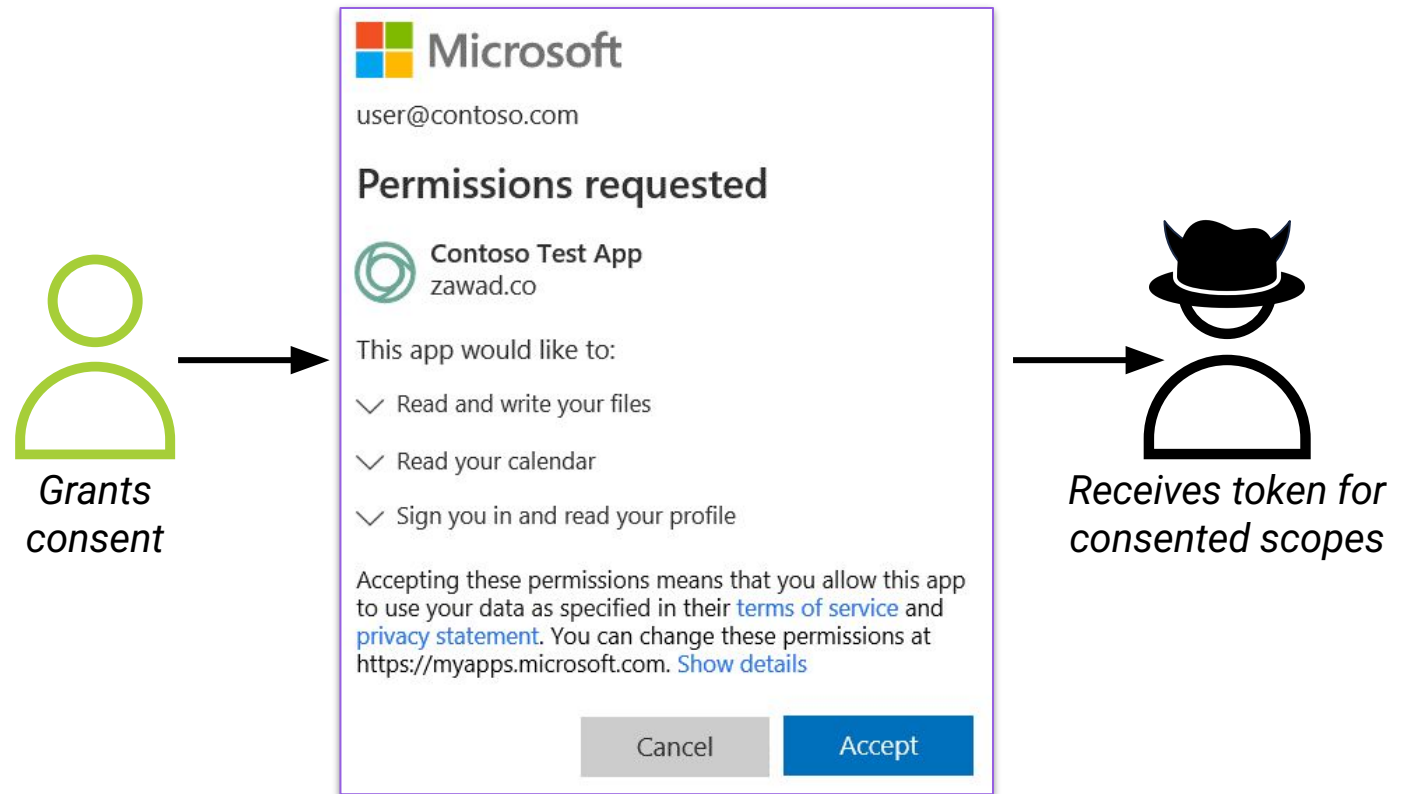
App registration credentials allow access as the target app in any tenant the app is installed in.



Attack: OAuth Consent Grant

OAuth consent phishing can be used for initial access, or to persist when an attacker can create app registrations.

Delegated permissions are granted when an attacker tricks a user into granting access to their data. A token with granted permissions is then returned to the attacker.



Detect: App Credentials and User Consent Grants

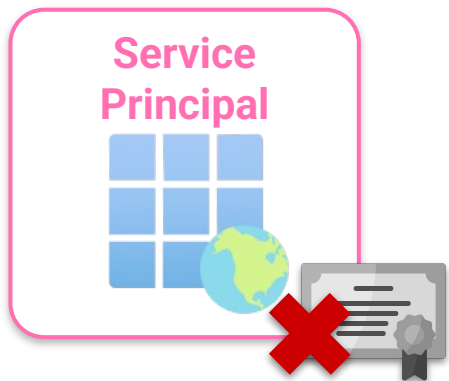
Monitor app permissions assignment **event names**:

- * "Add app role assignment to service principal"
- * "Consent to application"
- * "Add delegated permission grant"

Monitor **app registration** and **SP credential** additions:

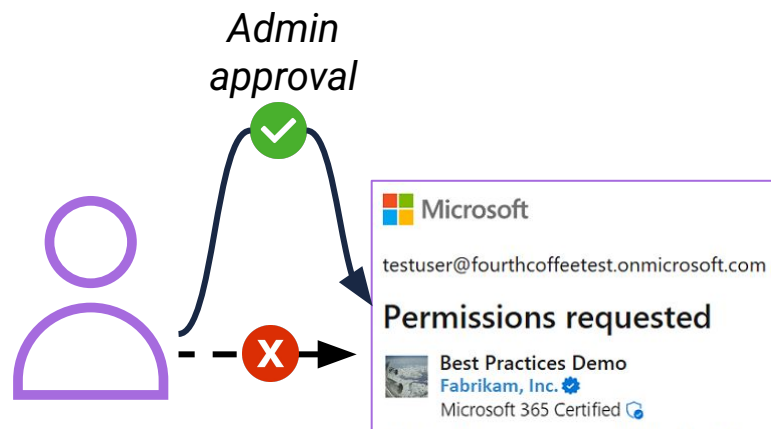
- * "Update application - Certificates and secrets management"
- * "Add service principal credentials"

Defend: Secure Applications and User Consent



Configure app instance property lock for local app registrations to prevent local SP credentials. Consider blocking secrets by policy.

App Property Lock



Enable user consent restrictions to prevent granting risky permissions without admin approval.

User Consent



Review secrets added to app registrations and SPs, and remove unnecessary credentials.

Credential Review

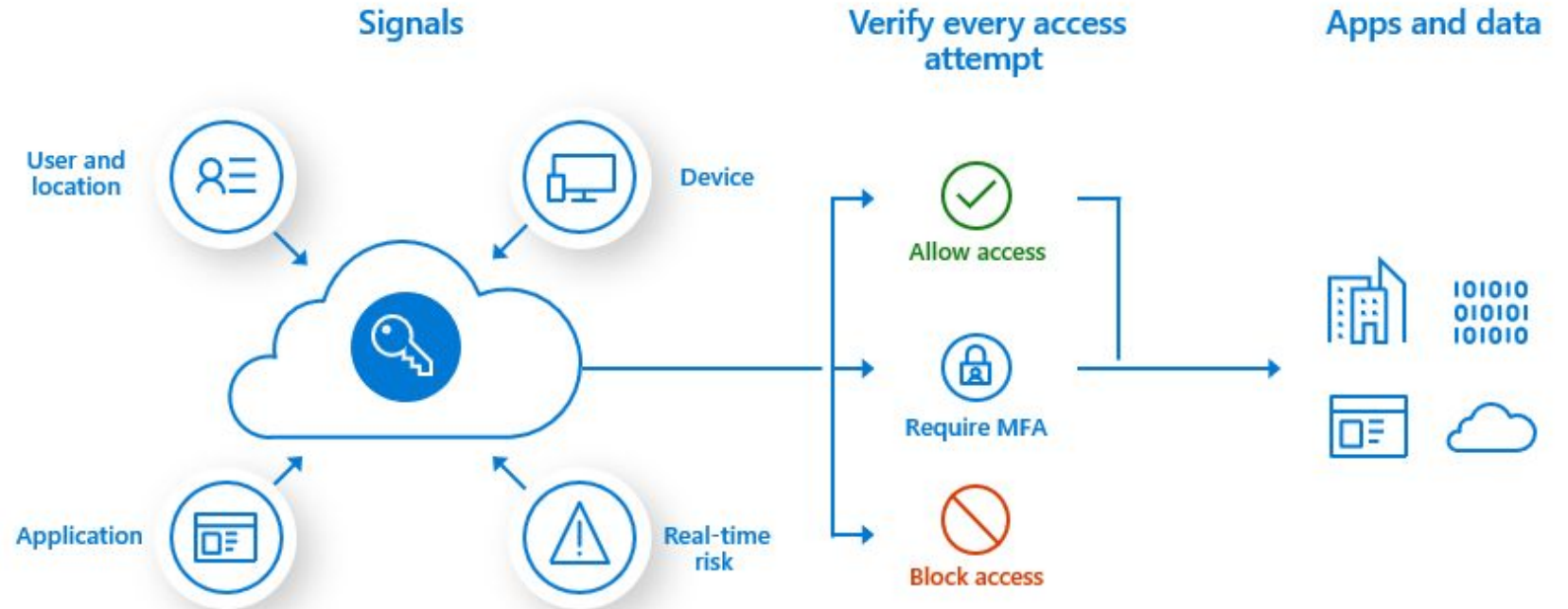


Authentication

Entra ID
Authentication
allows flexible access
to accounts.

Conditional Access
Policies (CAPs)
enforce auth strength
for these sign-ins.

Lesser-known
authentication types
and CAP modifications
can allow persistent
access.

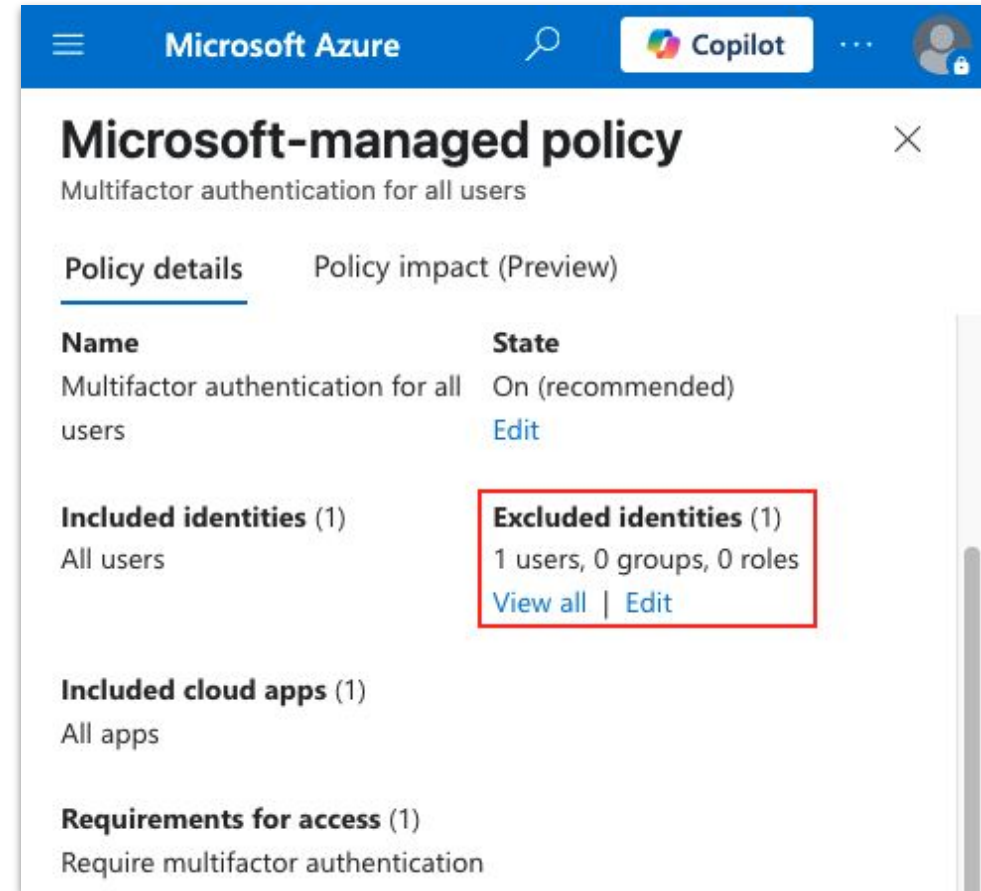


Attack: Modify or Disable MFA

An attacker with the following roles can modify CAPs:

- * Conditional Access Admin.
- * Security Administrator

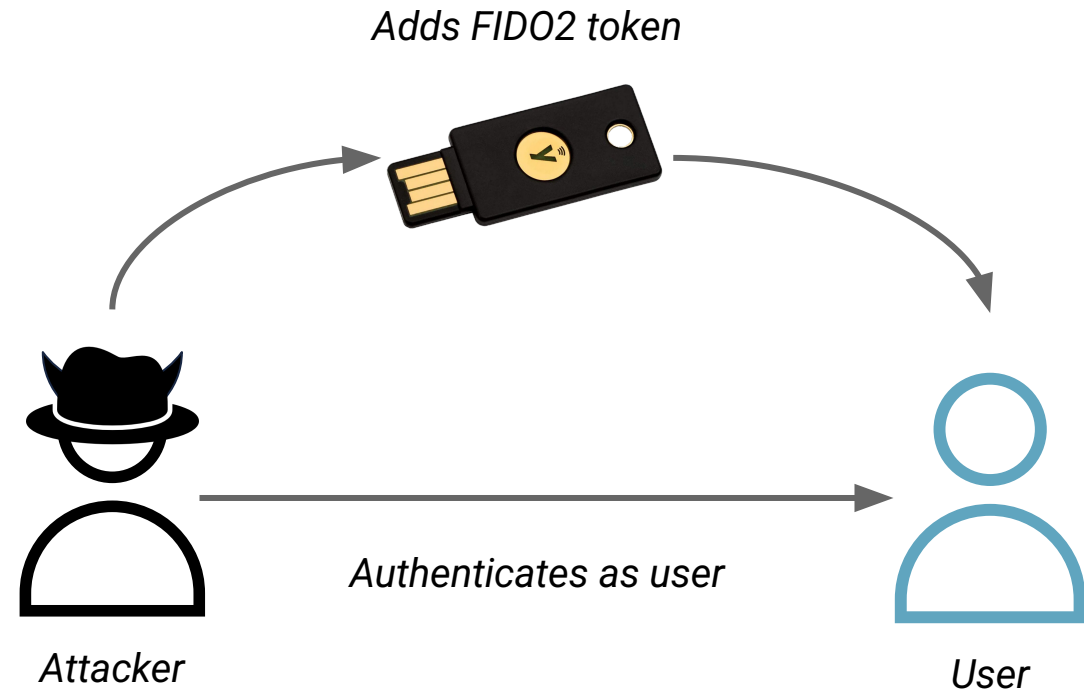
An attacker may exclude target identities from policy, delete policies, or change policy requirements.



Attack: Register Passkeys

A privileged attacker with a role allowing modification of user authentication could register a new FIDO2 token on a user's account.

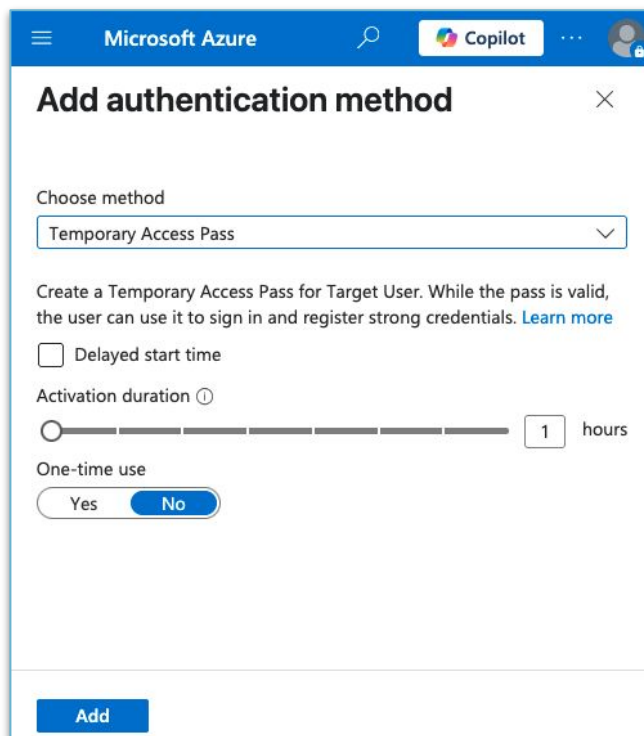
They could then use this token to authenticate as the target user.



Attack: Create TAP for User Account

A Temporary Access Passes (TAPs) are intended for short-term access to configure MFA.

An attacker with an authentication admin role can use a TAPs to sign into a target account without updating any passwords or MFA methods.



Microsoft Azure

Add authentication method

Choose method

Temporary Access Pass

Create a Temporary Access Pass for Target User. While the pass is valid, the user can use it to sign in and register strong credentials. [Learn more](#)

☐ Delayed start time

Activation duration ⓘ

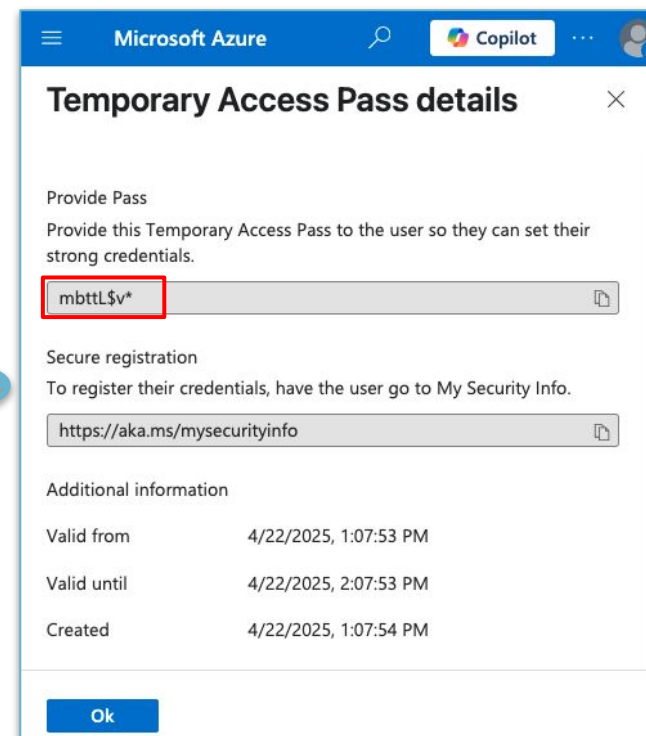
1 hours

One-time use

Yes No

Add

A TAP can be valid for up to 8 hours



Microsoft Azure

Temporary Access Pass details

Provide Pass

Provide this Temporary Access Pass to the user so they can set their strong credentials.

mbttL\$*

Secure registration

To register their credentials, have the user go to My Security Info.

<https://aka.ms/mysecurityinfo>

Additional information

Valid from	4/22/2025, 1:07:53 PM
Valid until	4/22/2025, 2:07:53 PM
Created	4/22/2025, 1:07:54 PM

Ok

TAPs are eight characters, and qualify as MFA compliant sign-ins

Detect: Authentication and CAP Modification

Monitor CAP modification event names:

- * "Update Conditional Access policy"
- * "Delete Conditional Access policy"
- * "Update named location"
- * "Update security defaults"

Monitor TAP Sign-in Logs:

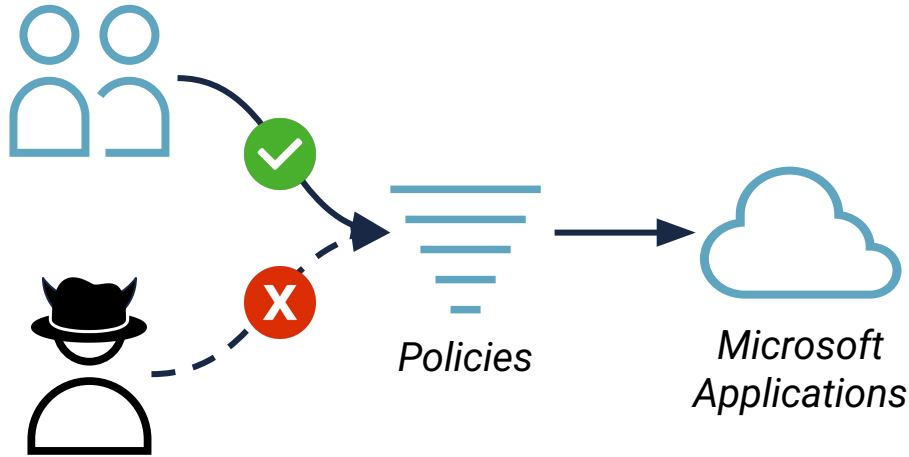
- * authenticationDetails.authenticationMethod: "Temporary Access Pass"

Monitor changes to user authentication methods:

- * "Admin registered security info" *
- * "Admin deleted security info"
- * "Reset password"
- * "User registered security info" *
- * "Admin started password reset"
- * "Admin registered temporary access pass method for user"

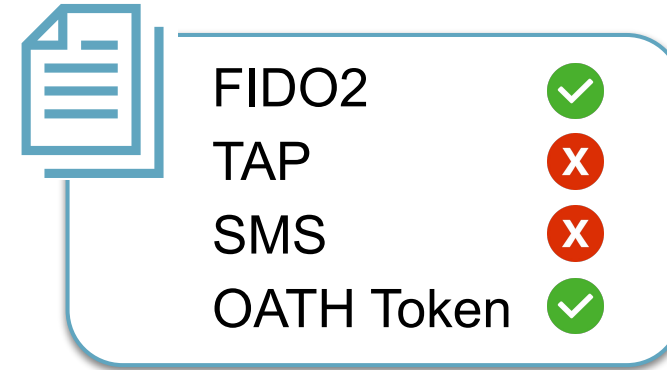
** Users can have multiple tokens registered.*

Defend: Limit Insecure & Unused Authentication



Review CAPs: Ensure only expected users bypass MFA. Block device codes. Require registered or enrolled devices.

Configure & Review CAPs



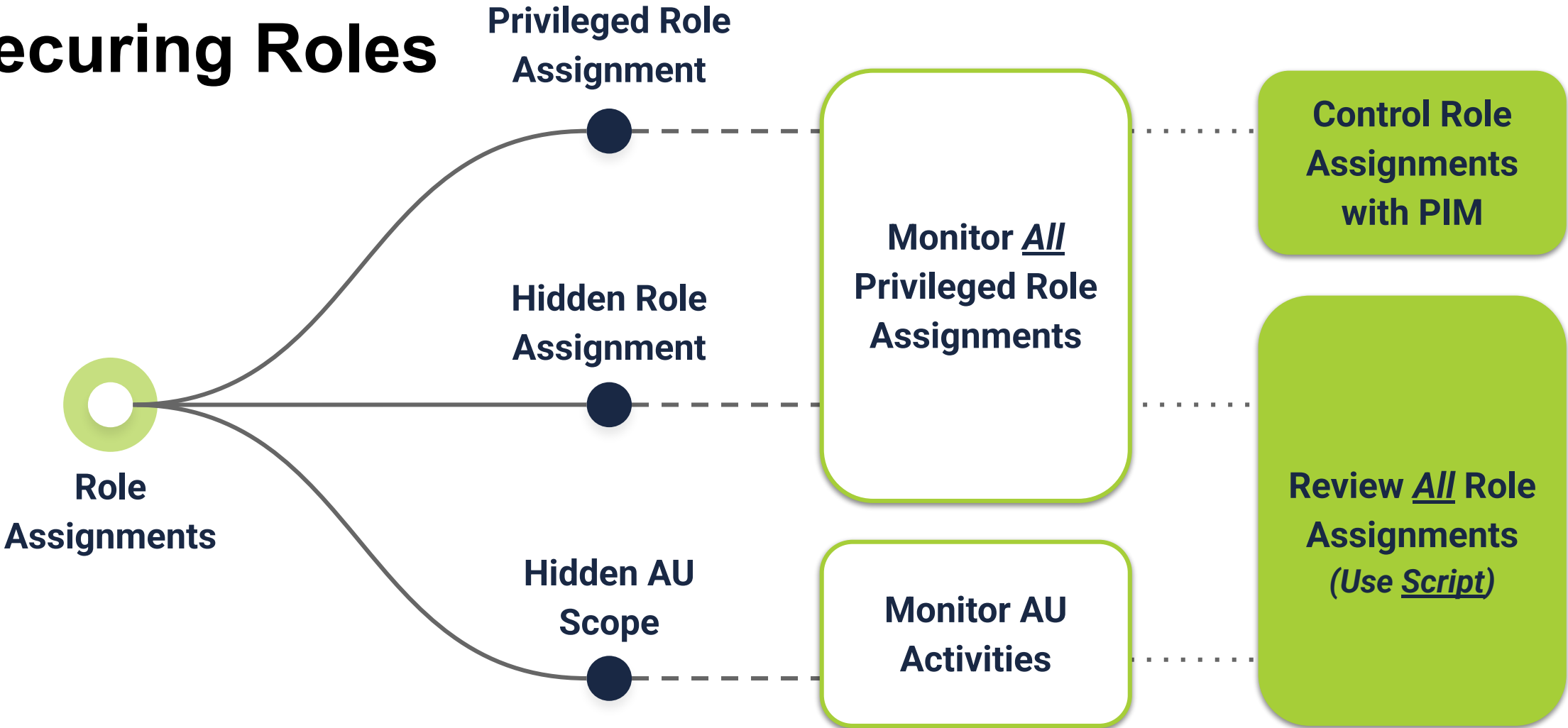
Review allowed authentication under Entra "Authentication methods > Policies". Disable authentication methods not in use.

Disable Unused Auth Methods

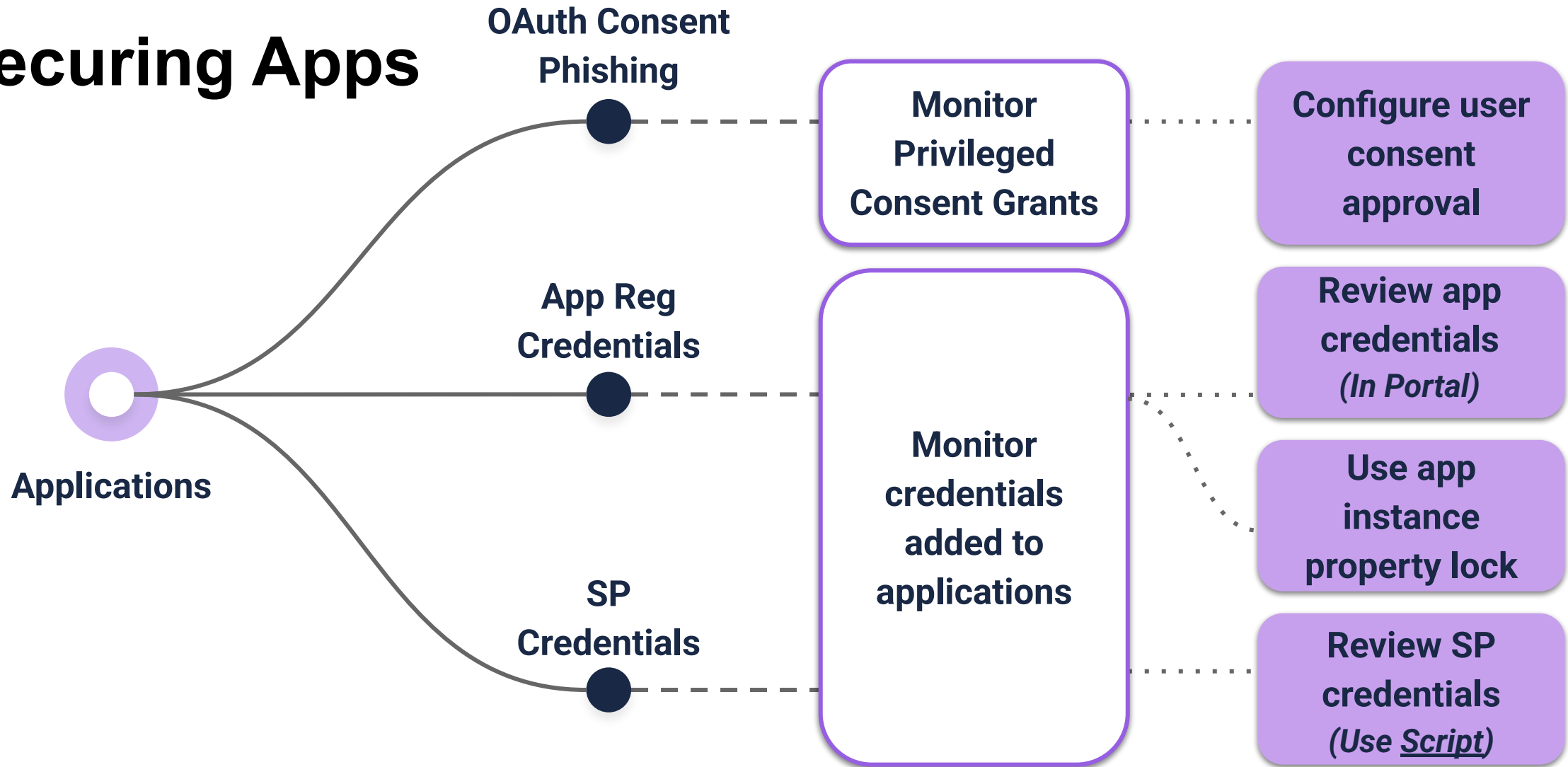


Recap

Securing Roles



Securing Apps



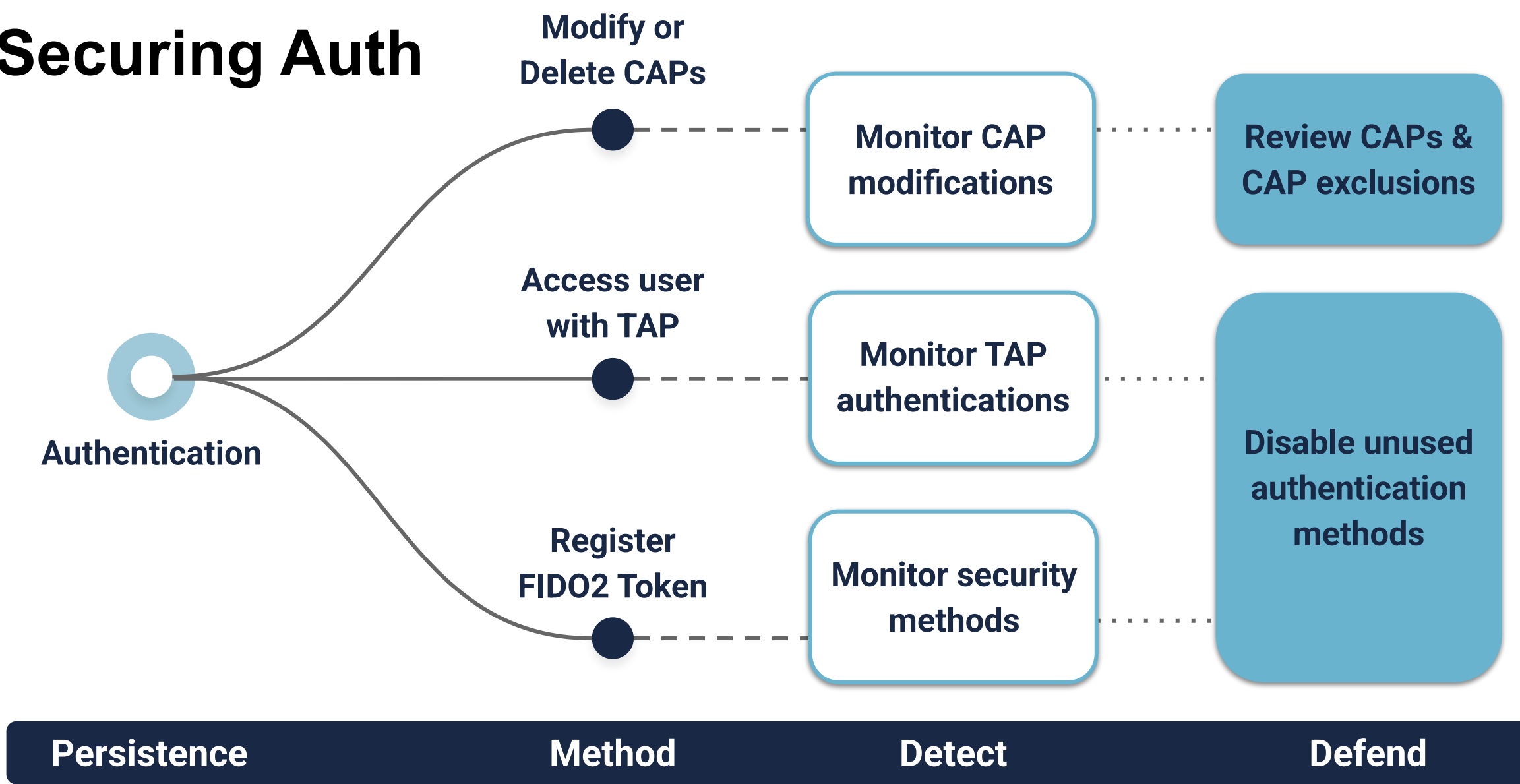
Persistence

Method

Detect

Defend

Securing Auth





Takeaways

Apply



Today, review links and resources from today's talk. Links are available in the next slides, or in blog format here: <https://kknowl.es/posts/defending-against-entra-id-persistence>



This week, review "Detect" steps for the persistence techniques discussed in this talk. Identify which detections should be implemented, and create a timeline for them.



This month, run scripts to review Entra ID role assignments and SP credentials. Identify an Entra administrator to discuss results, and which "Defend" steps from this talk could be implemented.

Defending Against Persistence

Logging & Monitoring

- [Microsoft, "Microsoft Entra audit log categories and activities"](#)

Role Assignments

Background

- [Microsoft, "Understand roles in Microsoft Entra ID"](#)
- [Microsoft, "Privileged roles and permissions in Microsoft Entra ID"](#)
- [Microsoft, "Administrative units in Microsoft Entra ID"](#)
- [Microsoft, "Elevate access to manage all Azure subscriptions and management groups"](#)
- [Trimarc Security, "Demystifying Privileged Identity Management - Part 1"](#)

Attacks

- [Andy Robbins, "The Most Dangerous Entra Role You've \(Probably\) Never Heard Of"](#)
- [Katie Knowles, "Hidden in Plain Sight: Abusing Entra ID Administrative Units for Sticky Persistence"](#)

Defense

- [Vasil Michev, "Reporting on Entra ID directory role assignments \(including PIM\)"](#)
- [Microsoft, "List Microsoft Entra role assignments"](#)
- [Microsoft, "Privileged Identity Management documentation"](#)

Applications

Overview

- [Microsoft, "Application model"](#)

Attacks

- [Dirk-jan Mollema, "Azure AD privilege escalation"](#)
- [Eric Woodruff, "UnOAuthed: Privilege Elevation Through Microsoft Applications"](#)
- [Microsoft, "Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard"](#)
- [Lior Sonntag, "Midnight Blizzard attack on Microsoft corporate environment"](#)
- [Microsoft, "Threat actor consent phishing campaign abusing the verified publisher process"](#)

Defense

- [Vasil Michev, "Script to review and remove service principal credentials"](#)
- [Microsoft, "How to configure app instance property lock for your applications"](#)
- [Daniel Bradley, "How to block the creation of Client Secrets on Entra applications"](#)
- [Microsoft, "Configure user consent settings"](#)
- [Microsoft, "Security best practices for application properties in Microsoft Entra ID"](#)
- [Microsoft, "Protect against consent phishing"](#)
- [Microsoft, "Investigate and remediate risky OAuth apps"](#)

Defending Against Persistence

Authentication

Overview

- [Microsoft, "What authentication and verification methods are available in Microsoft Entra ID?"](#)
- [Microsoft, "What is Conditional Access?"](#)

Attacks

- [Microsoft, "Octo Tempest crosses boundaries to facilitate extortion, encryption, and destruction"](#)
- [CISA, "Scattered Spider"](#)
- [Max Rozendaal, "Abusing FIDO2 passkeys to take over Global Administrators in Entra ID"](#)
- [Daniel Heinsen, "I'd TAP That Pass"](#)

Defense

- [Microsoft, "Use access reviews to manage users excluded from Conditional Access policies"](#)
- [Microsoft, "Block authentication flows with Conditional Access policy"](#)



DATADOG

THANK YOU

Katie Knowles

Cloud Security Researcher, Datadog

 | [/siigil](https://twitter.com/siigil)

 | [/in/kaknowles](https://www.linkedin.com/company/kaknowles)

 | kknowl.es