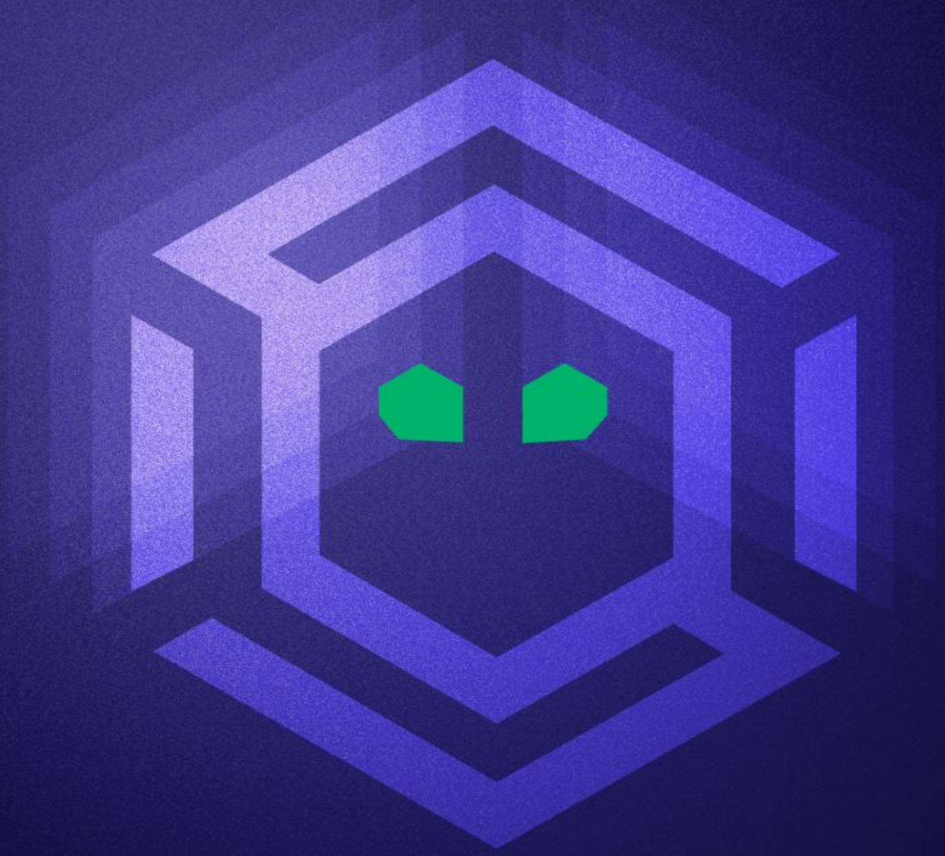
SPECTEROPS

Synced User Attack Path Analysis w/ BloodHound



Permalink to this deck: https://bit.ly/46Xjzjw

About Us

Andy Robbins

Product Architect at SpecterOps

Co-creator of BloodHound

@_wald0

Cody Thomas

Senior Software Engineer at SpecterOps

Creator of Mythic

@its_a_feature_

Microsoft Hybrid Identity

Admins can sync users with two Microsoft technologies:

Entra Connect

✅ Supports user synchronization

✅ Supports password hash sync

✅ Supports password writeback

Entra Cloud Sync

✅ Supports user synchronization

✅ Supports password hash sync

✅ Supports password writeback

https://learn.microsoft.com/en-us/entra/identity/hybrid/cloud-sync/what-is-cloud-sync#comparison-between-microsoft-entra-connect-and-cloud-sync

Why this matters

Cross-platform attack paths

User synchronization can enable attack paths that traverse identity and compute platforms

Synced users, synced risk

The security posture of one platform will affect the posture of the other.

Implicit, obscure trust

Entra user sync attack paths can expose on-prem Active Directory forests that do not explicitly trust one another.

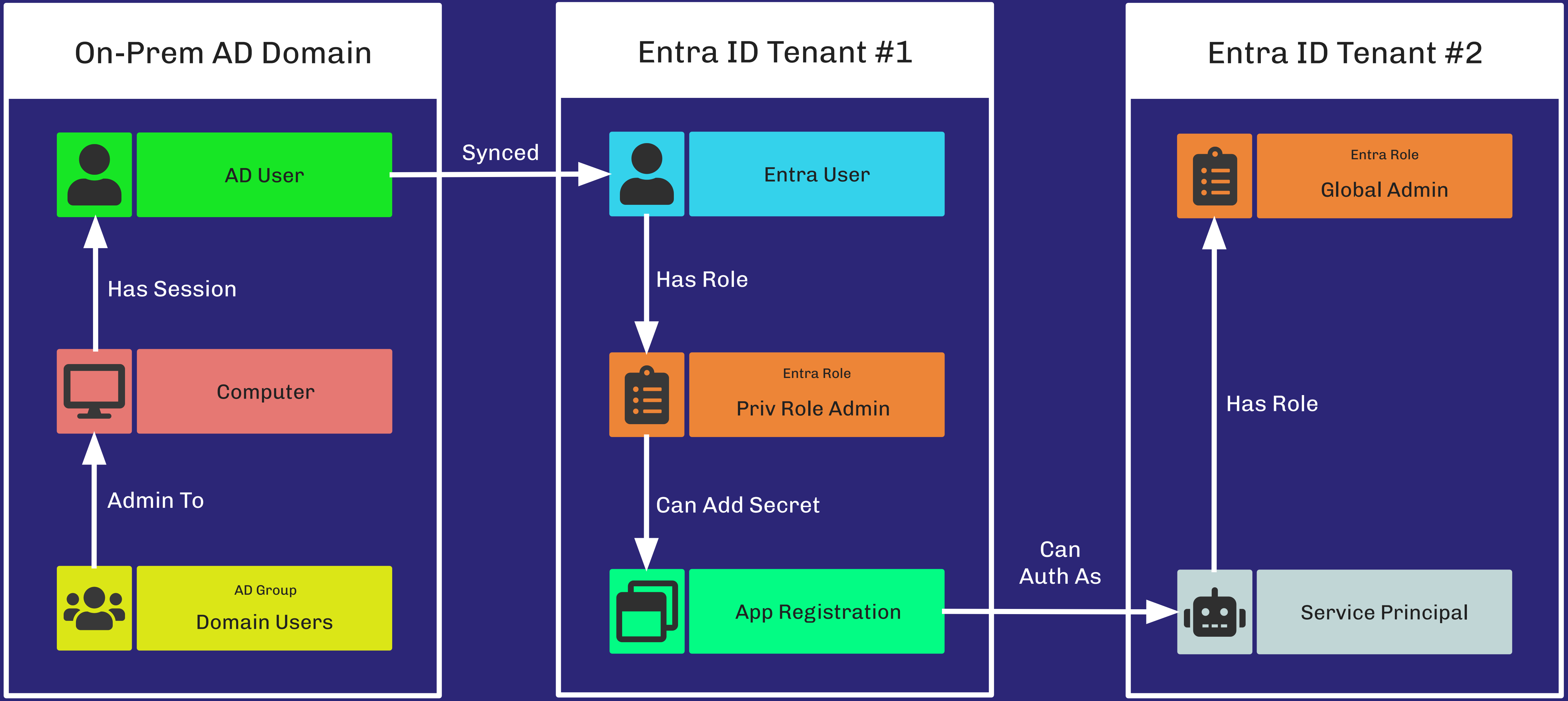
Two New Edges

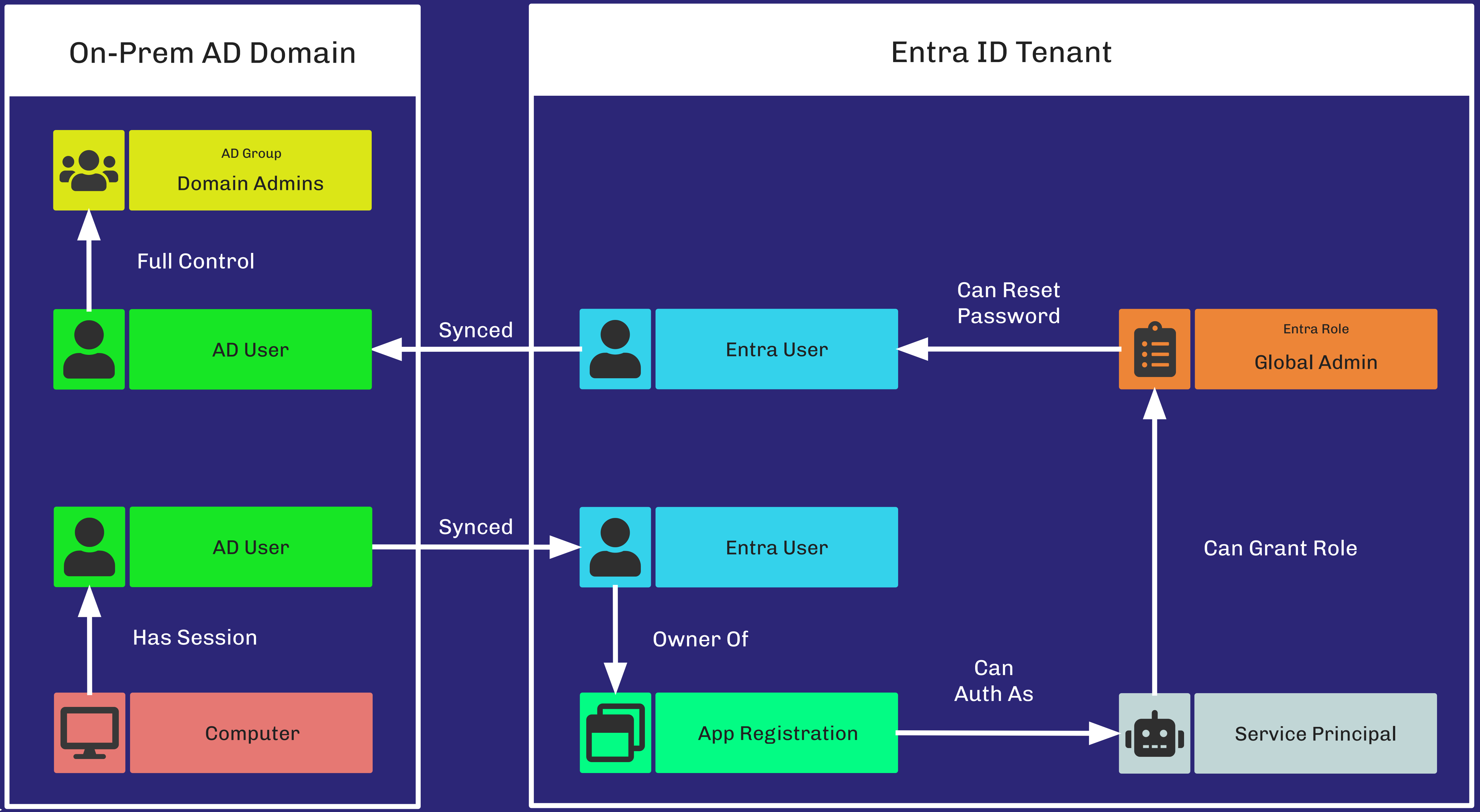
SyncedToEntraUser

- May reveal attack paths from on-prem AD users to their synchronized Entra users.
- Potentially abusable due to identical passwords, federated authentication, or artifacts left behind by single sign-on.

SyncedToADUser

- May reveal attack paths from Entra users to their synchronized on-prem AD users.
- Potentially abusable due to password write-back or cloud kerberos trust.

On-Prem AD Domain
AD User
Has Session
Computer
Admin To
AD Group
Domain Users
Synced
Entra ID Tenant #1
Entra User
Has Role
Entra Role
Priv Role Admin
Can Add Secret
App Registration
Can
Auth As
Entra ID Tenant #2
Entra Role
Global Admin
Has Role
Service Principal



On-Prem AD Domain

Entra ID Tenant

AD Group
Domain Admins

Full Control

AD User

Synced

Entra User

Can Reset
Password

Entra Role
Global Admin

AD User

Synced

Entra User

Can Grant Role

Has Session

Owner Of

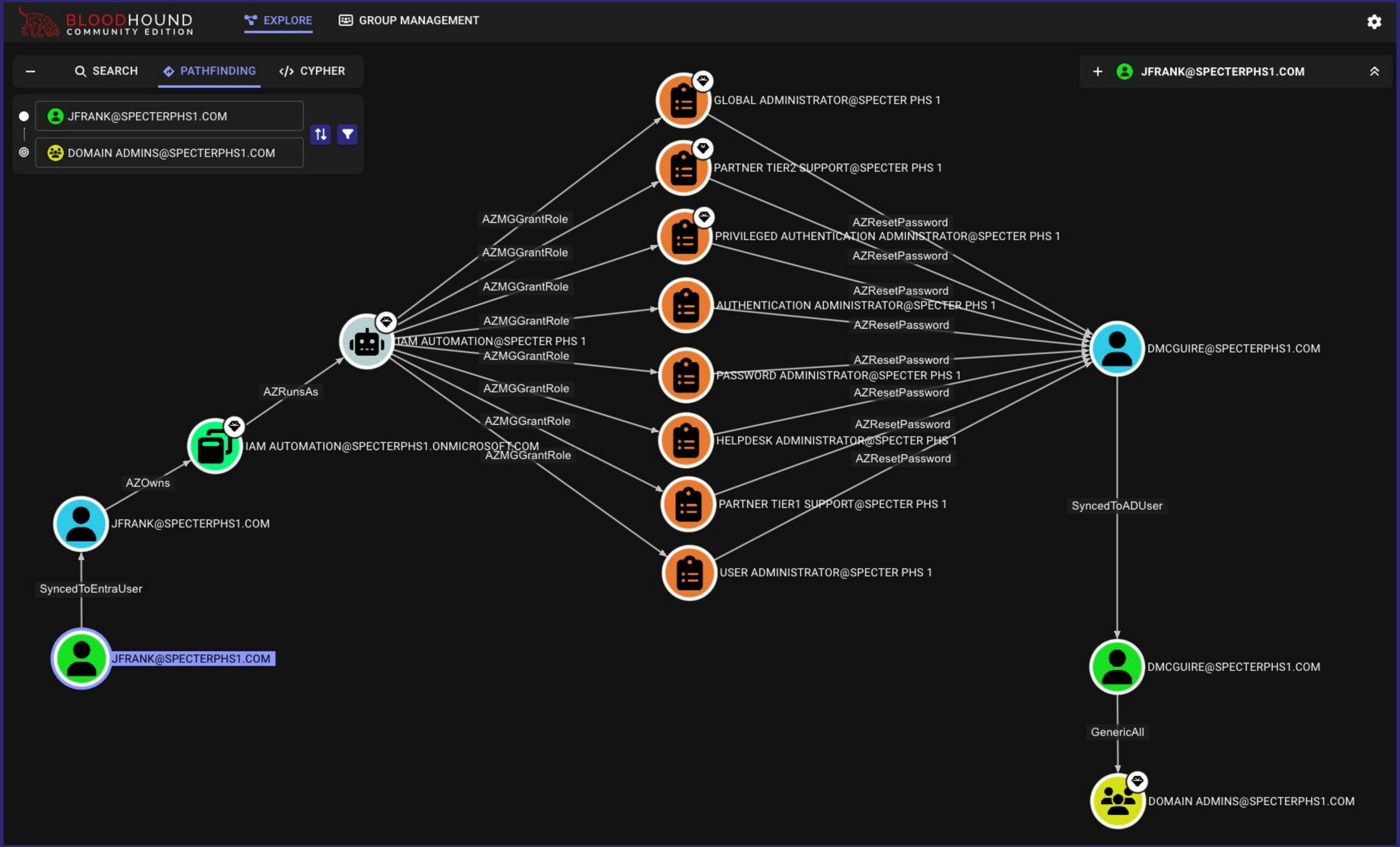
Can
Auth As

Computer

App Registration

Service Principal

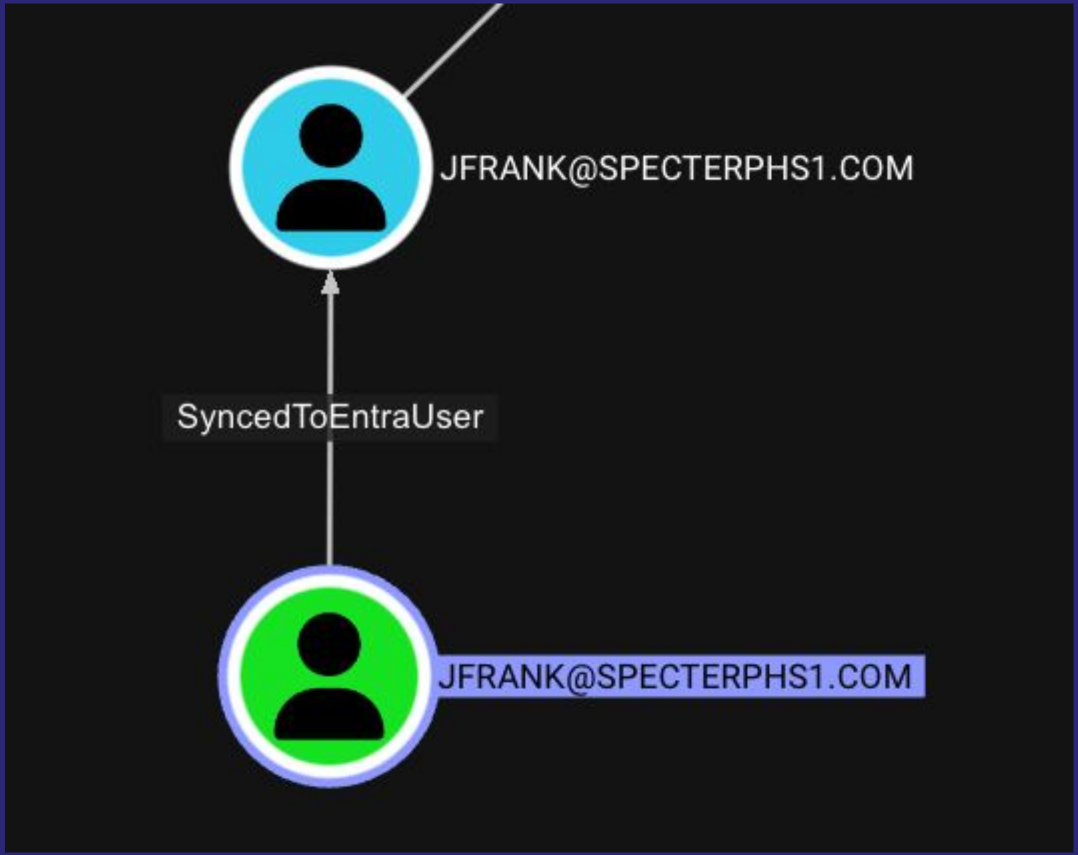
SPECTEROPS



JFRANK@SPECTERPHS1.COM

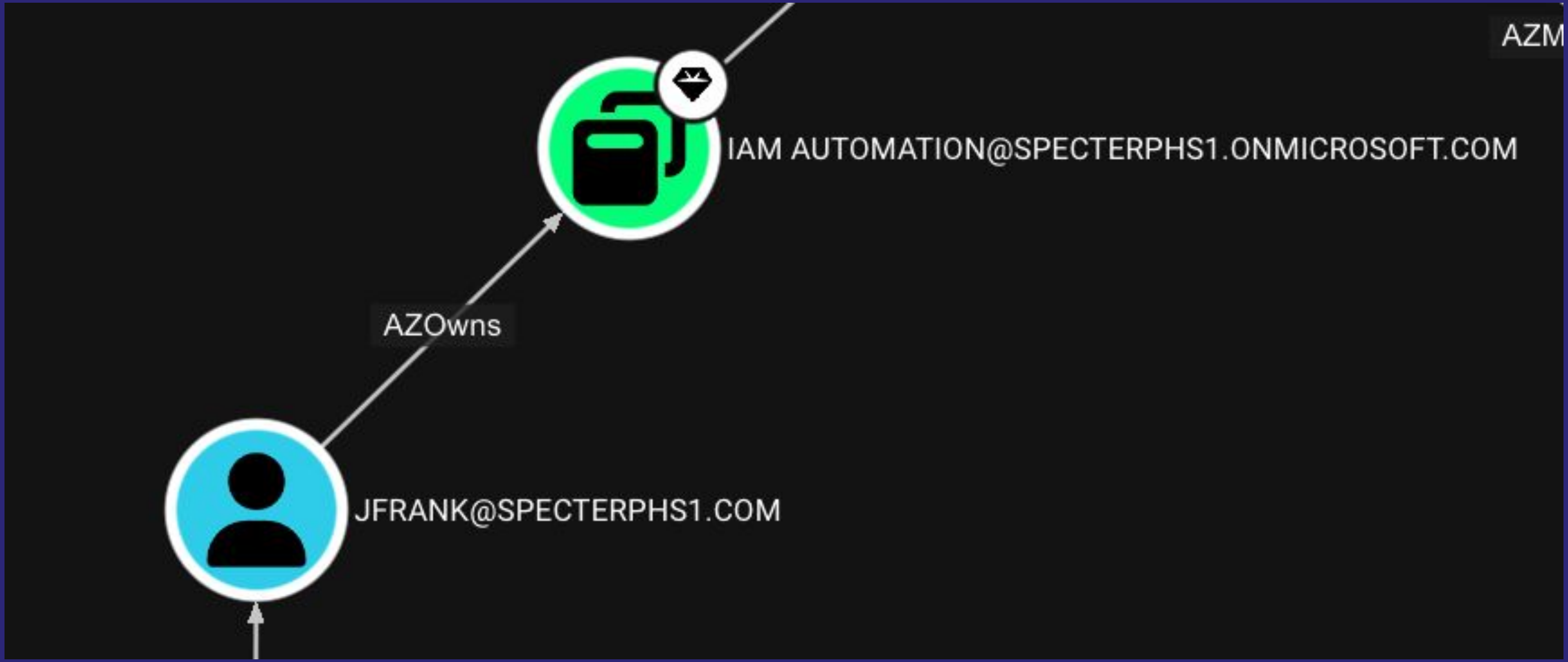
DOMAIN ADMINS@SPECTERPHS1.COM

Demo

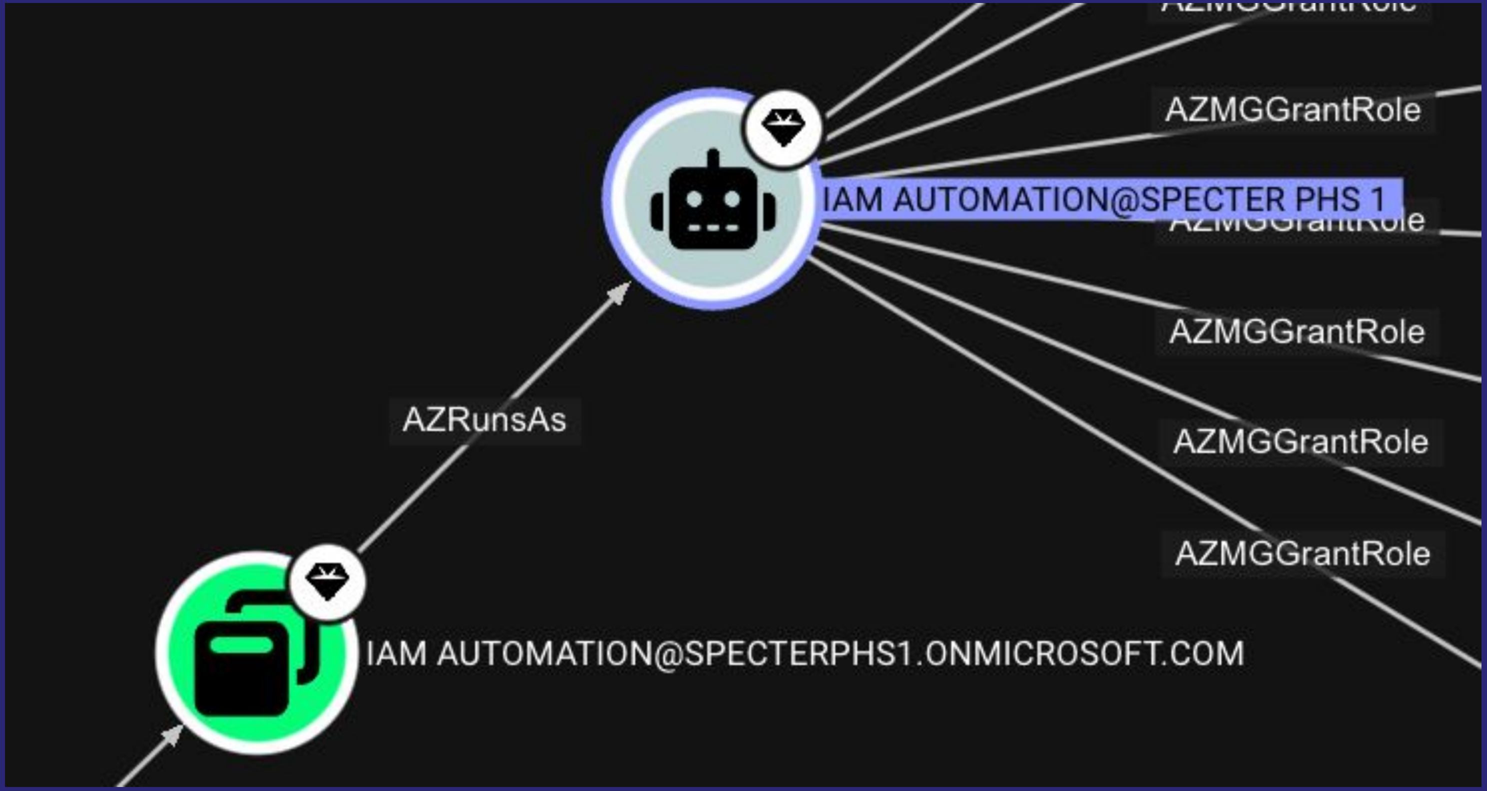


Attack Path Step 1:
Get execution as on-prem user.

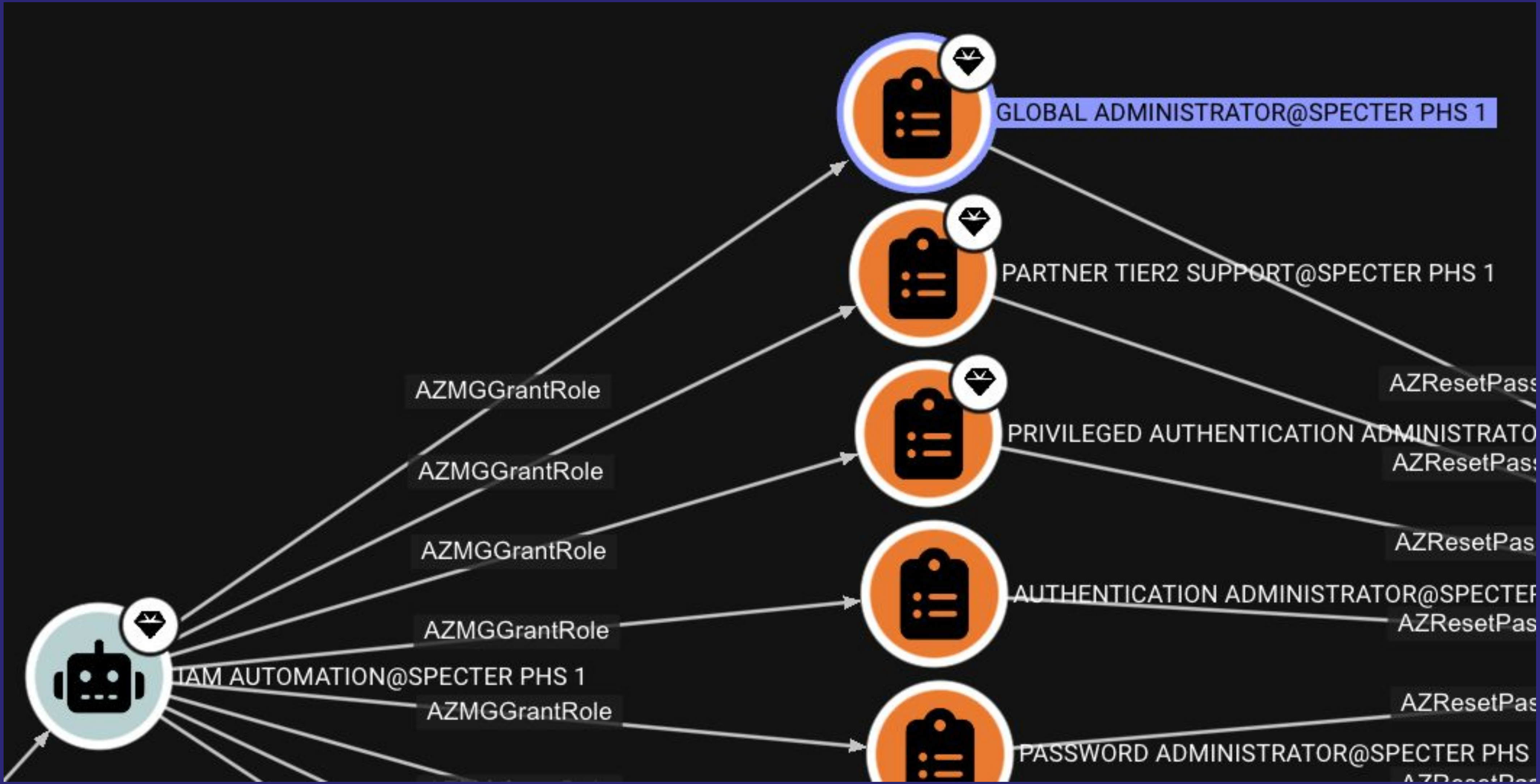
Attack Path Step 2:
Steal a token for the Entra user from the system used by the on-prem Active Directory user.



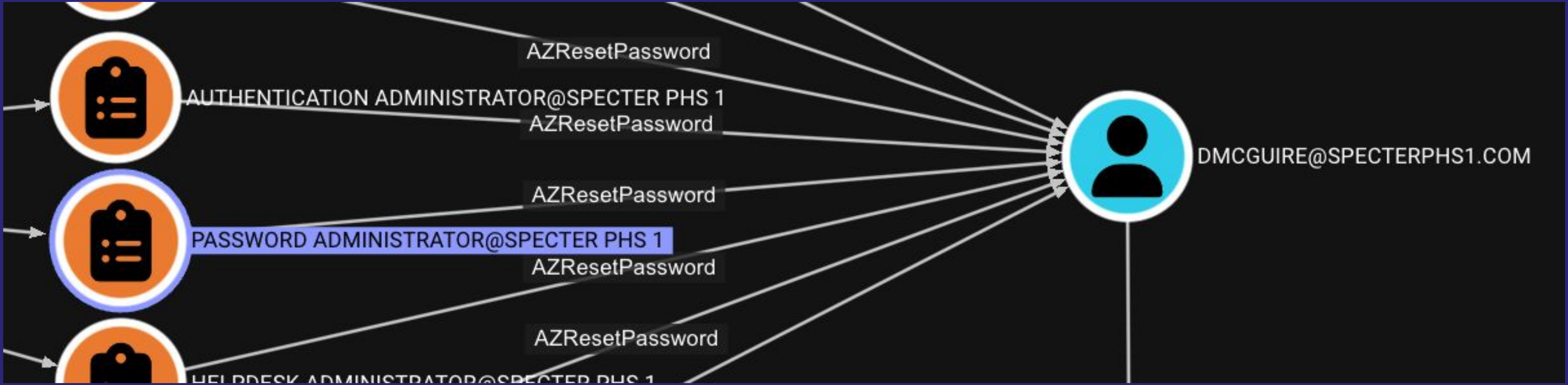
Attack Path Step 3:
Add a new credential to the “IAM Automation” application registration object.



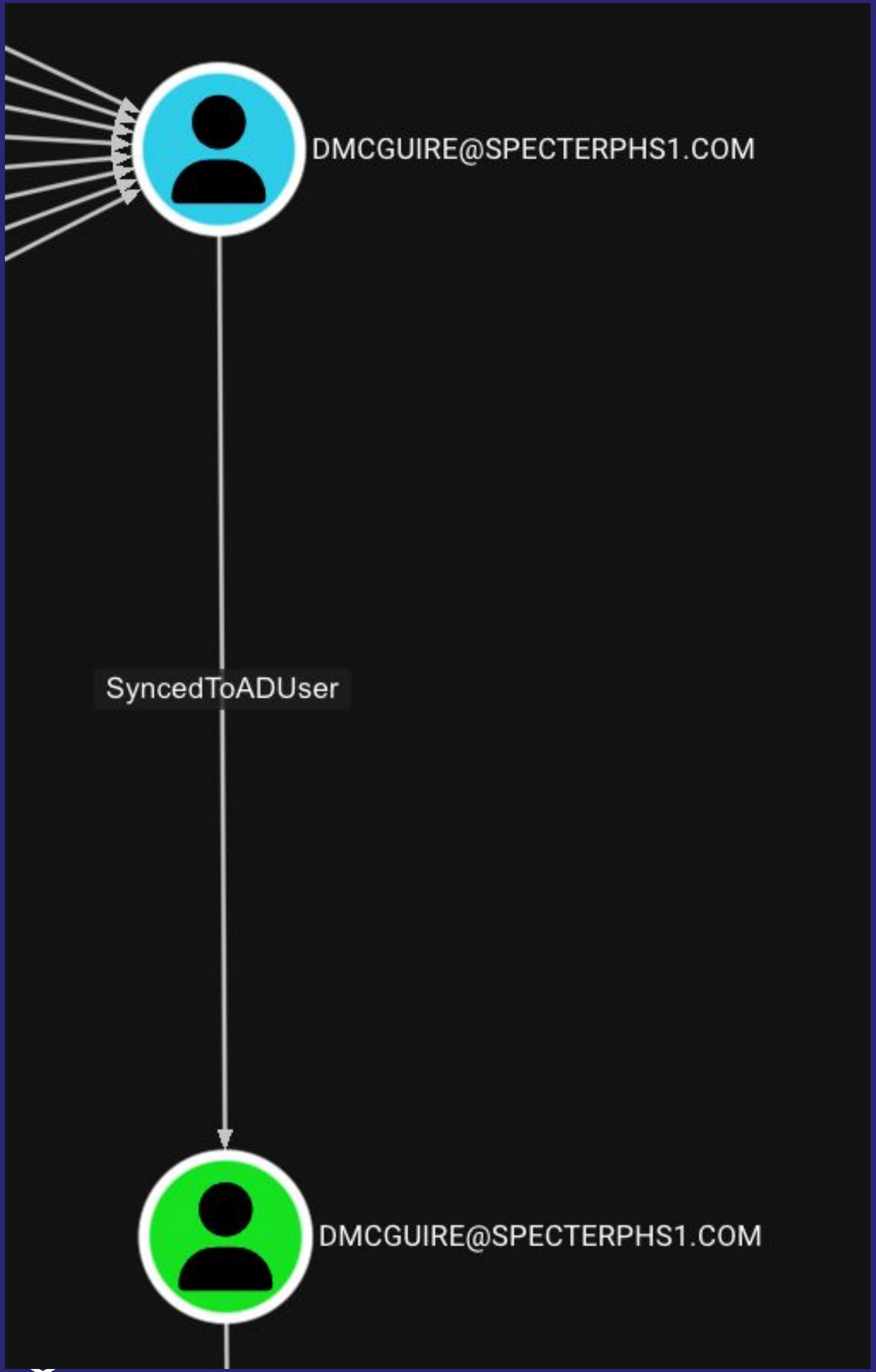
Attack Path Step 4:
Authenticate as the “IAM Automation” service principal.


GLOBAL ADMINISTRATOR@SPECTER PHS 1
PARTNER TIER2 SUPPORT@SPECTER PHS 1
PRIVILEGED AUTHENTICATION ADMINISTRATO
AUTHENTICATION ADMINISTRATOR@SPECTEF
PASSWORD ADMINISTRATOR@SPECTER PHS
IAM AUTOMATION@SPECTER PHS 1
AZMGGrantRole
AZMGGrantRole
AZMGGrantRole
AZMGGrantRole
AZMGGrantRole
AZResetPass
AZResetPass
AZResetPas
AZResetPas
AZResetPas

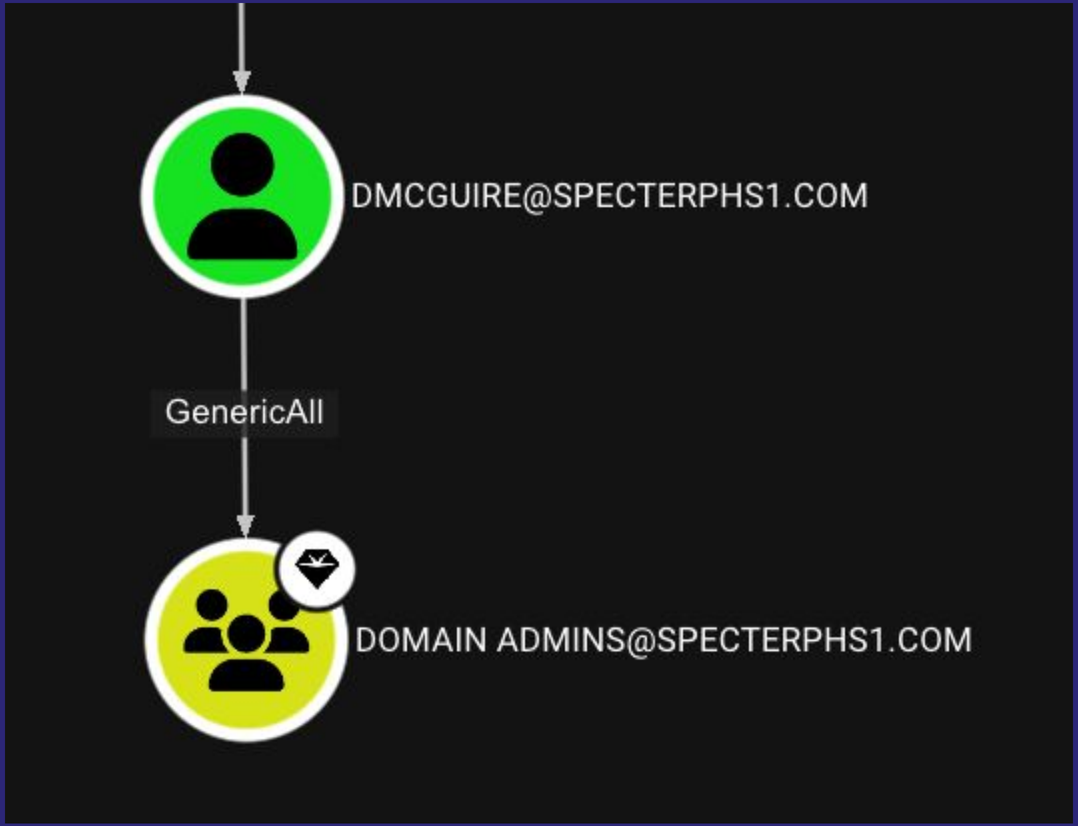
Attack Path Step 5:
Promote the “IAM Automation” service principal to Global Admin.


AZResetPassword
AUTHENTICATION ADMINISTRATOR@SPECTER PHS 1
AZResetPassword
DMCGUIRE@SPECTERPHS1.COM
AZResetPassword
PASSWORD ADMINISTRATOR@SPECTER PHS 1
AZResetPassword
AZResetPassword
HELPDESK ADMINISTRATOR@SPECTER PHS 1

Attack Path Step 6 (part 1):
Get updated token with new roles from step 5.
Create a new user and grant it the “Password Administrator” role.



Attack Path Step 6 (part 2):
Reset the password for the Entra user "DMCGUIRE", which will be written back to the on-prem AD user "DMCGUIRE".

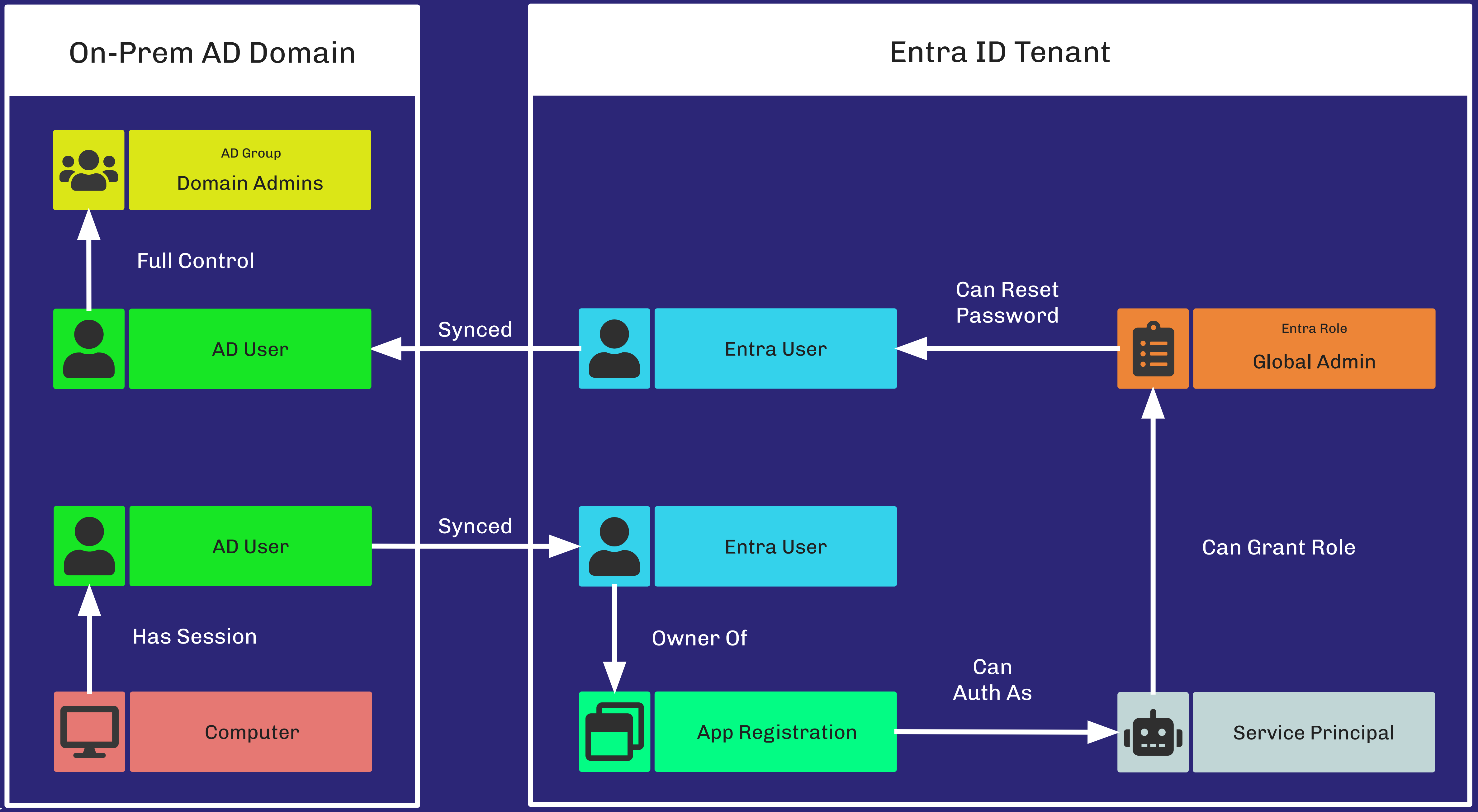


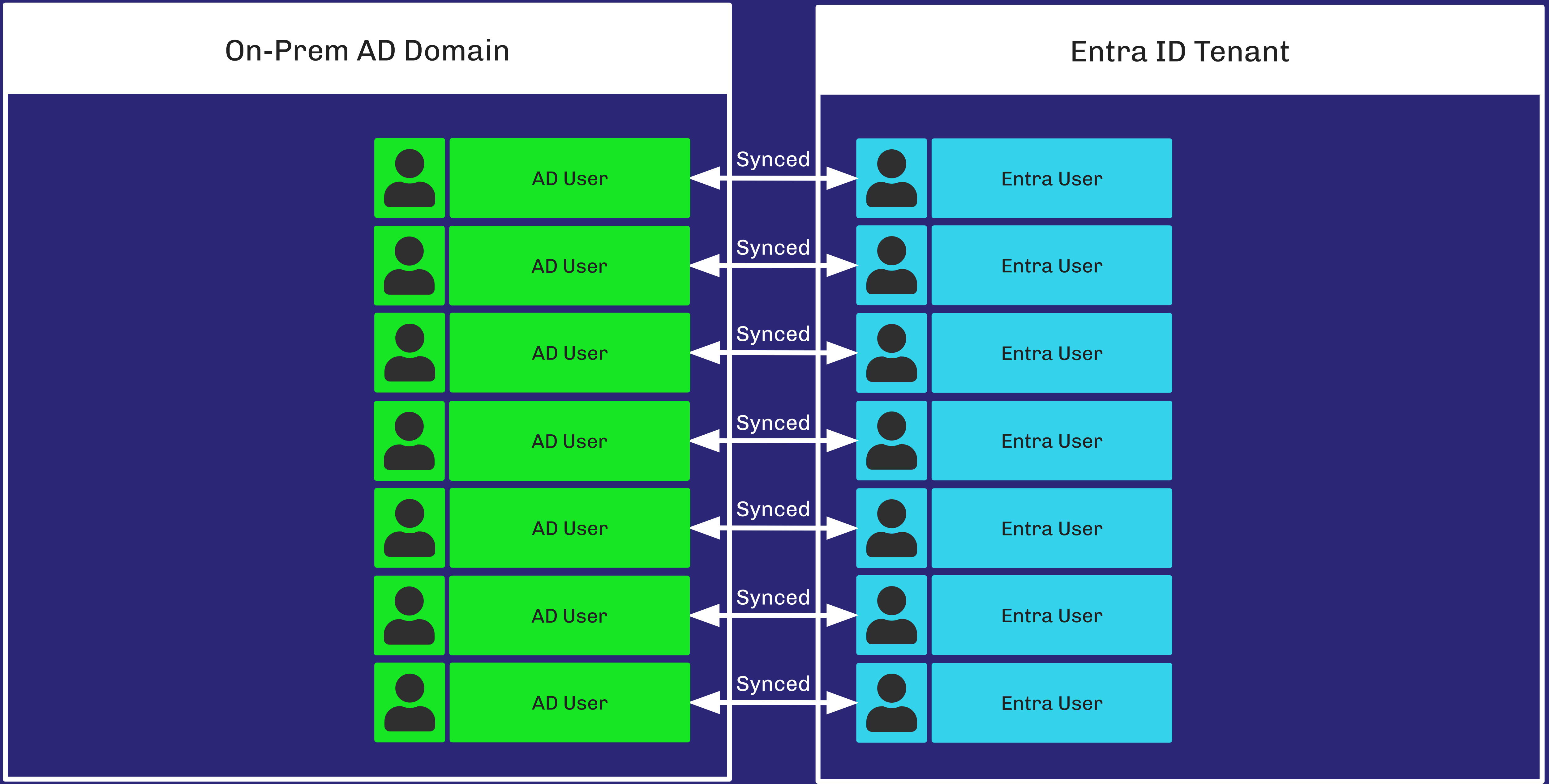
Attack Path Step 7:
Authenticate as the on-prem AD user “DMCGUIRE”, add ourselves to the Domain Admins group.

What should defenders do?

Identify risky attack paths

- Most synced user relationships are harmless.
- Some synced user relationships create immense risk.


On-Prem AD Domain
Entra ID Tenant
AD Group
Domain Admins
Full Control
AD User
Synced
Entra User
Can Reset Password
Entra Role
Global Admin
AD User
Synced
Entra User
Can Grant Role
Has Session
Owner Of
Can Auth As
Computer
App Registration
Service Principal



On-Prem AD Domain

Entra ID Tenant

AD User — Synced — Entra User

AD User — Synced — Entra User

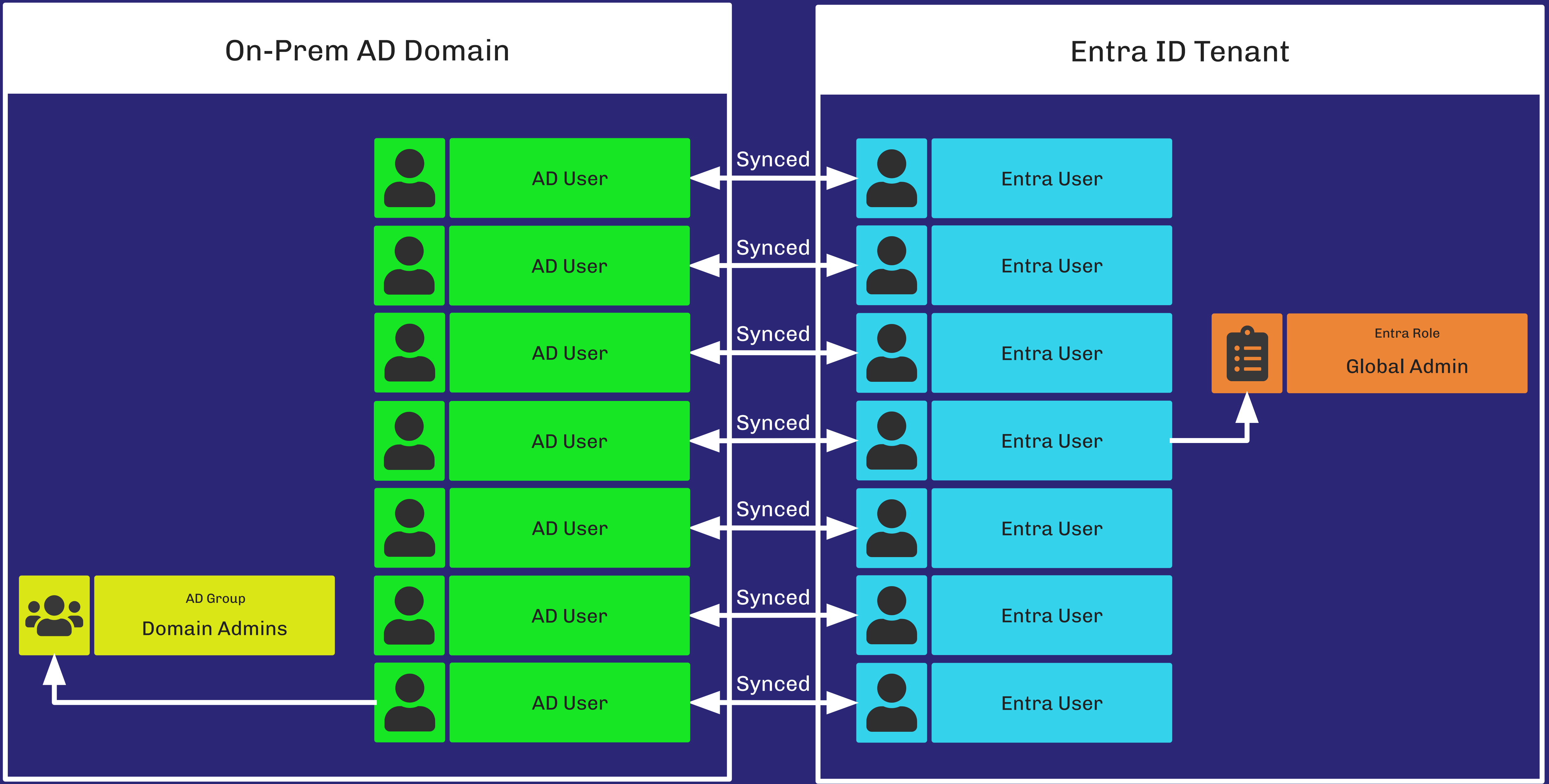
AD User — Synced — Entra User

AD User — Synced — Entra User

AD User — Synced — Entra User

AD User — Synced — Entra User

AD User — Synced — Entra User



On-Prem AD Domain

AD User

AD User

AD User

AD User

AD User

AD User

AD User

AD Group

Domain Admins

Synced

Synced

Synced

Synced

Synced

Synced

Synced

Entra ID Tenant

Entra User

Entra User

Entra User

Entra User

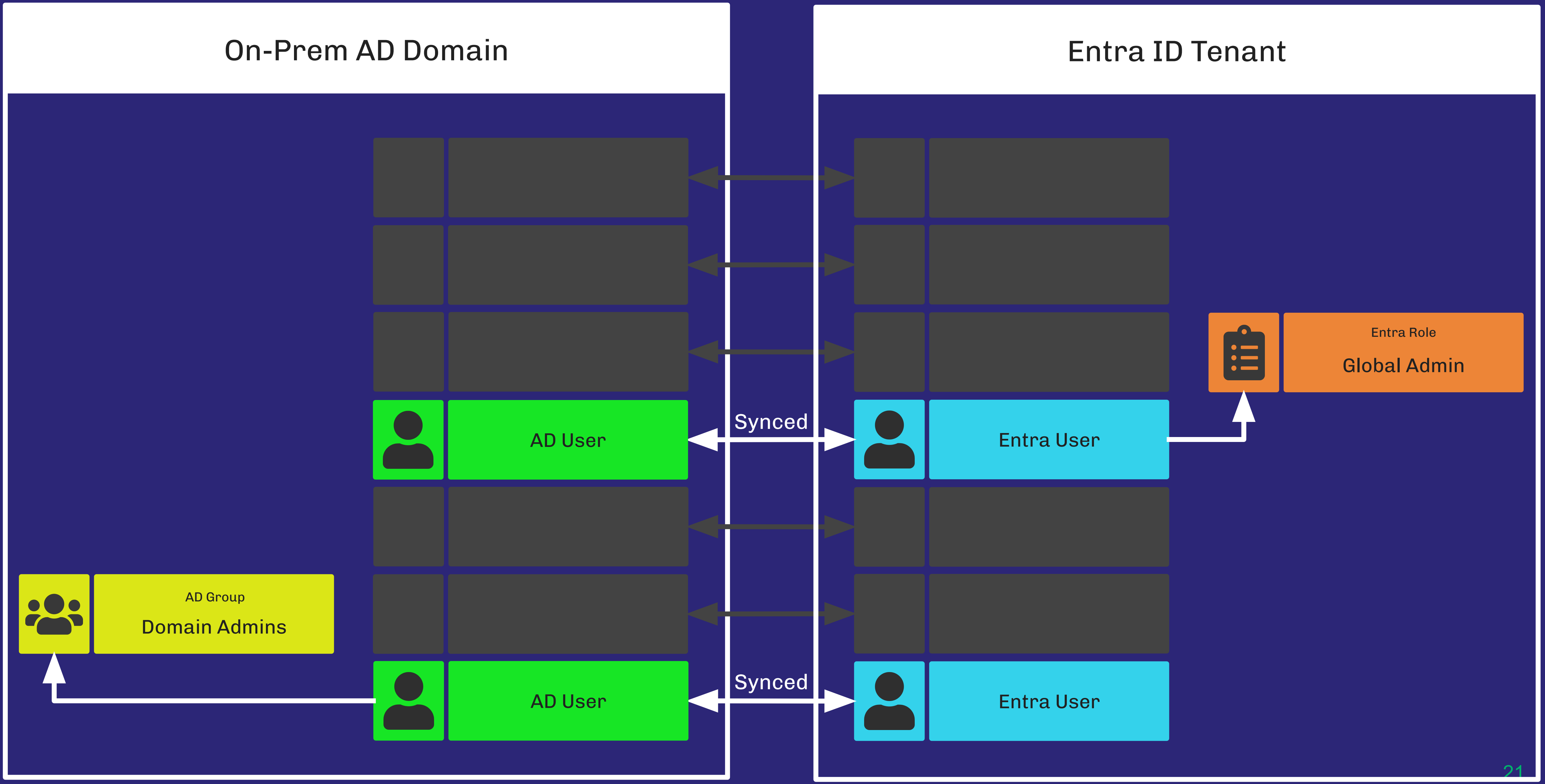
Entra User

Entra User

Entra User

Entra Role

Global Admin



On-Prem AD Domain

Entra ID Tenant

AD User

Synced

Entra User

Entra Role

Global Admin

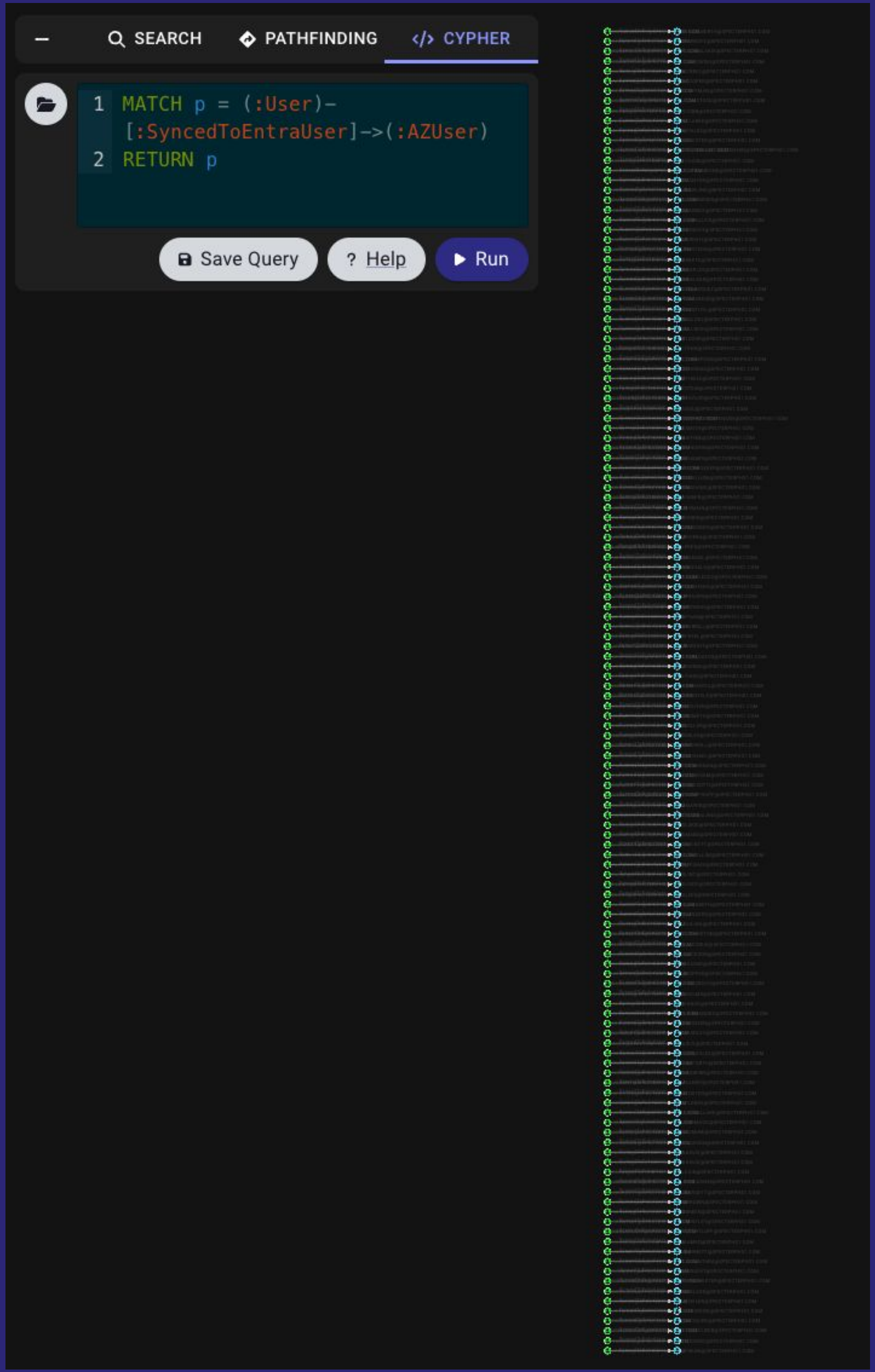
AD Group

Domain Admins

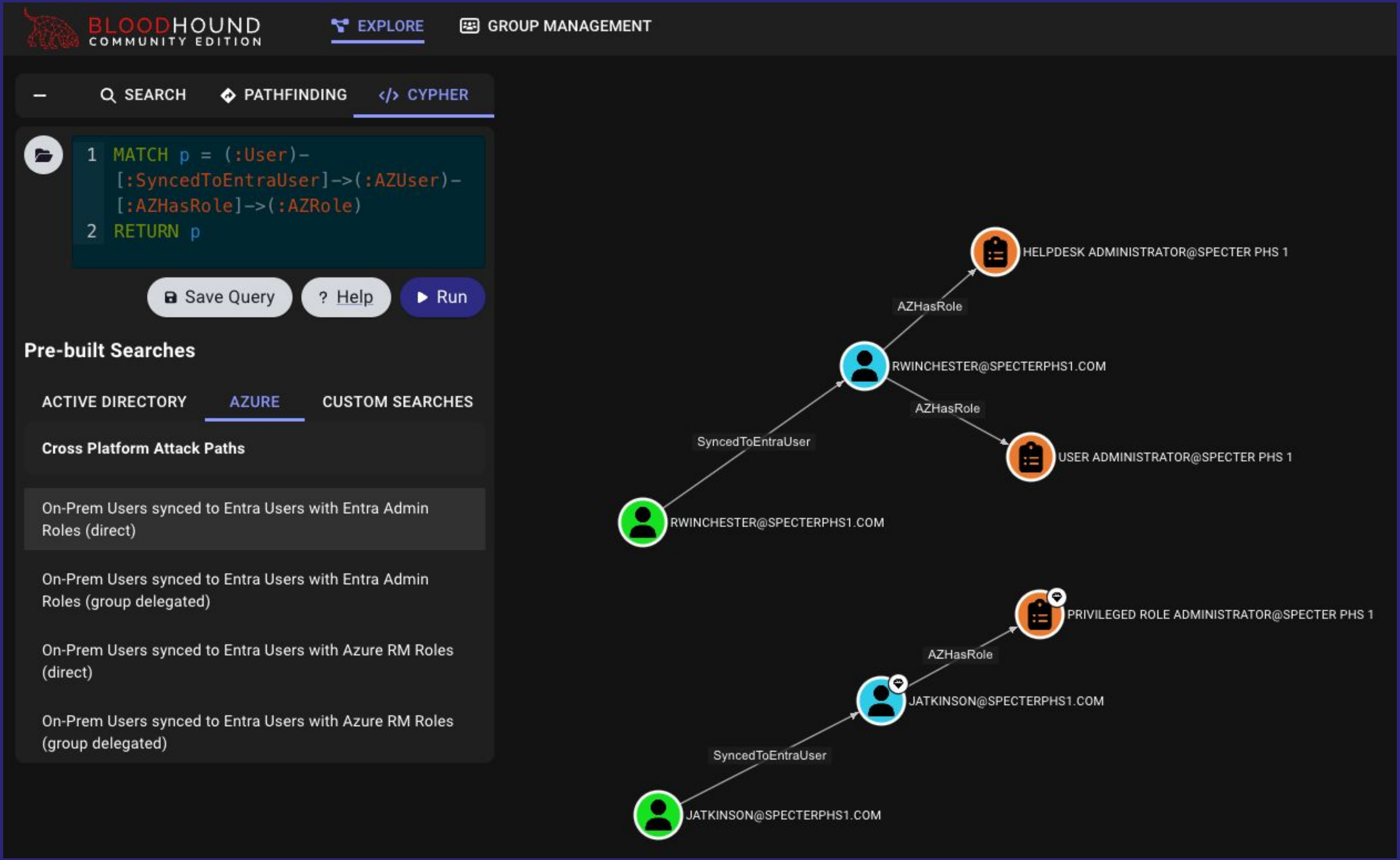
AD User

Synced

Entra User



```
MATCH p = (:User)-[:SyncedToEntraUser]->(:AZUser)
RETURN p
```



```
MATCH p = (:User)-
[:SyncedToEntraUser]->(:AZUser)-
[:AZHasRole]->(:AZRole)
RETURN p
```

Pre-built Searches

Cross Platform Attack Paths

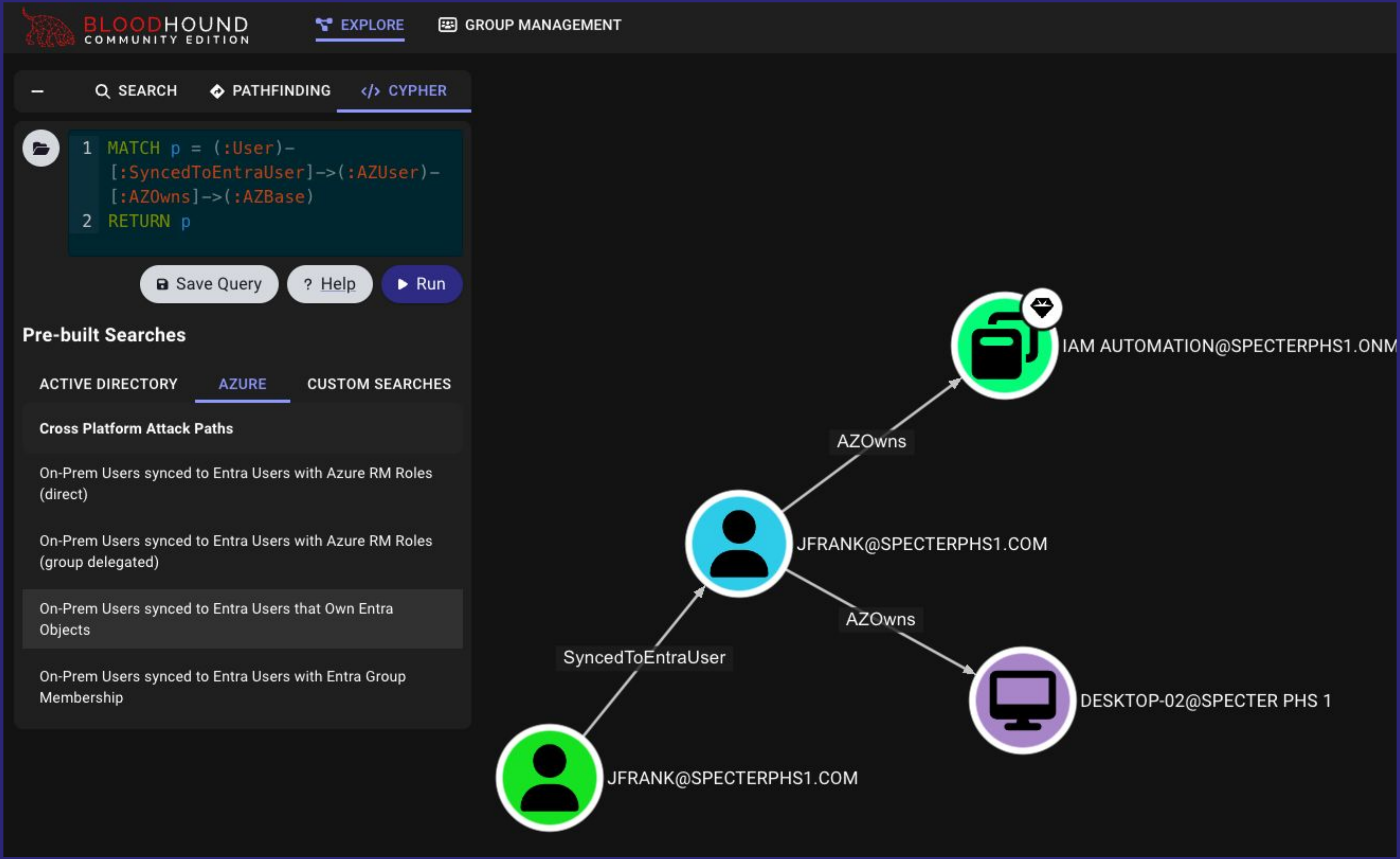
On-Prem Users synced to Entra Users with Entra Admin Roles (direct)

On-Prem Users synced to Entra Users with Entra Admin Roles (group delegated)

On-Prem Users synced to Entra Users with Azure RM Roles (direct)

On-Prem Users synced to Entra Users with Azure RM Roles (group delegated)

HELPDESK ADMINISTRATOR@SPECTER PHS 1
AZHasRole
RWINCHESTER@SPECTERPHS1.COM
AZHasRole
USER ADMINISTRATOR@SPECTER PHS 1
SyncedToEntraUser
RWINCHESTER@SPECTERPHS1.COM
PRIVILEGED ROLE ADMINISTRATOR@SPECTER PHS 1
AZHasRole
JATKINSON@SPECTERPHS1.COM
SyncedToEntraUser
JATKINSON@SPECTERPHS1.COM



```
MATCH p = (:User)-[:SyncedToEntraUser]->(:AZUser)-[:AZOwns]->(:AZBase)
RETURN p
```

Pre-built Searches

ACTIVE DIRECTORY | AZURE | CUSTOM SEARCHES

Cross Platform Attack Paths

On-Prem Users synced to Entra Users with Azure RM Roles (direct)

On-Prem Users synced to Entra Users with Azure RM Roles (group delegated)

On-Prem Users synced to Entra Users that Own Entra Objects

On-Prem Users synced to Entra Users with Entra Group Membership

What should defenders do?

Identify risky attack paths

- Most synced user relationships are harmless.
- Some synced user relationships create immense risk.

Eliminate the attack paths that you can

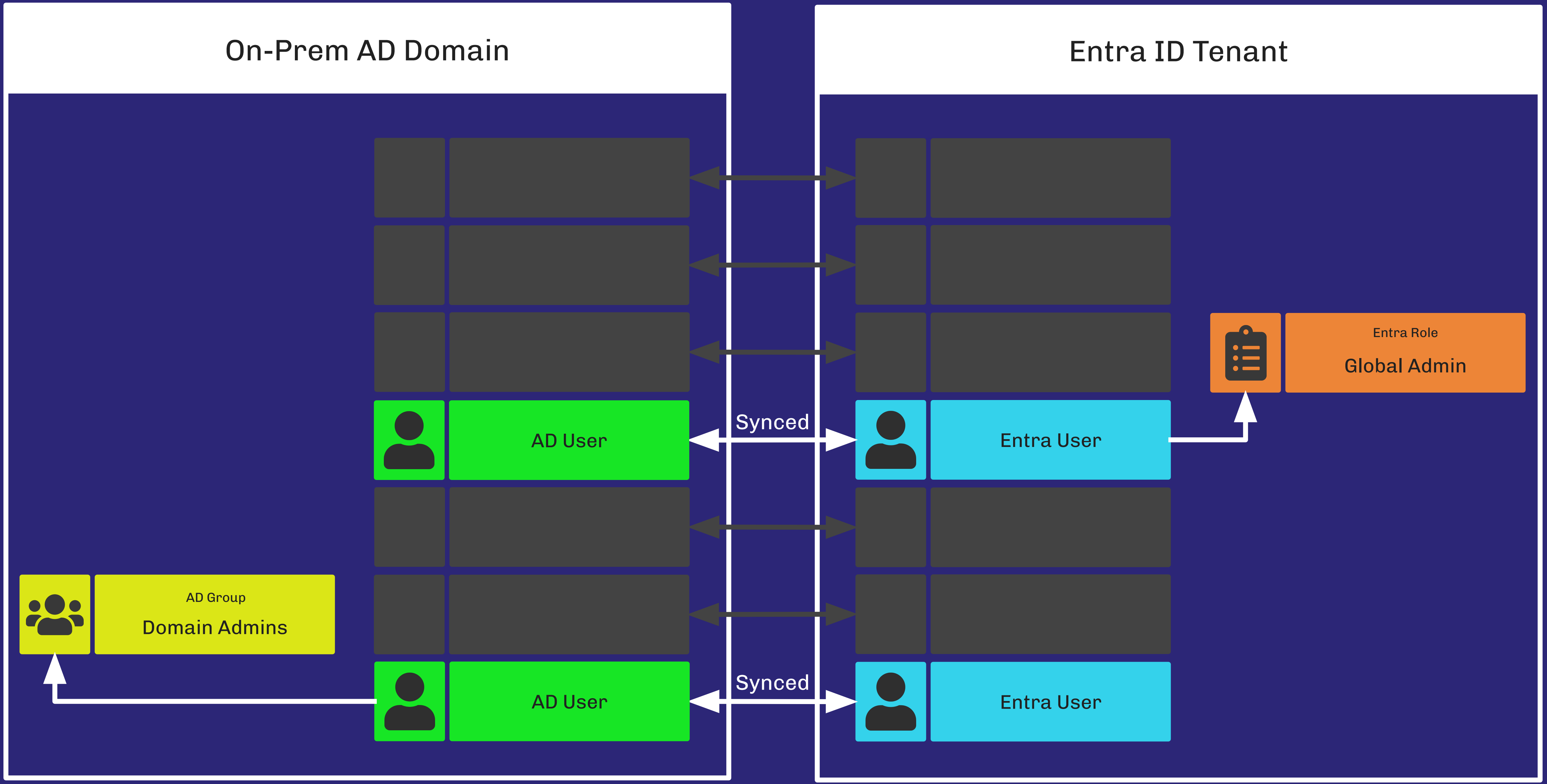
- An ounce of prevention is worth a pound of cure.
- An attacker can’t execute an attack path if the path <u>doesn’t exist</u>.

John Lambert
@JohnLaTwC

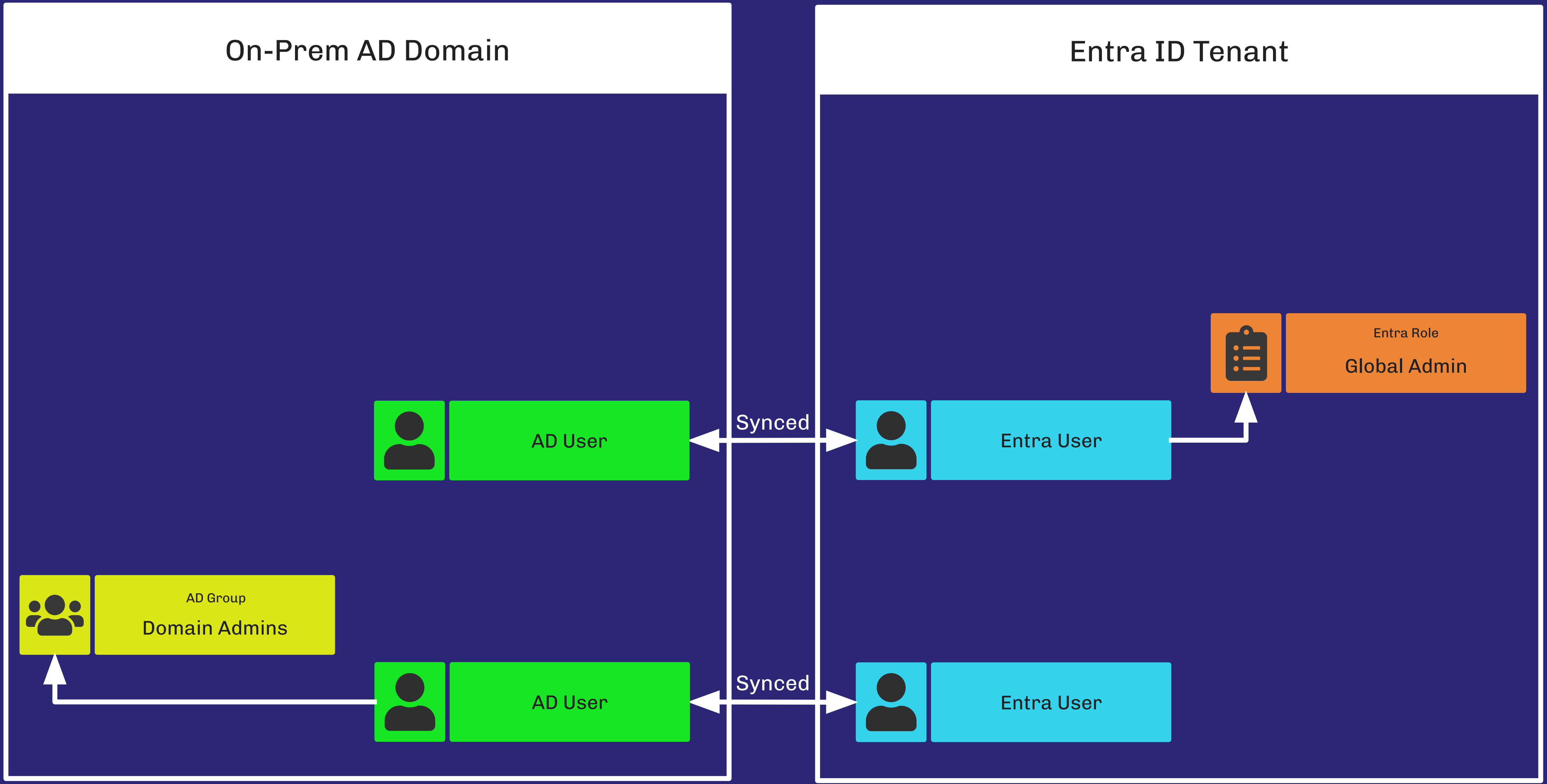
8/10 Prevention is the guardian of detection. Prevention creates the whitespace to detect and respond to the most important things.

4:05 PM · Dec 30, 2015

https://medium.com/@johnlatwc/defenders-mindset-319854d10aaa



On-Prem AD Domain
Entra ID Tenant
Entra Role
Global Admin
AD User
Synced
Entra User
AD Group
Domain Admins
AD User
Synced
Entra User


On-Prem AD Domain
Entra ID Tenant
Entra Role
Global Admin
AD User
Synced
Entra User
AD Group
Domain Admins
AD User
Synced
Entra User

SPECTEROPS

What should defenders do?

Identify risky attack paths

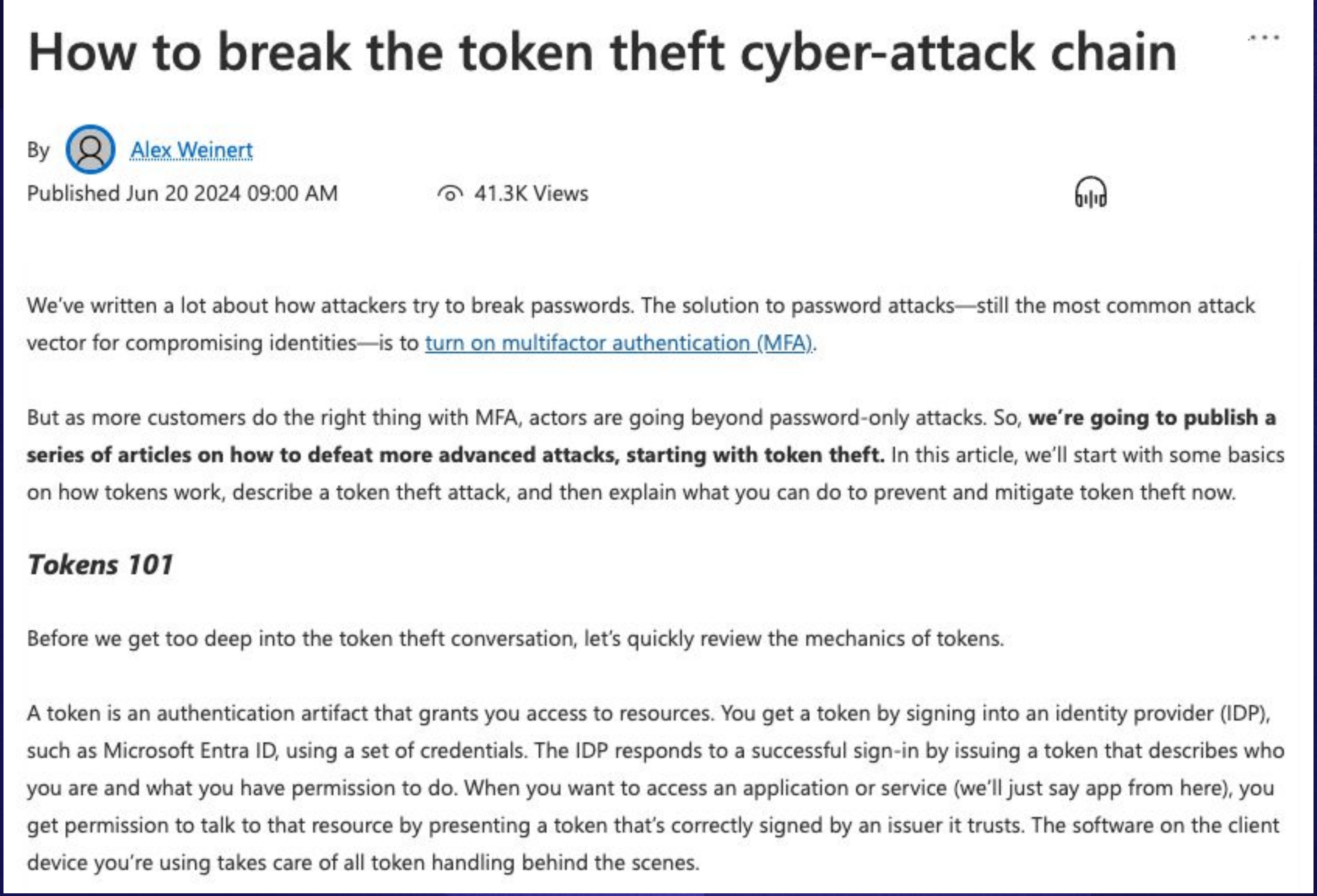
- Most synced user relationships are harmless.
- Some synced user relationships create immense risk.

Eliminate the attack paths that you can

- An ounce of prevention is worth a pound of cure.
- An attacker can't execute an attack path if the path doesn't exist.

Mitigate the attack paths that remain

- Use preventative tools like Conditional Access and token binding.
- Create high-fidelity, high-importance alerts.



How to break the token theft cyber-attack chain

By Alex Weinert

Published Jun 20 2024 09:00 AM

41.3K Views

We've written a lot about how attackers try to break passwords. The solution to password attacks—still the most common attack vector for compromising identities—is to turn on multifactor authentication (MFA).

But as more customers do the right thing with MFA, actors are going beyond password-only attacks. So, **we're going to publish a series of articles on how to defeat more advanced attacks, starting with token theft.** In this article, we'll start with some basics on how tokens work, describe a token theft attack, and then explain what you can do to prevent and mitigate token theft now.

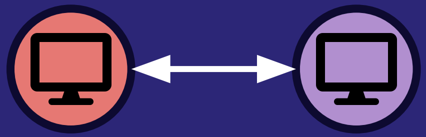
Tokens 101

Before we get too deep into the token theft conversation, let's quickly review the mechanics of tokens.

A token is an authentication artifact that grants you access to resources. You get a token by signing into an identity provider (IDP), such as Microsoft Entra ID, using a set of credentials. The IDP responds to a successful sign-in by issuing a token that describes who you are and what you have permission to do. When you want to access an application or service (we'll just say app from here), you get permission to talk to that resource by presenting a token that's correctly signed by an issuer it trusts. The software on the client device you're using takes care of all token handling behind the scenes.

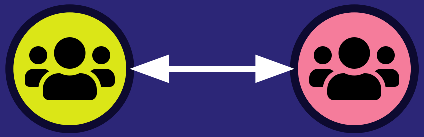
https://techcommunity.microsoft.com/t5/microsoft-entra-blog/how-to-break-the-token-theft-cyber-attack-chain/ba-p/4062700

What’s next?



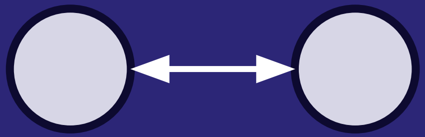
Host equivalency

Hybrid-joined computers are represented as both “Computer” and “Device” nodes, but control of one guarantees control of the other.



Group sync/writeback

Permissions delegated to groups will make cross-platform attack paths that traverse group sync/writeback configurations even more difficult to identify without tools like BloodHound.



More…

We have our eyes on other hybrid and inter-platform attack paths.

Further Reading/Viewing

- Alex Weinert: How to break the token theft cyber-attack chain
- Daniel Heinsen: I'd TAP That Pass
- Adam Chester: WAM BAM - Recovering Web Tokens From Office
- Melvin Flangvik: Post-Compromise Session Hijacking with Mythic C2 and RoadTools!

Further Reading/Viewing

- Dirk-jan Mollema: Obtaining Domain Admin from Azure AD by abusing Cloud Kerberos Trust
- Fabien Bader: From on-prem to Global Admin without password reset
- Nestori Syynimaa: Stealing and faking Azure AD device identities
- Renos Nikolaou: Abusing Azure Arc for lateral movement

SPECTEROPS

Thank you!

Get BloodHoundCE: https://ghst.ly/bh-github

Get Mythic: https://github.com/its-a-feature/Mythic

Join the BloodHound Slack: https://ghst.ly/BHSlack

Get the 2024 BloodHound shirt:
https://ghst.ly/bh-tshirt-24

All funds go directly to the American Cancer Society

We are HIRING: https://specterops.io/careers/#careers