Mostly harmless?

The Helpdesk Admin (and some other unsuspicious roles) as Tier 0 Admins

About us

Michael Freistetter

Cloud Solution Architect

Unified Support Team
The team supporting customers to get the most out of our products and services

Dagmar Heidecker

Cyber Security Consultant

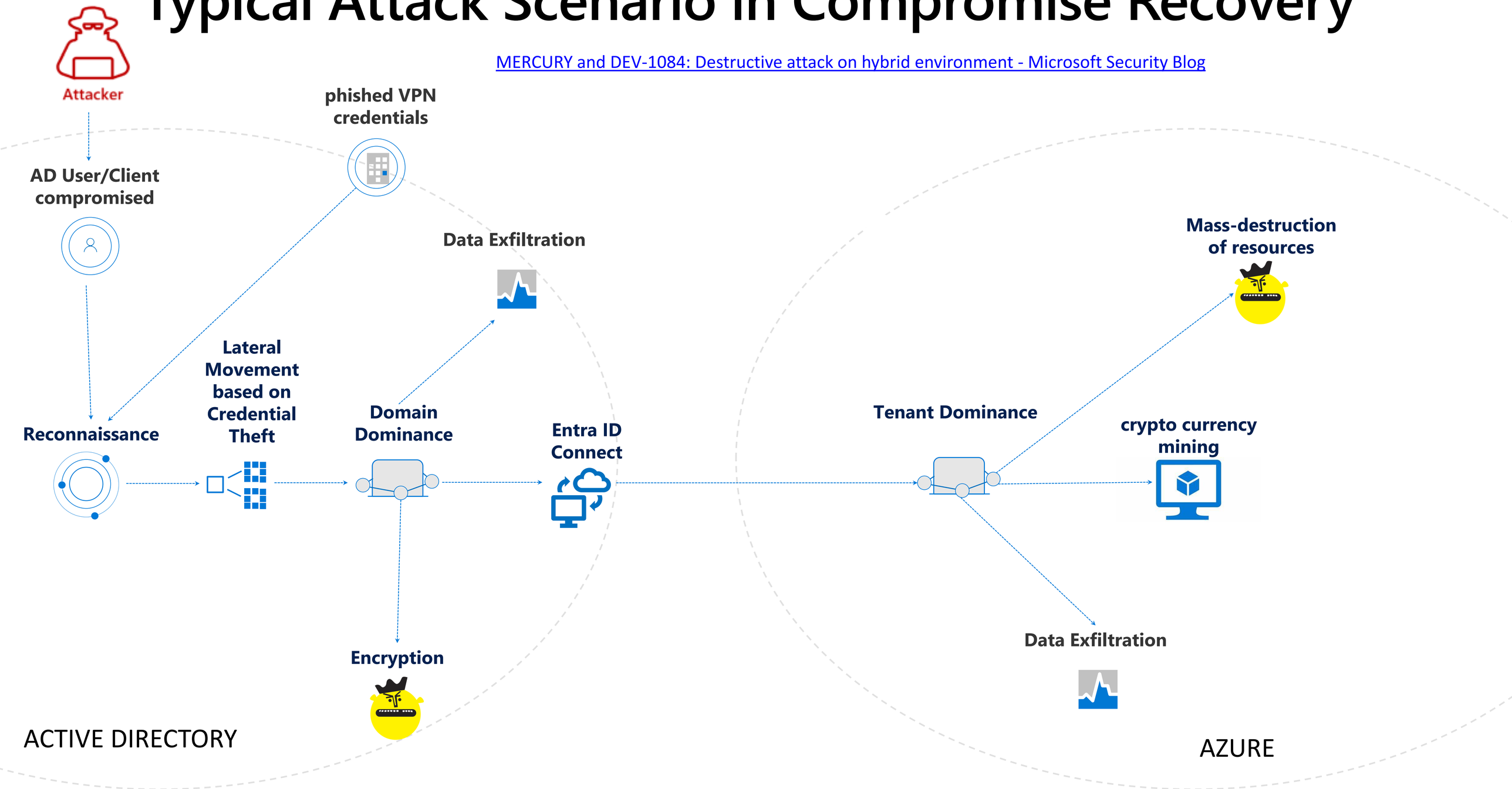
Microsoft Security CyberOps Resilience
Security Service Line | Industry Solutions
https://aka.ms/DagmarHeidecker

Agenda

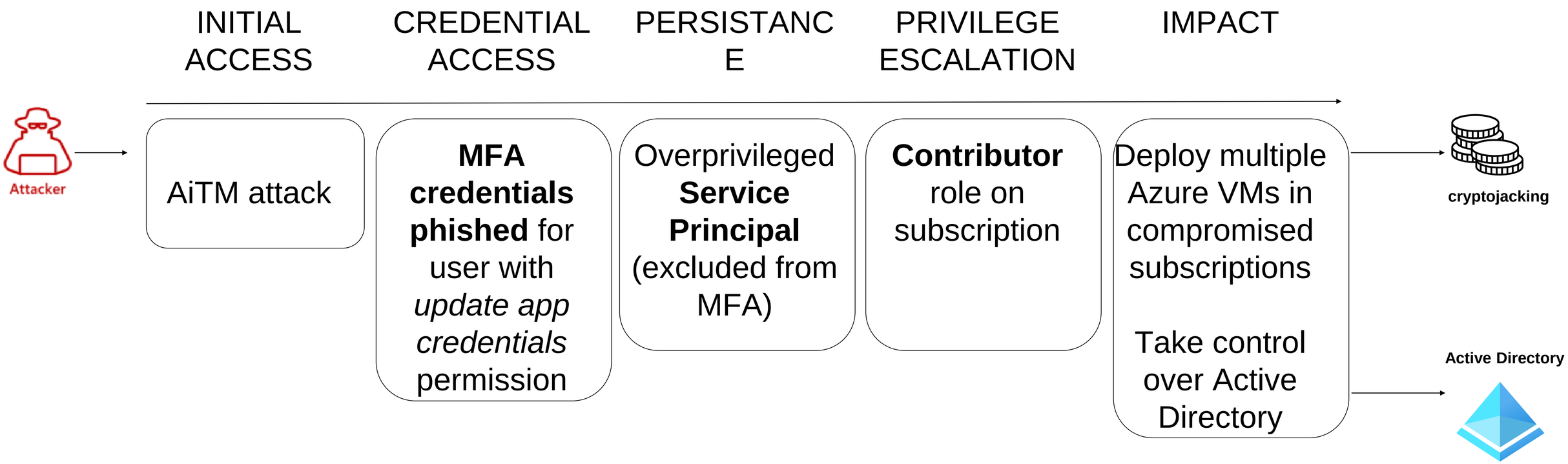
While protecting Active Directory, don’t ignore other paths to your “kingdom”!

Typical Attack Scenario in Compromise Recovery

[MERCURY and DEV-1084: Destructive attack on hybrid environment - Microsoft Security Blog]



Attackers are adopting quickly…



AiTM Attack Technical Overview

- AiTM attacks involve an attacker intercepting communication between two parties.
- The attacker can obtain sensitive information such as passwords or access tokens.
- Through the usage of phishing tactics, the attacker can compromise an authentication session.

Refresher

Azure Service Principals

For a service to connect to resources in a subscription, it needs an associated service principal within that subscription's tenant.

Managed Identity
(formerly known as Managed Service Identity (MSI))

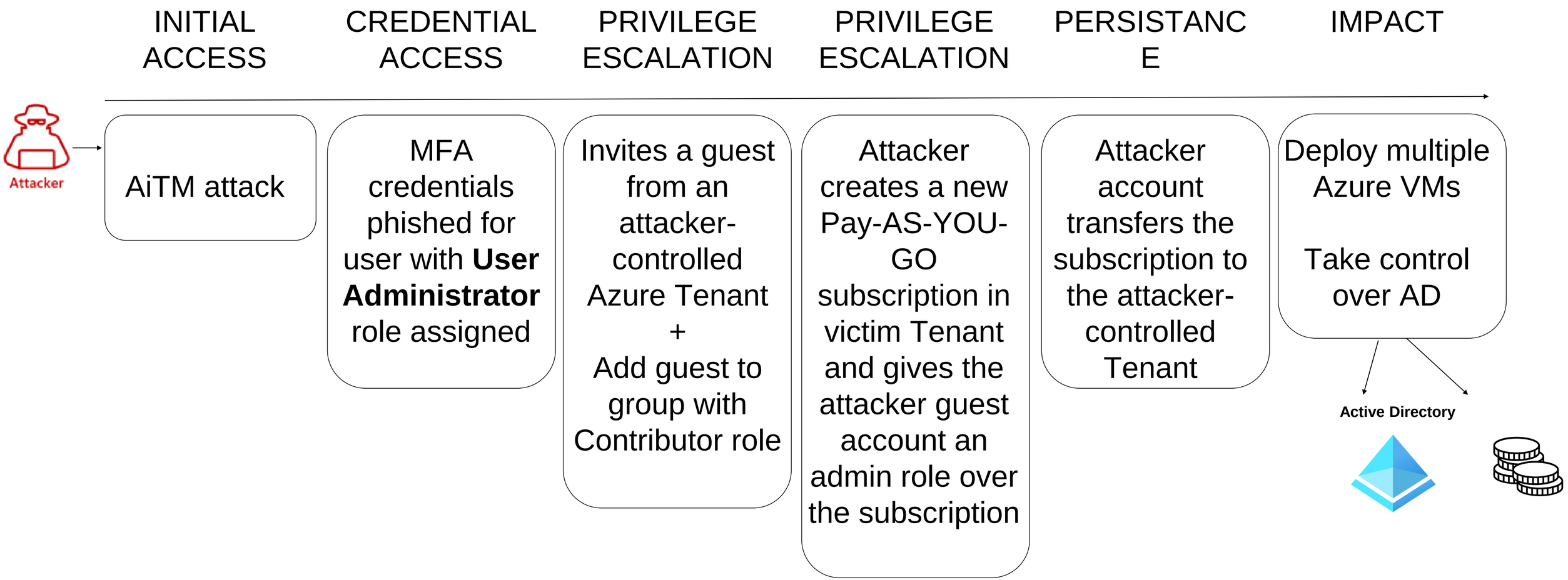
- Can be used to authenticate to any resource that supports Entra authentication.
- Created automatically.
- No need to manage credentials.
- Azure services supporting Managed Identities: https://aka.ms/AzureManagedIdentityStatus

Application
(aka Enterprise Apps, Service Principals)

- When an application is given permission to access resources in a tenant (upon registration or consent), a service principal object is created.
- Mechanisms for authentication: certificates and client secrets
- The default role for a password-based authentication Service Principal *was* Contributor in the past.

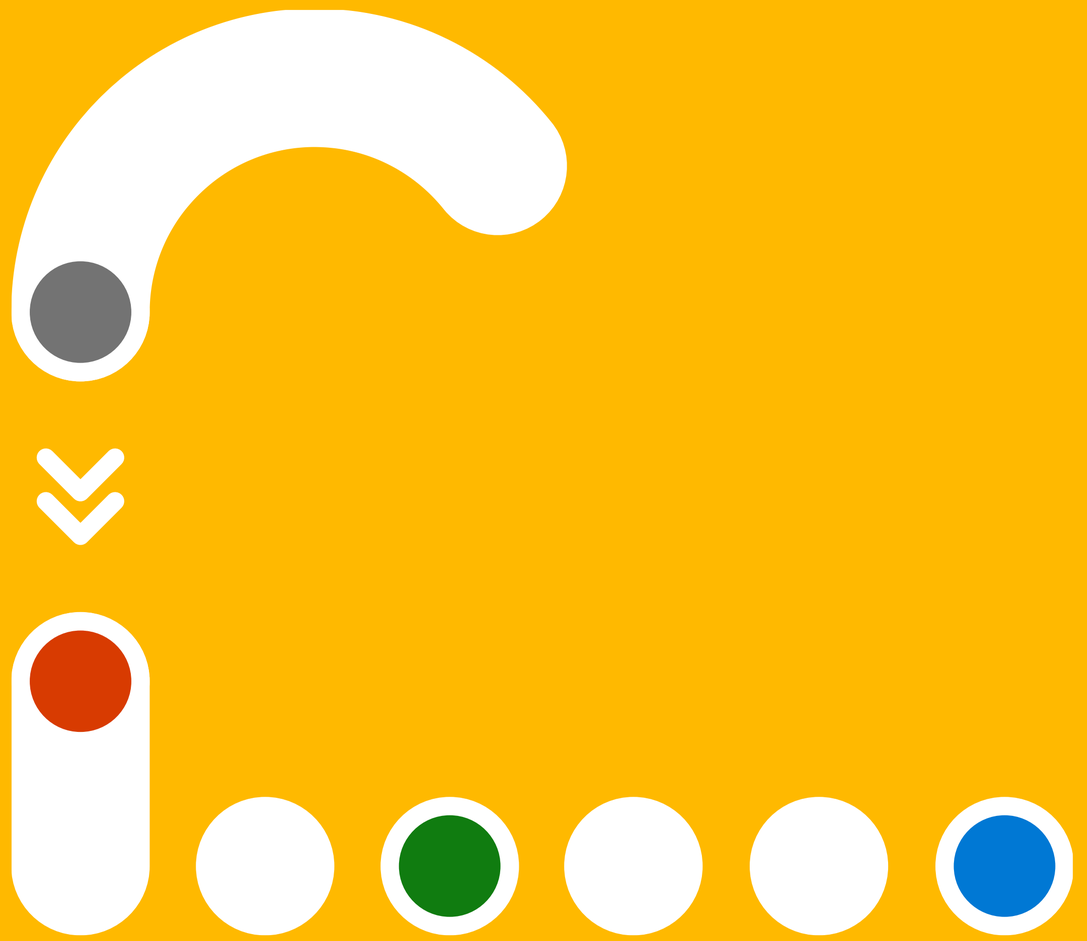
Azure User Account

Attackers are adopting quickly…

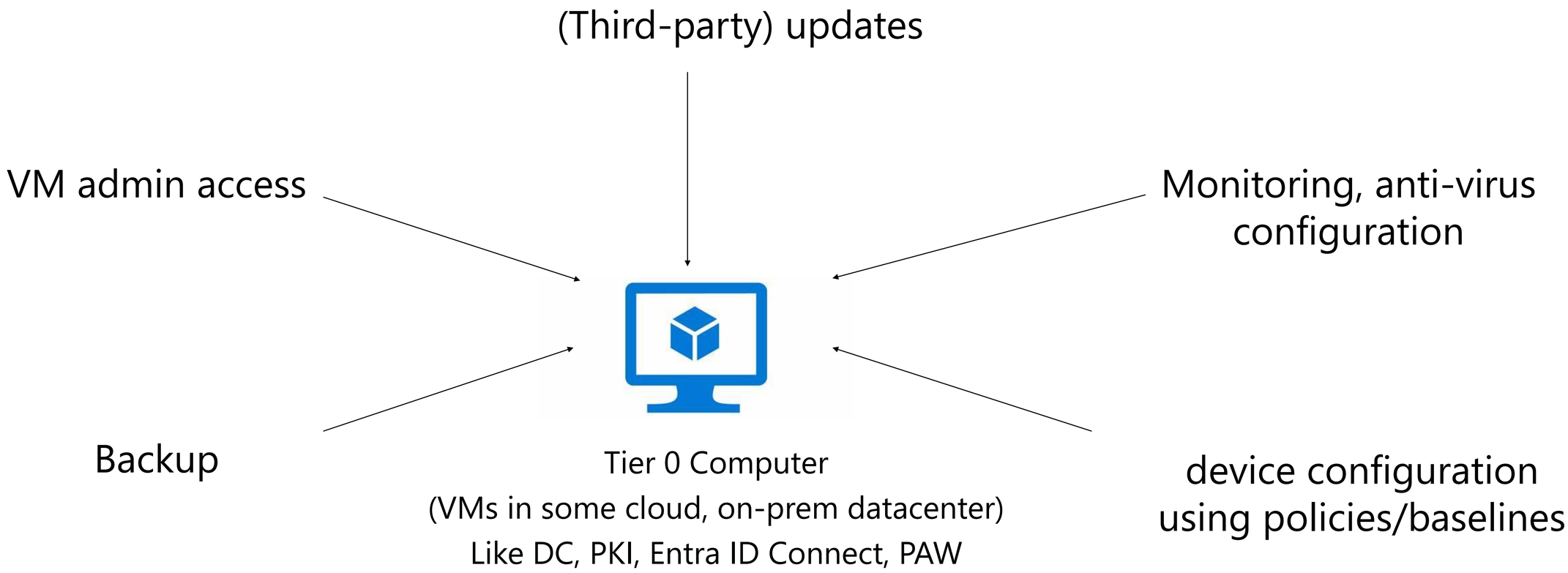


- The User Administrator role is a PRIVILEGED role, because it includes several PRIVILEGED permissions.
- microsoft.directory/users/inviteGuest is not classified as PRIVILEGED

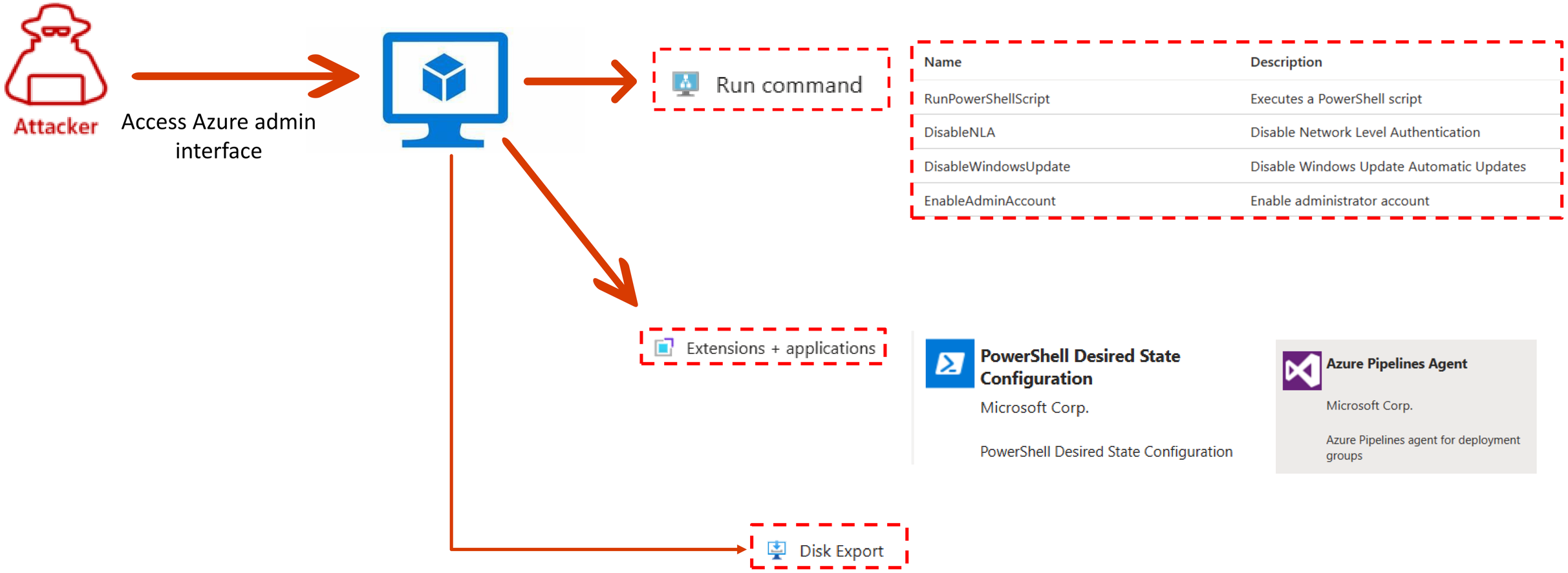
From Azure to AD – What happened?



Azure/Entra ID & AD Tier 0 Involvement (Examples)



Attacker & Azure VM (Examples)



Name	Description
RunPowerShellScript	Executes a PowerShell script
DisableNLA	Disable Network Level Authentication
DisableWindowsUpdate	Disable Windows Update Automatic Updates
EnableAdminAccount	Enable administrator account

PowerShell Desired State Configuration

Microsoft Corp.

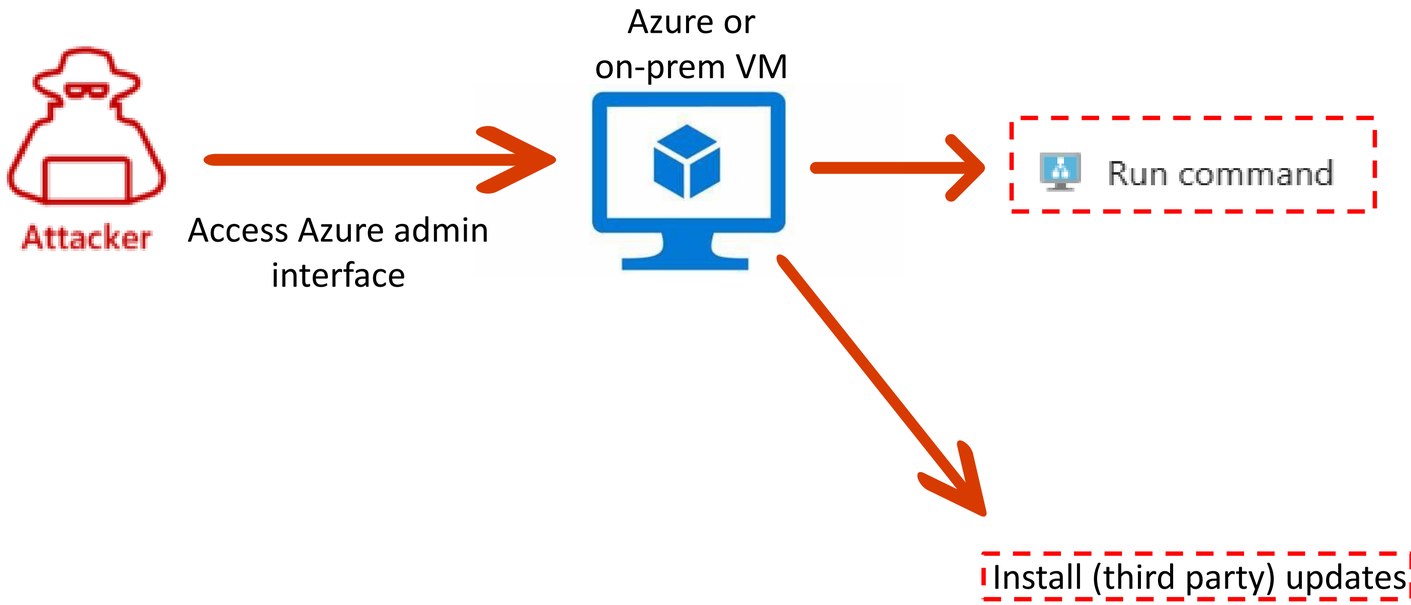
PowerShell Desired State Configuration

Azure Pipelines Agent

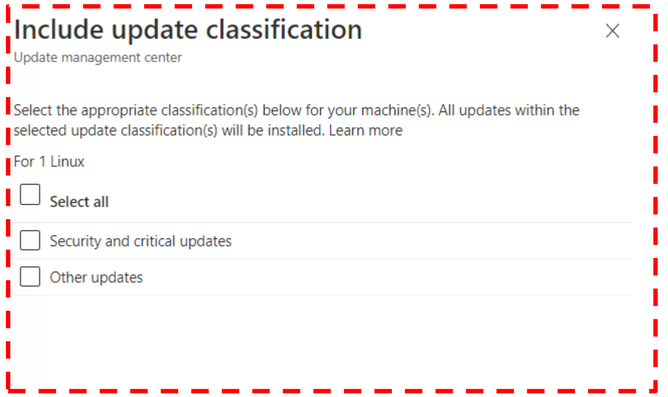
Microsoft Corp.

Azure Pipelines agent for deployment groups

Attacker & Azure Arc (Examples)



Create Or Update	The operation will create a new Run command to update an existing Run Command
Delete	The operation will delete or stop an existing Run command
Get	The operation will get details for an existing Run Command
List	The operation will get all the Run Commands for an Arc-enabled server
Update	The operation will update an existing Run Command



See https://aka.ms/arc for more details about Azure Arc.

Azure Arc: Security Considerations for Tier 0 Assets*

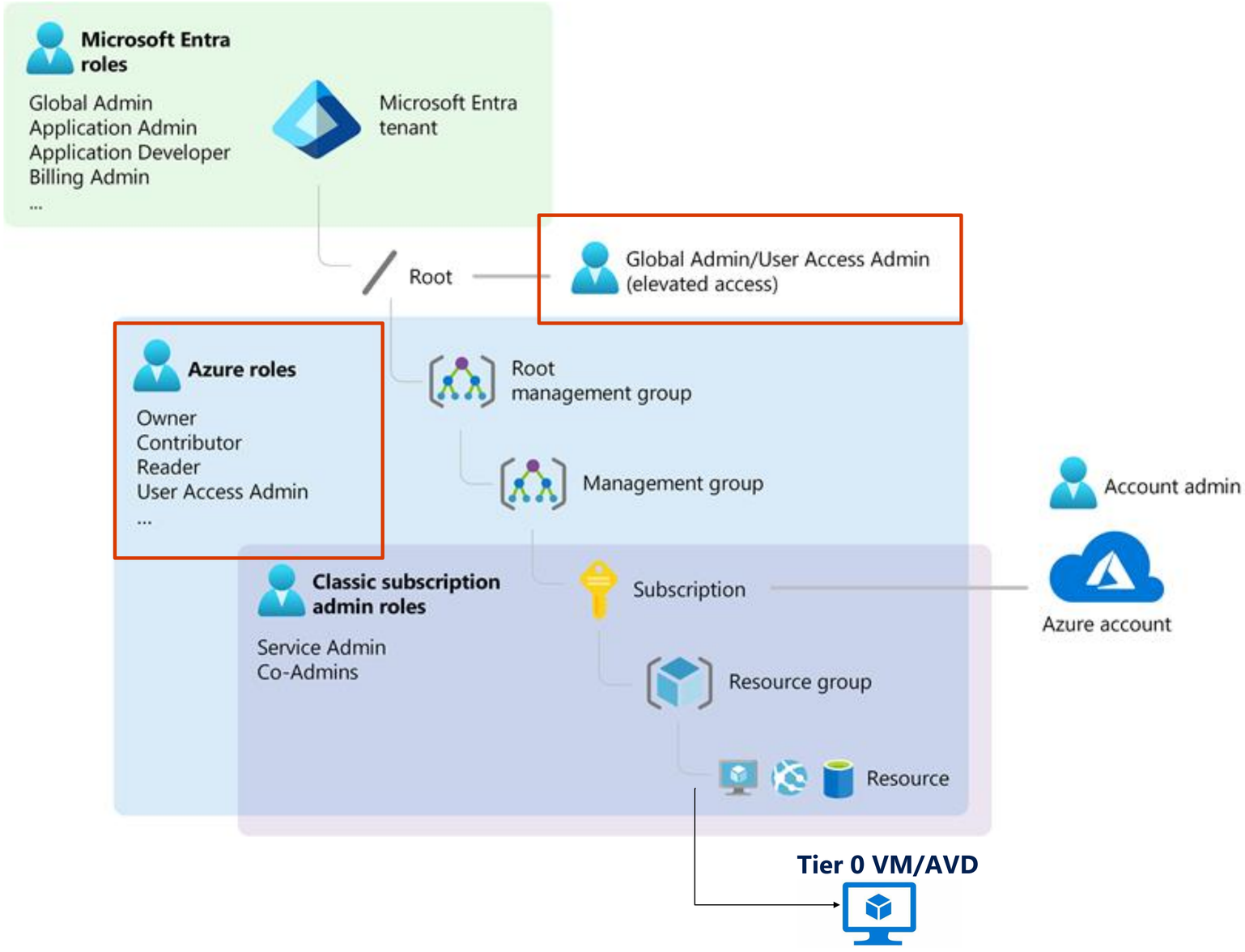
Dedicated Tier 0 Azure Subscription* OR even Management Group

Disable unnecessary management features

- Disabling remote access capabilities
- Setting an extension allowlist for the extensions you intend to use, or disabling the extension manager if you are not using extensions
- Disabling the machine configuration agent if you don’t intend to use machine configuration policies**

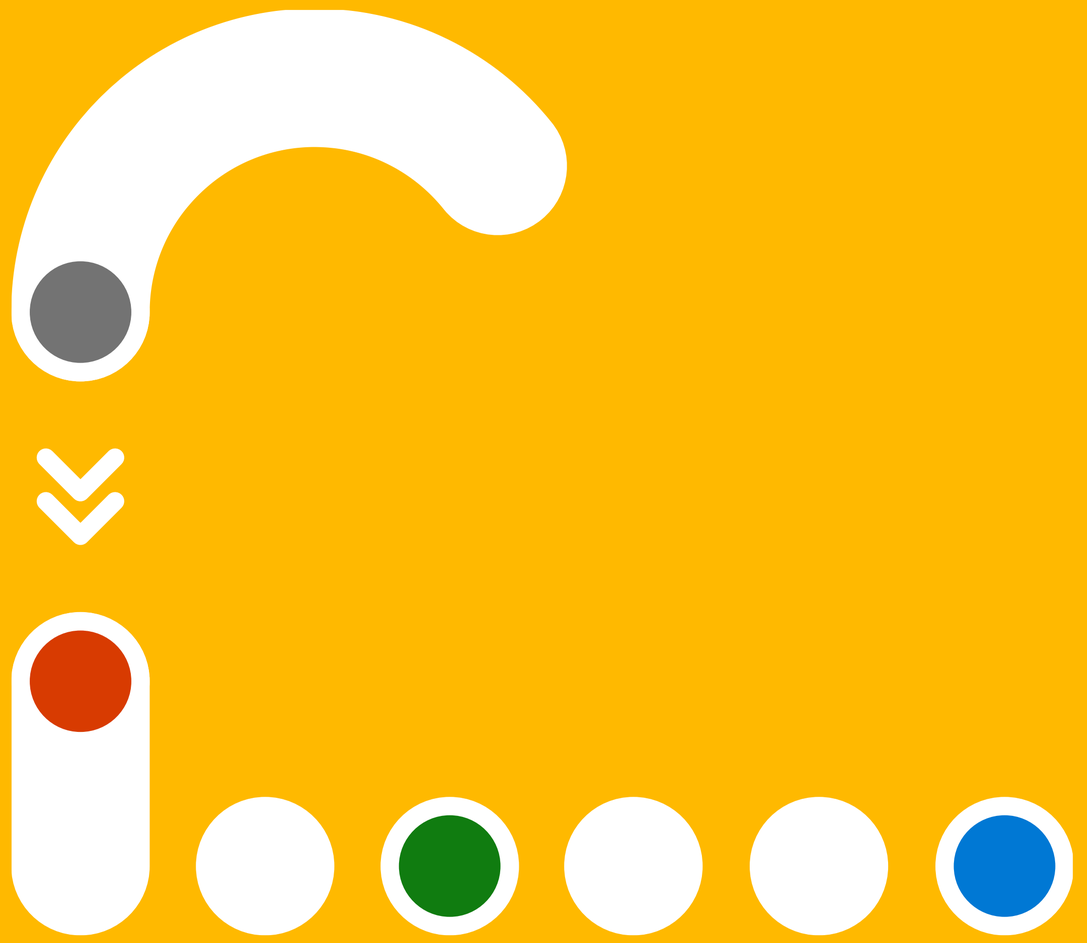
* https://learn.microsoft.com/en-us/azure/azure-arc/servers/security-overview#security-considerations-for-tier-0-assets
** Azure Connected Machine agent command line tool commands provided at https://learn.microsoft.com/en-us/azure/azure-arc/servers/azcmagent

How Entra ID & Azure Roles are related

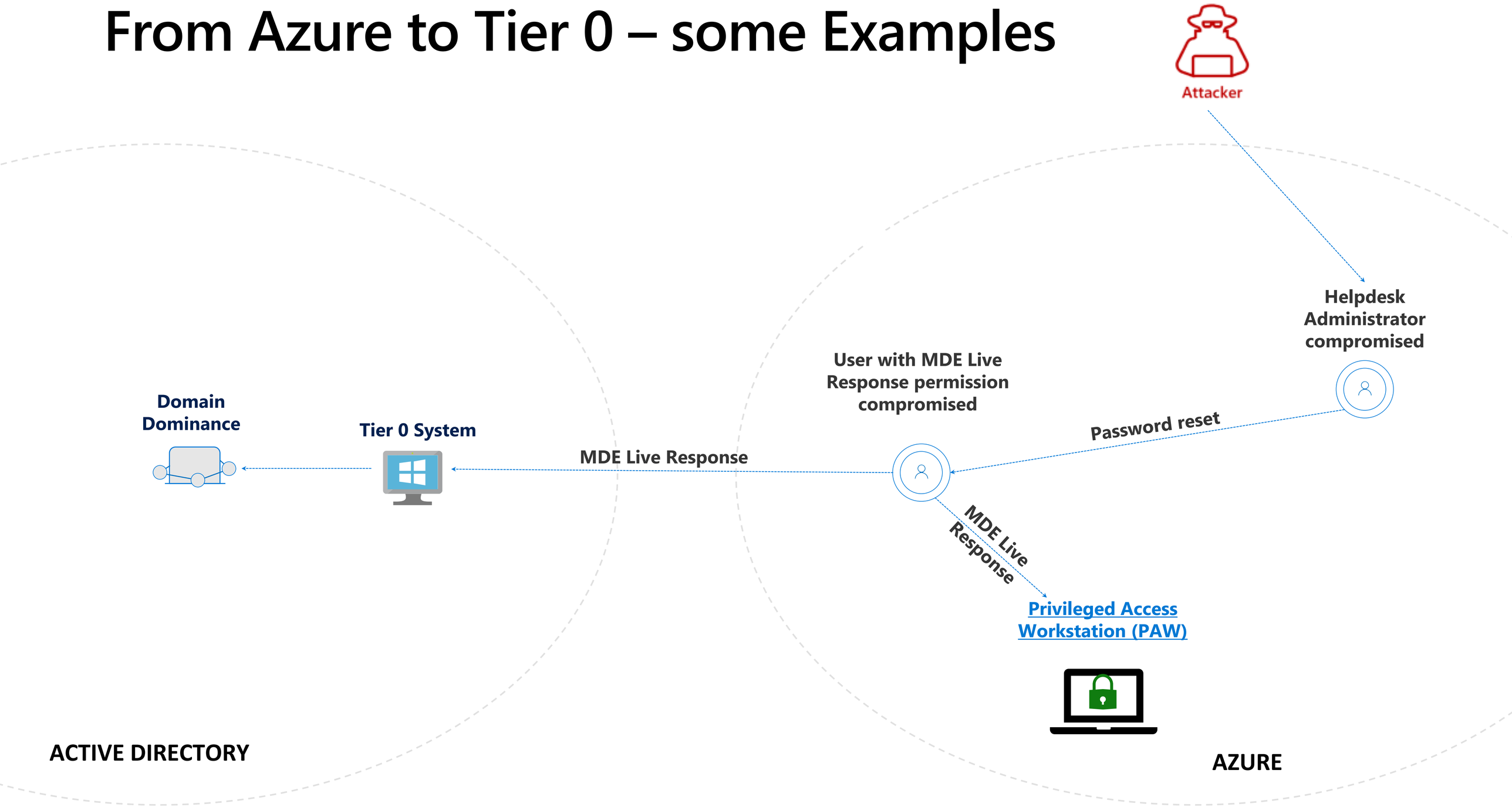


Controlling Access to MDE Life Response

Leveraging MDE Device Groups



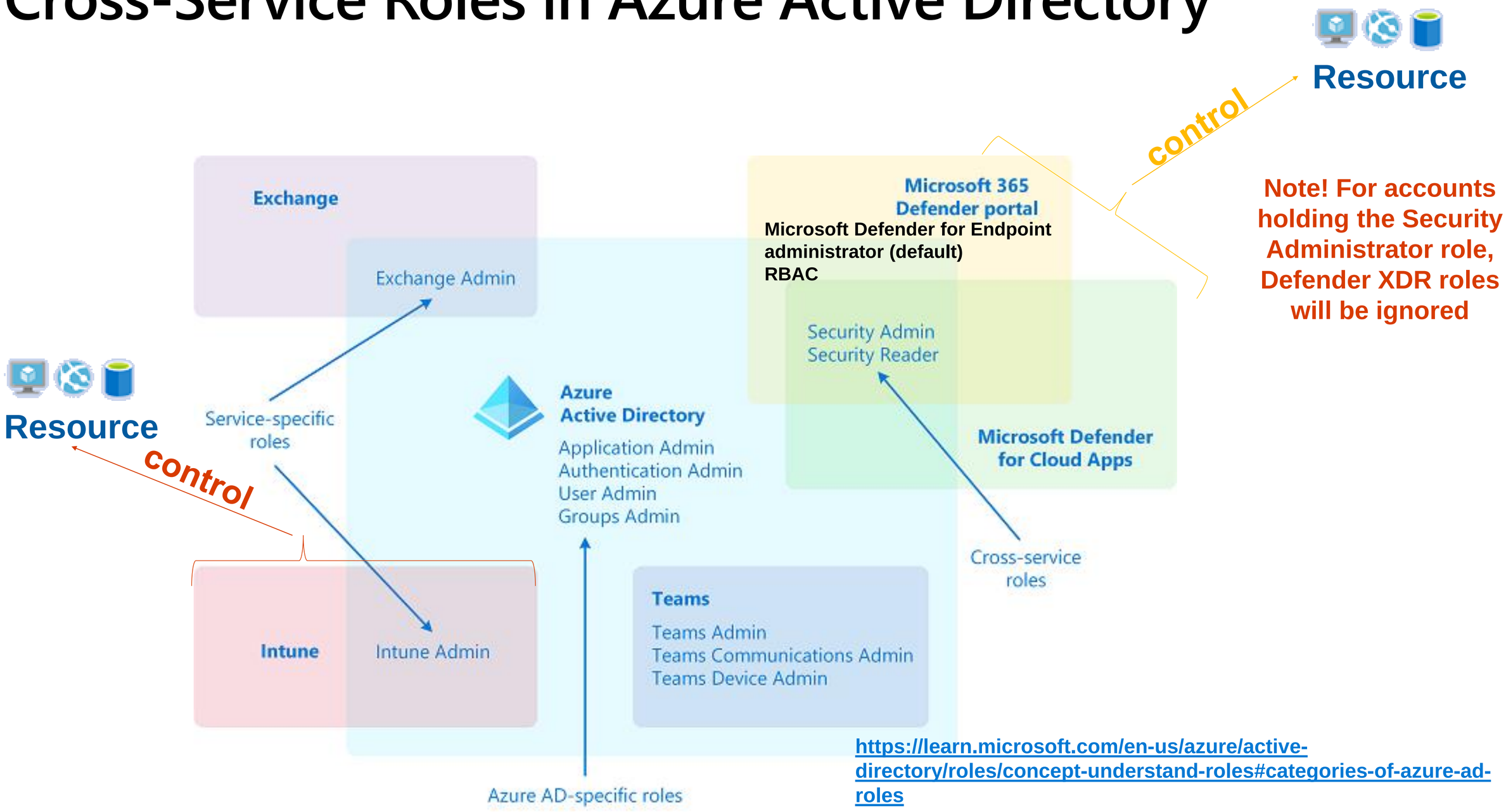
From Azure to Tier 0 – some Examples



Defender for Endpoint – Live Response

- Real-time live connection to a remote MDE onboarded system
  - Run basic and advanced commands to do investigative work on a device.
  - Download files such as malware samples and outcomes of PowerShell scripts.
  - Download files in the background
  - Upload a PowerShell script or executable to the library and run it on a device from a tenant level.
  - Take or undo remediation actions. Extendable (write your own command, build your own tool)
- RBAC + permissions applied

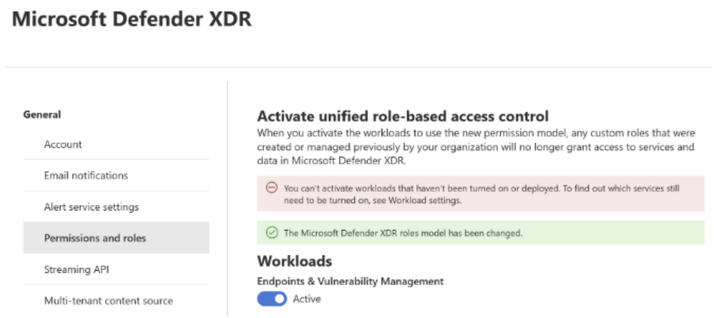
Cross-Service Roles in Azure Active Directory



https://learn.microsoft.com/en-us/azure/active-directory/roles/concept-understand-roles#categories-of-azure-ad-roles

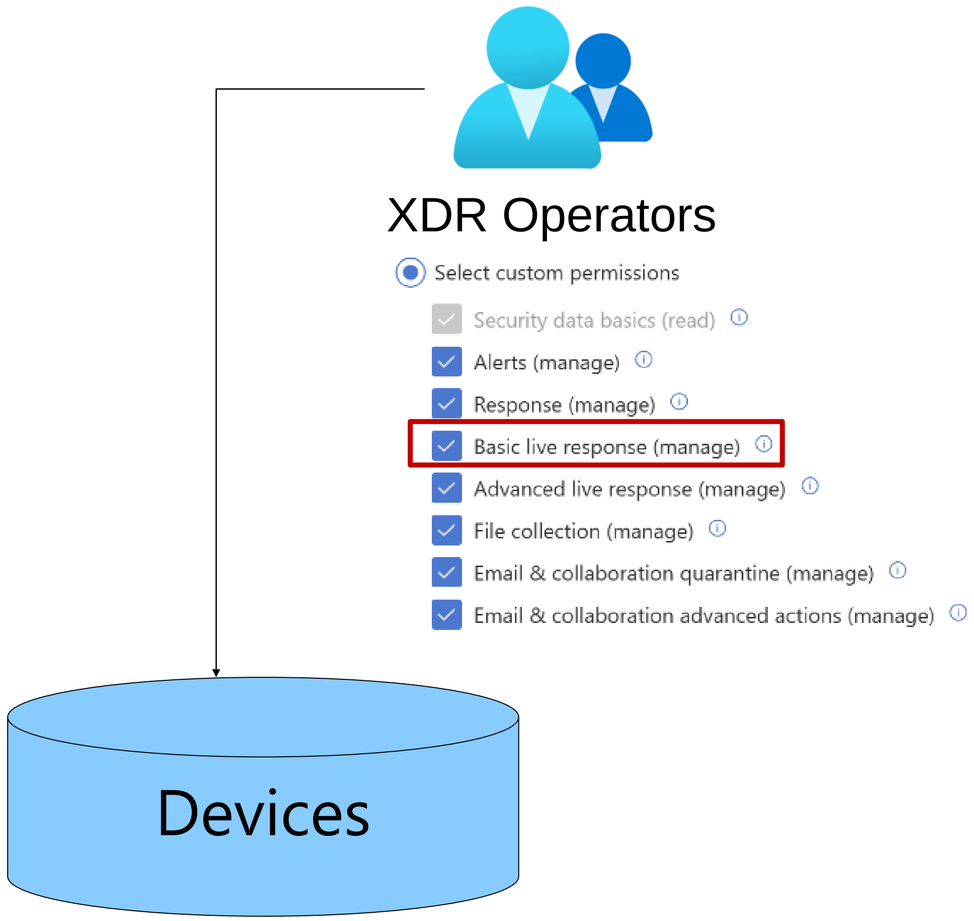
Defender XDR RBAC

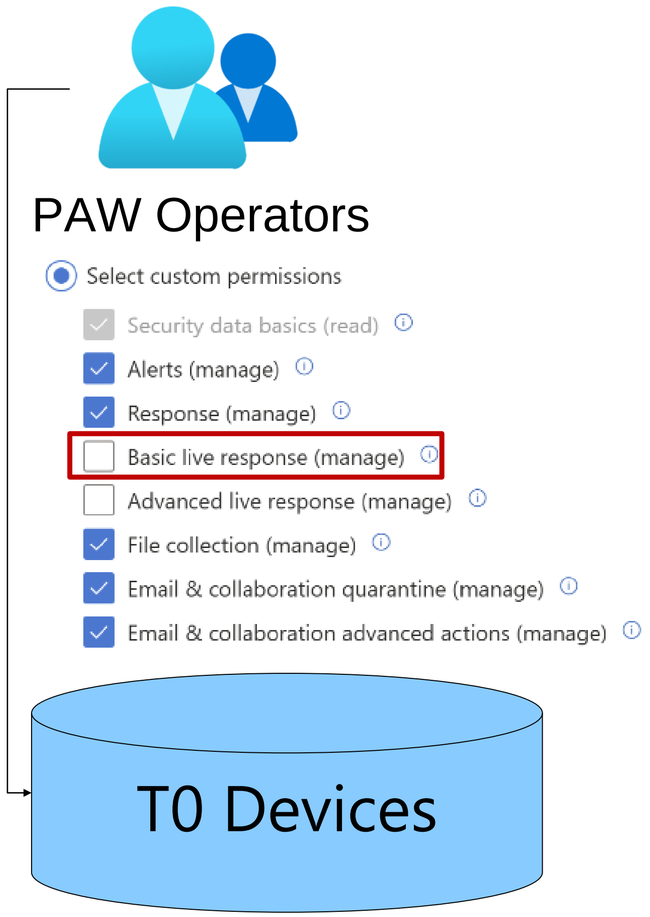
1. Enable XDR RBAC



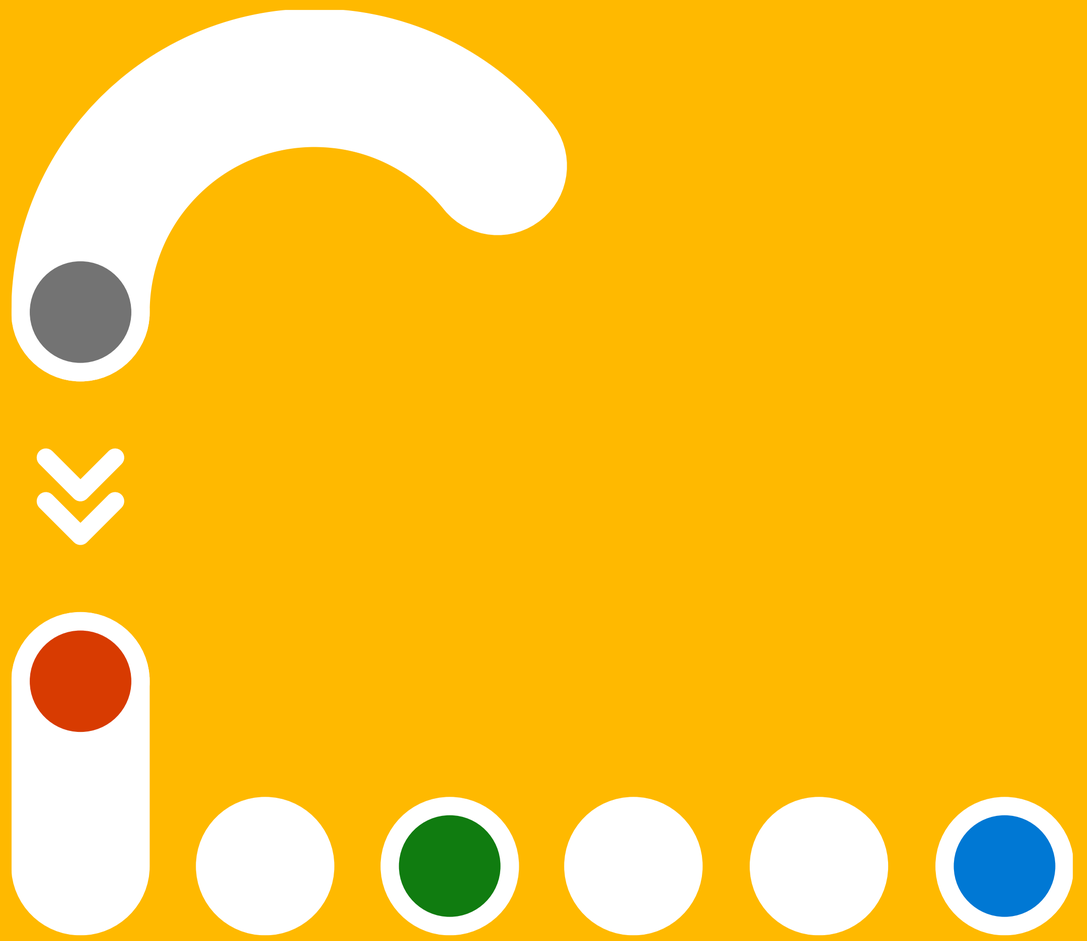
2. Create Entra ID group for T0 MDE Admins and non-T0 MDE Admins
3. Create MDE RBAC role
   - Assign users/groups
4. Create T0 and non-T0 MDE device group
   - Assign devices
   - Assign user groups that should have access to the device group

Defender XDR Roles – Use Case

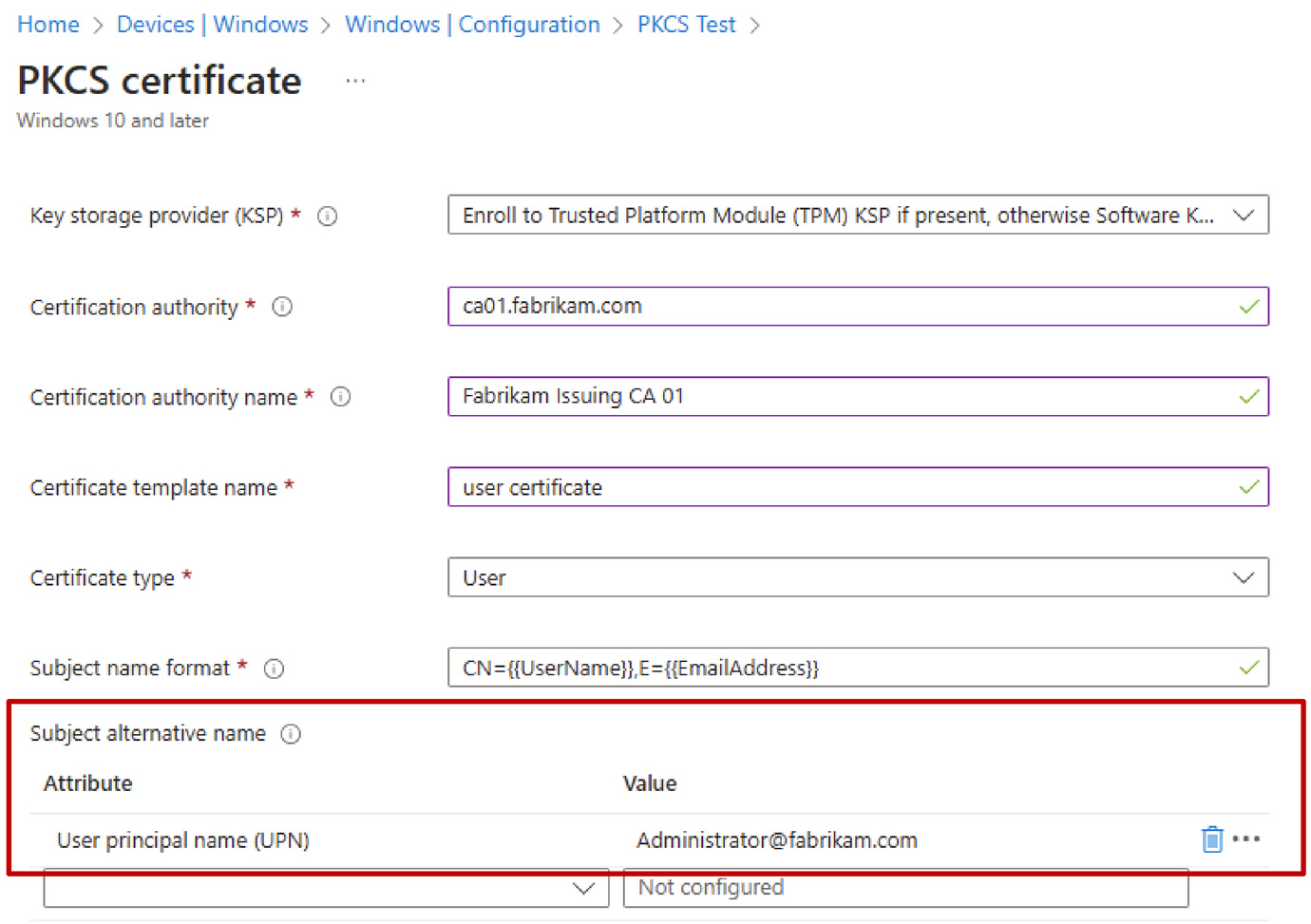




From Intune Admin to Domain Admin in 30 seconds



PKCS or SCEP Certificate Template



What’s the Issue?

Certificate-based authentication methods typically MAP the UPN in the certificate’s SAN to an account

- PKINIT
- Azure Certificate-based Authentication (CBA)

Mitigations

Intune RBAC does not provide enough granularity to block access to PKCS/SCEP settings

- Defender for Identity sensor for ADCS
- Remove Issuing CA certificate from NTAuth certificate store in AD
- Certificate Policy Module

Danke an unsere Sponsoren

PLATINUM SPONSOR

ACP IT for innovators.

mann&mouse
WE LIVE IT

SquaredUp

GOLD SPONSOR

SEPP MAIL

NiCE
IT Management Solutions
www.nice.de

INFOTECH
[IT & Communication]

Thank you!

Experts Live Austria