



Microsoft Entra Permissions Management

Automation and Alerts

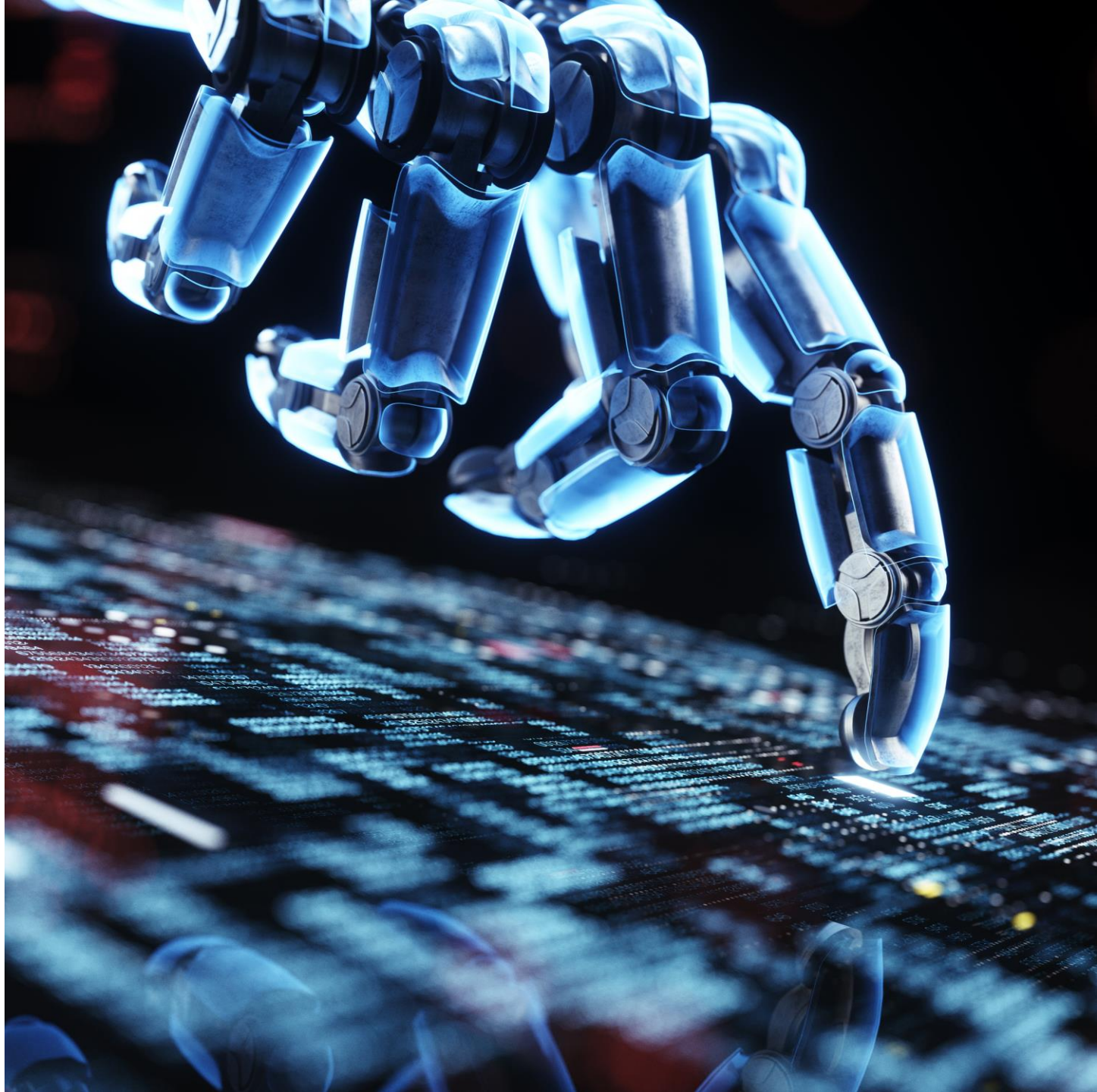
<Name>

<Job role>

Agenda

- Remediation Phase (Continued)
 - Day 60
 - Alerting
 - Day 90
 - Automation
 - Autopilot
 - Automated Reports
- Next Steps

Day 60 Remediations (continued): Set up Alerting

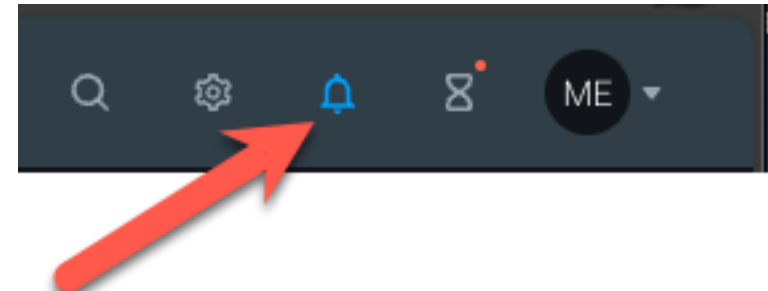


Alert Types

- Rule Based
 - Activity taking place for the first time
- Statistical Anomaly Based
 - Tasks with unusual number, results, timing or types
- Permissions Analytic Based
 - Any of the findings from the Permissions Analytics Report
- Activity Based
 - Customizable logic rules. Ex: (Any failure on this crown jewel resource)

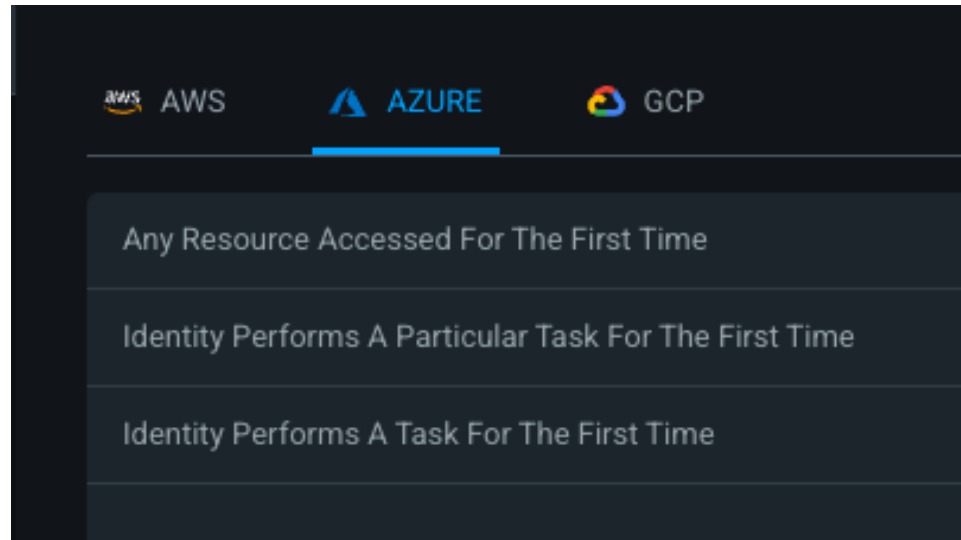
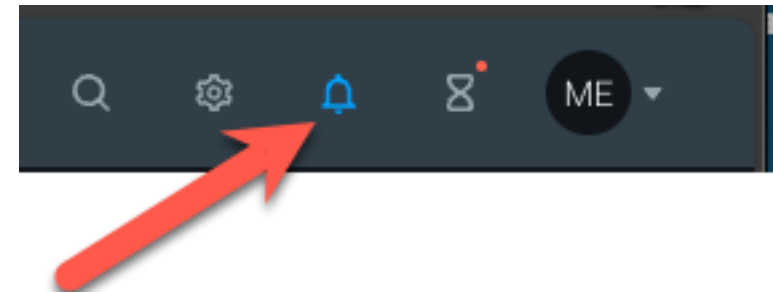
Recommended Alerts

- Click the bell icon in the upper right corner of the Permissions Management portal to access the alerting menu



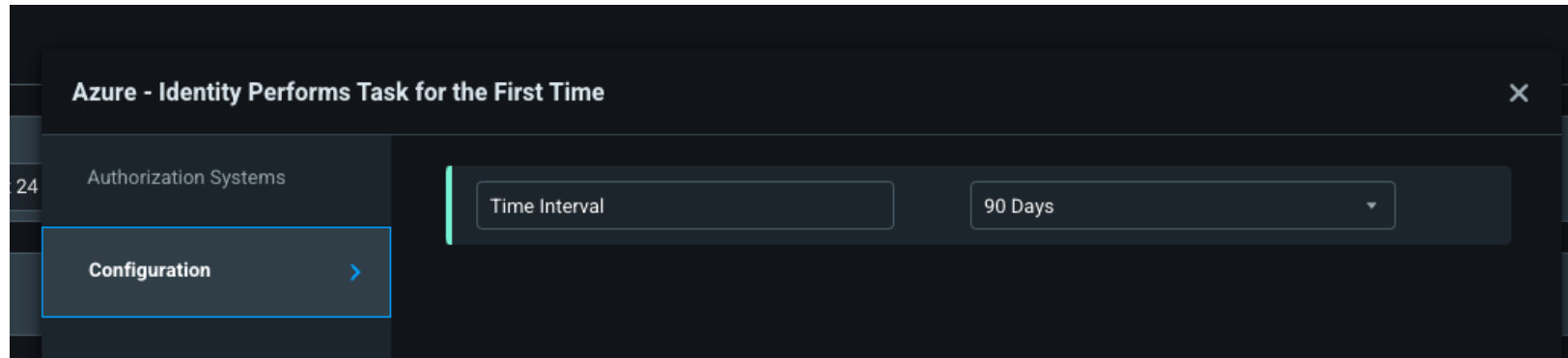
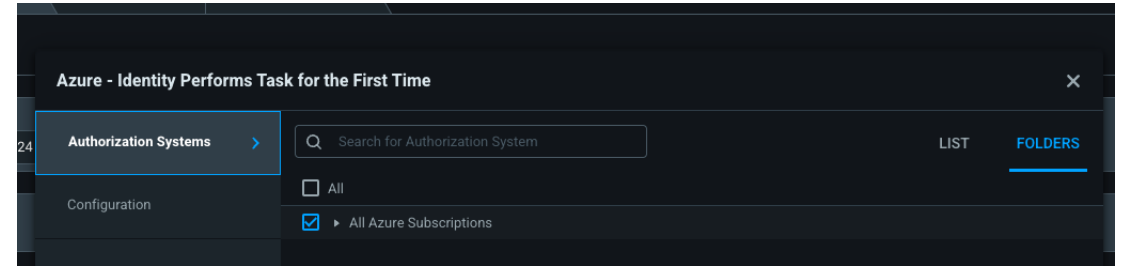
Recommended Alerts – Rule-Based Anomaly

- Click the bell icon in the upper right corner of the Permissions Management portal to access the alerting menu
- There are 3 types of rule-based anomaly triggers:



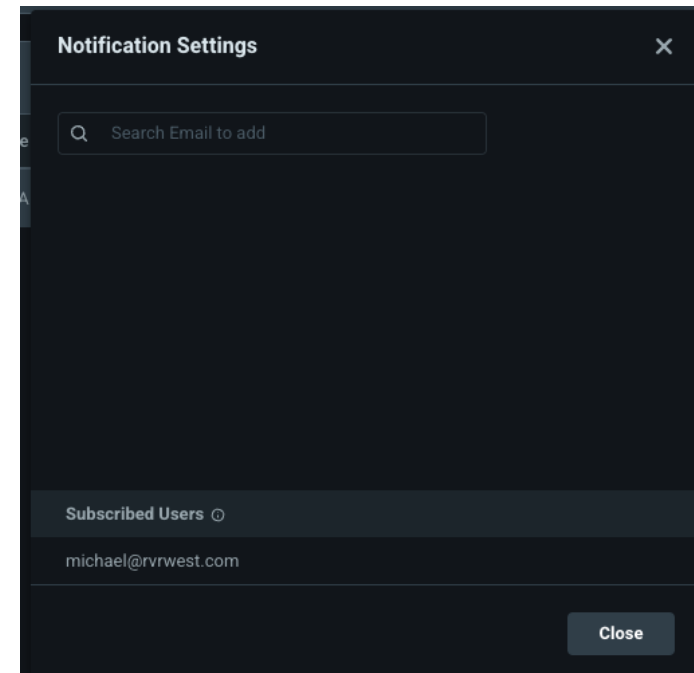
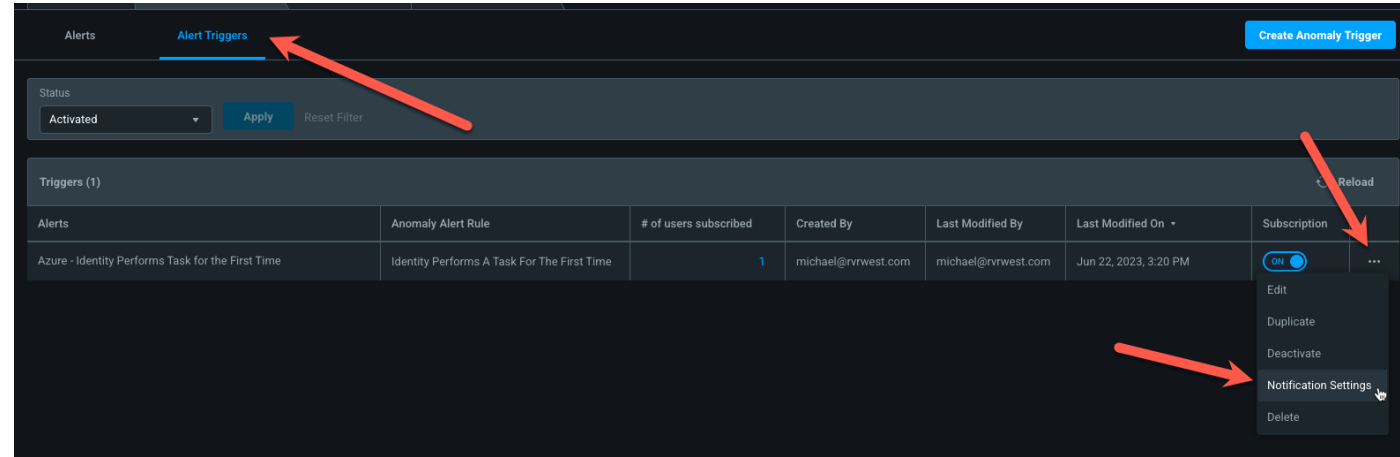
Recommended Alerts – Rule-Based Anomaly

- Choose the rule type you'd like to create. Recommended to start with "Identity Performs Task for the First Time"
- Choose your authorization system(s)
- Choose the time period to evaluate:



Recommended Alerts – Rule-Based Anomaly

- Go to the Alert Triggers tab, click on the 3 dots menu on your new trigger, and choose Notification Settings:
- Choose which admins should receive the alerts:
- Repeat the process for other authorization systems



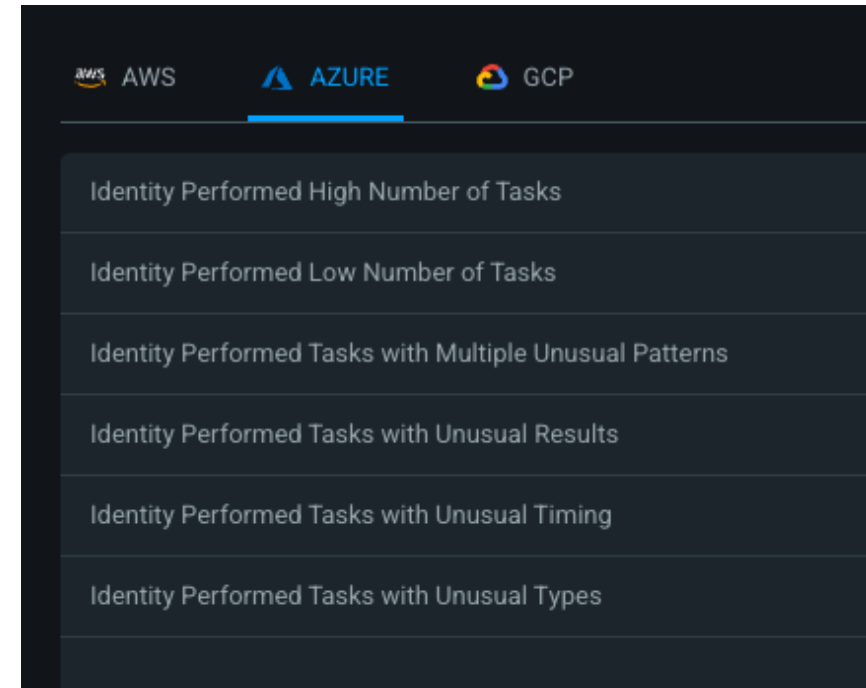
Recommended Alerts – Statistical Anomaly

- Go to the Statistical Anomaly tab, Alert Triggers, and choose Create Alert Trigger:



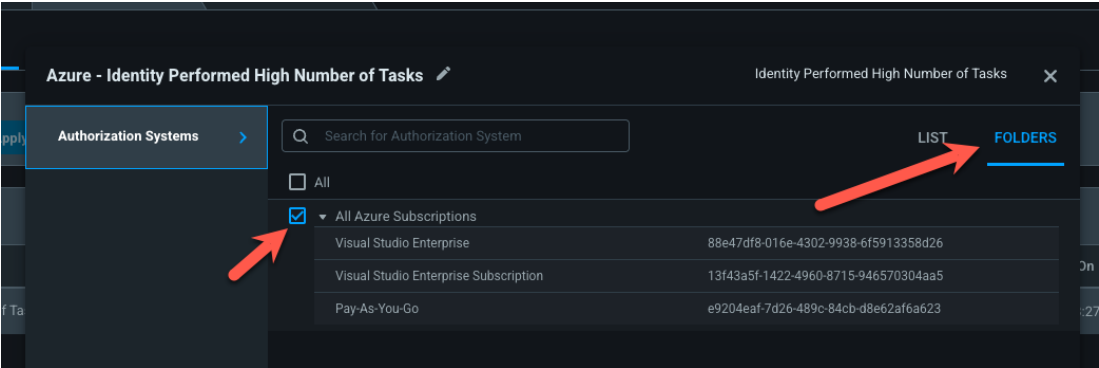
Recommended Alerts – Statistical Anomaly

- Go to the Statistical Anomaly tab, Alert Triggers, and choose Create Alert Trigger:
- There are 6 kinds of Statistical Anomaly Alerts you can create. Recommended to start with these:
 - Identity Performed High Number of Tasks
 - Identity Performed Tasks with Multiple Unusual Patterns
 - Identity Performed Tasks with Unusual Results
 - Identity Performed Tasks with Unusual Timing
 - Identity Performed Tasks with Unusual Types



Recommended Alerts – Statistical Anomaly

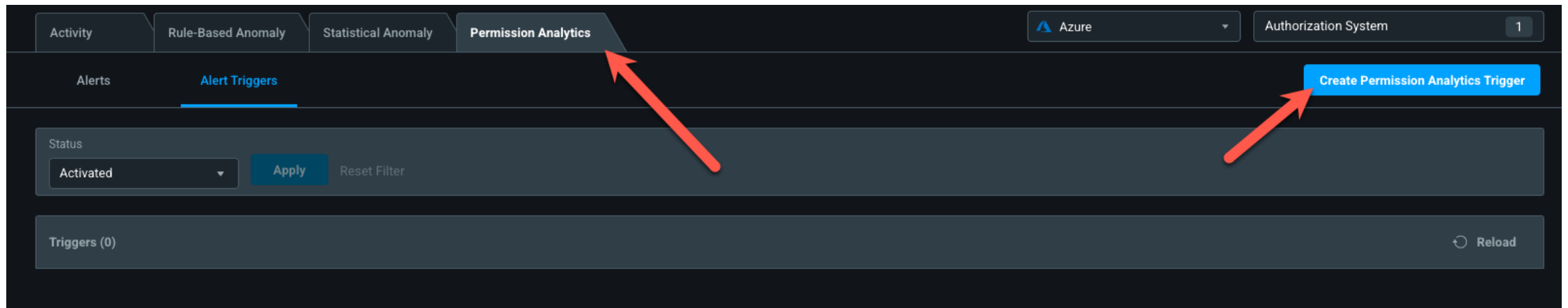
- It's recommended that you set up your alert triggers based on folders rather than picking and choosing individual subscriptions
- When completed, you should have at least 5 alert triggers:



Alerts							
Alert Triggers							
Status							
Activated							
Apply Reset Filter							
Triggers (5)							
Reload							
Alerts	Anomaly Alert Rule	# of users subscribed	Created By	Last Modified By	Last Modified On	Subscription	
Azure - Identity Performed Tasks with Unusual Results	Identity Performed Tasks with Unusual Results	1	michael@rwrwest.com	michael@rwrwest.com	Jun 22, 2023, 3:29 PM	ON	...
Azure - Identity Performed Tasks with Multiple Unusual Patterns	Identity Performed Tasks with Multiple Unusual Patterns	1	michael@rwrwest.com	michael@rwrwest.com	Jun 22, 2023, 3:29 PM	ON	...
Azure - Identity Performed High Number of Tasks	Identity Performed High Number of Tasks	1	michael@rwrwest.com	michael@rwrwest.com	Jun 22, 2023, 3:31 PM	ON	...
Azure - Identity Performed Tasks with Unusual Timing	Identity Performed Tasks with Unusual Timing	1	michael@rwrwest.com	michael@rwrwest.com	Jun 27, 2023, 7:10 AM	ON	...
Azure - Identity Performed Tasks with Unusual Types	Identity Performed Tasks with Unusual Types	1	michael@rwrwest.com	michael@rwrwest.com	Jun 27, 2023, 7:10 AM	ON	...

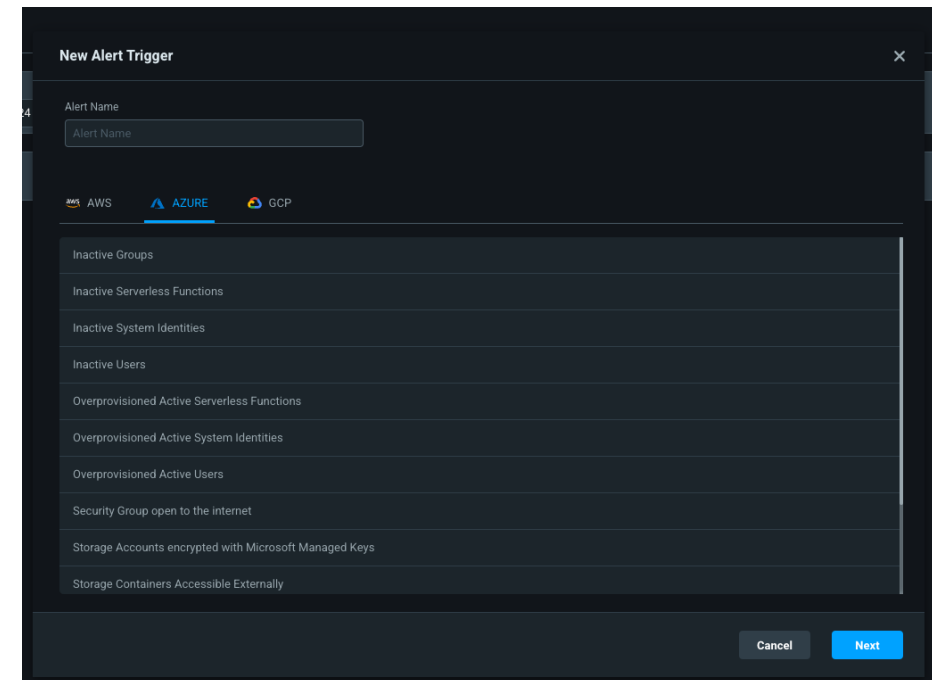
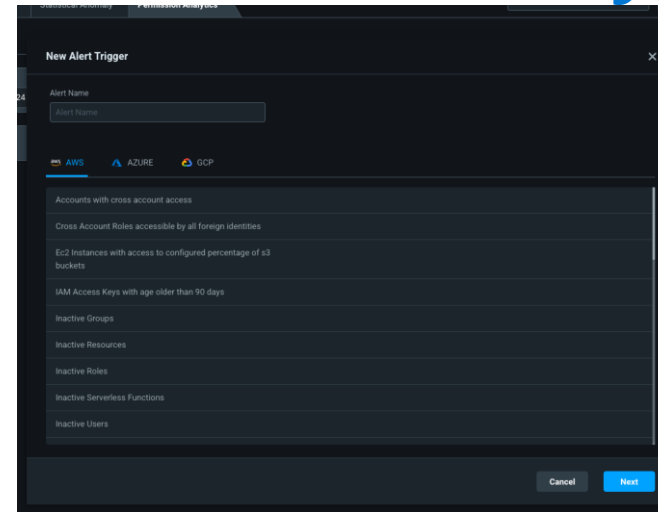
Recommended Alerts – Permissions Analytics

- Go to the Permission Analytics tab, Alert Triggers, and choose Create Alert Trigger:



Recommended Alerts – Permissions Analytics

- There are different permissions analytics for AWS, Azure, and GCP
- Create the alerts on the following pages for each provider, to start



Recommended Alerts – Permissions Analytics

Recommended initial set of alerts, start here at minimum, add additional Permissions Analytics alerts depending on need:

AWS

- Overprovisioned Active Roles
- Overprovisioned Active Users
- Roles with Privilege Escalation
- Service Accounts with Privilege Escalation
- Super Roles
- Super Users
- Users with Privilege Escalation
- (Optional, depending on use of IDP for MFA) User with no MFA

Azure

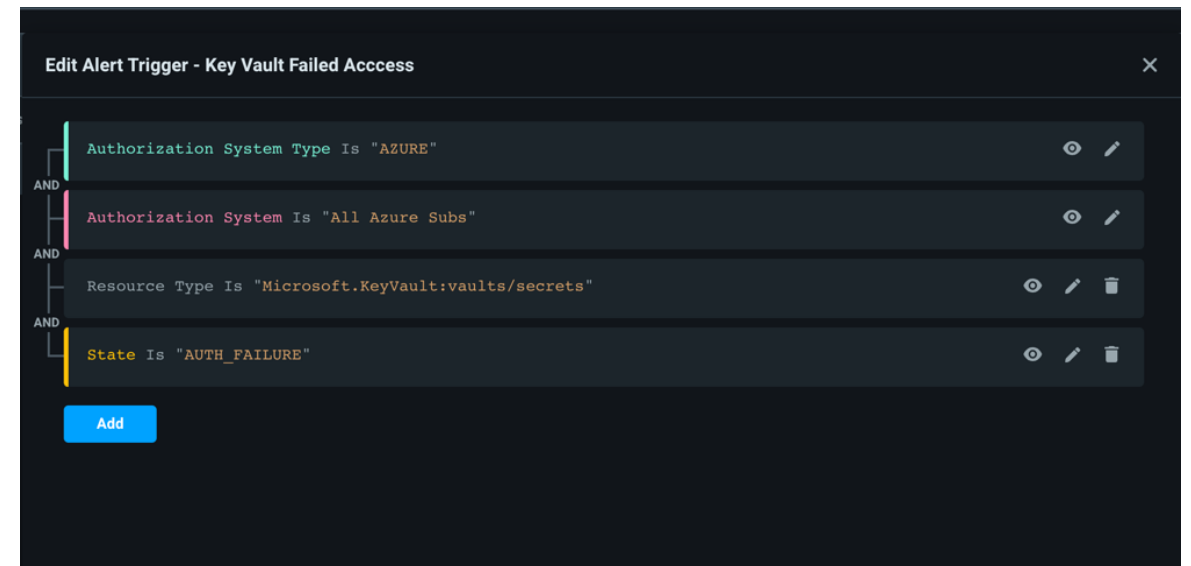
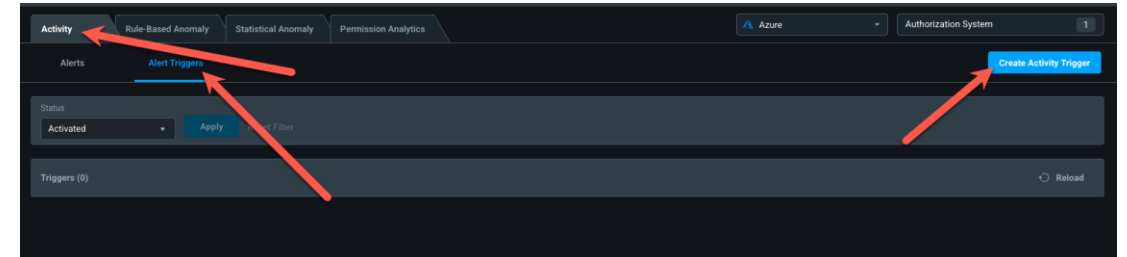
- Overprovisioned Active System Identities
- Overprovisioned Active Users
- Super System Identities
- Super Users

GCP

- Overprovisioned Active Service Accounts
- Overprovisioned Active Users
- Service Accounts with Privilege Escalation
- Super Service Accounts
- Super Users
- Users with Privilege Escalation

Recommended Alerts – Activity Alerts

- Can customize which specific resources to generate alerts on
 - Resource Type
 - Resource Name
 - Task Name
 - Username
 - State
 - Authorization Failure, Error, Success
- Focus on crown jewel type resources
 - Ex: Failure Access to KeyVault



Day 90 Remediations: Leverage Automation

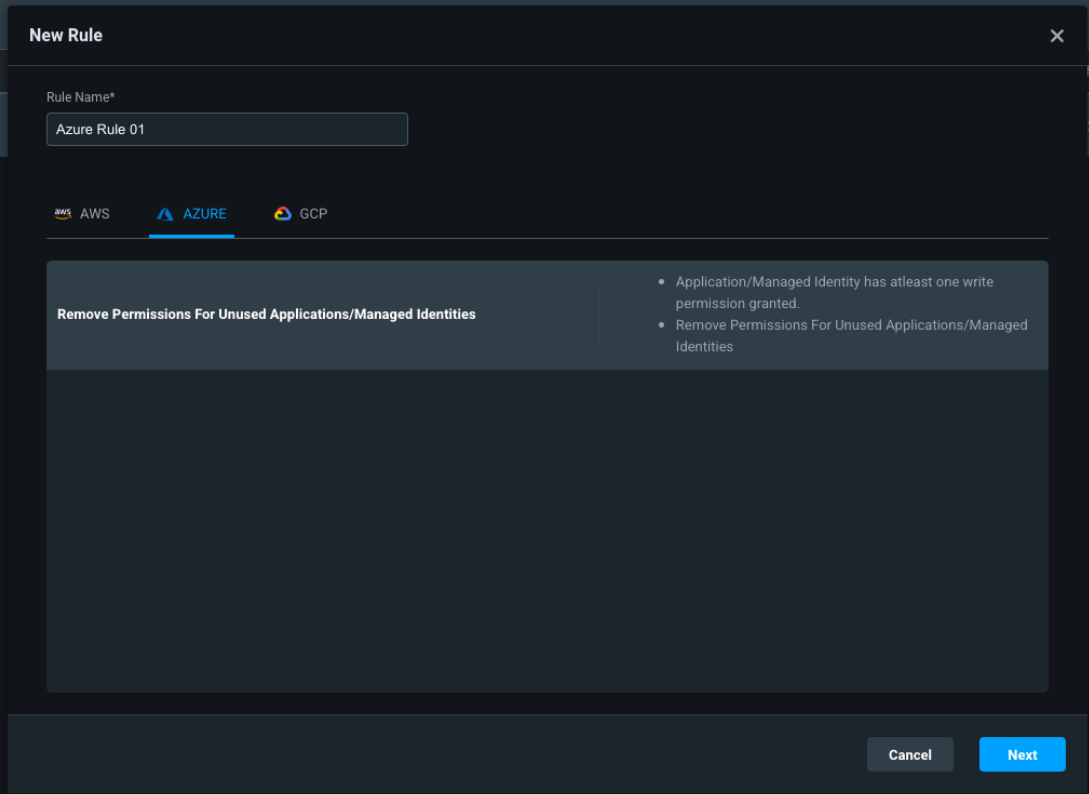


Automation – Autopilot

- Autopilot allows you to automate the right-sizing of permissions, remove unused roles, and remove unused role assignments / permissions
- Rules are based on inactivity – remember that EPM has 90 days of activity data, so inactivity will be based on 90 days of usage or less
- Available Rules
 - AWS-Delete Unused Roles
 - Azure-Remove Permissions For Unused Applications/Managed Identities
 - GCP-Remove Permissions for Unused ServiceAccounts

Recommended Autopilot Rule

- Go to the Autopilot tab
- Click the New Rule button
- Select Azure as the auth system type
- Provide a name and click Next



The screenshot shows a 'New Rule' dialog box with a dark background. At the top, there's a title bar with 'New Rule' and a close button. Below it, a 'Rule Name*' field contains the text 'Azure Rule 01'. Underneath the field, there are three tabs: 'AWS' (with the AWS logo), 'AZURE' (with the Azure logo and a blue underline), and 'GCP' (with the GCP logo). The main content area is divided into two sections. The left section has a header 'Remove Permissions For Unused Applications/Managed Identities' and a large, empty rectangular box below it. The right section contains a bulleted list: '• Application/Managed Identity has atleast one write permission granted.' and '• Remove Permissions For Unused Applications/Managed Identities'. At the bottom right, there are two buttons: 'Cancel' and 'Next'.

New Rule

Rule Name*

Azure Rule 01

AWS AZURE GCP

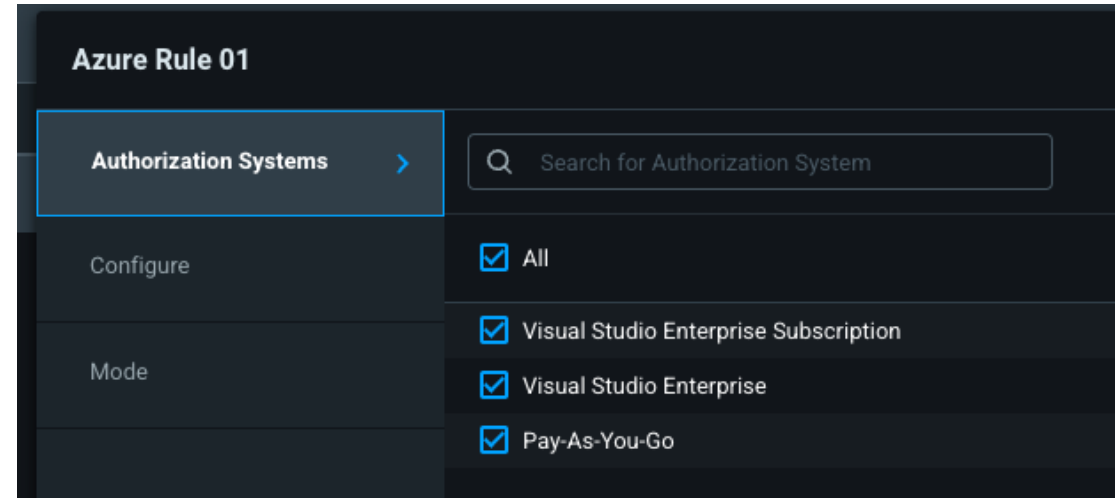
Remove Permissions For Unused Applications/Managed Identities

- Application/Managed Identity has atleast one write permission granted.
- Remove Permissions For Unused Applications/Managed Identities

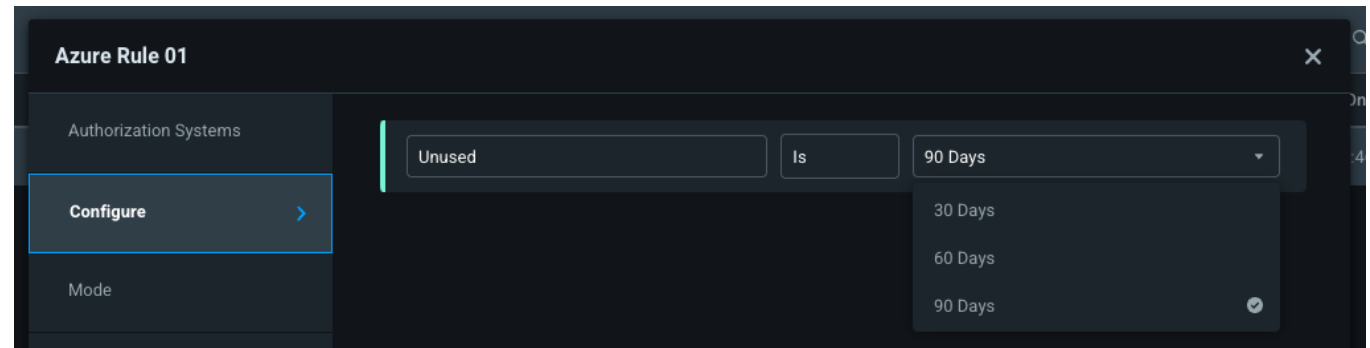
Cancel Next

Recommended Autopilot Rule

- Select your authorization system(s). You may select one or more than one

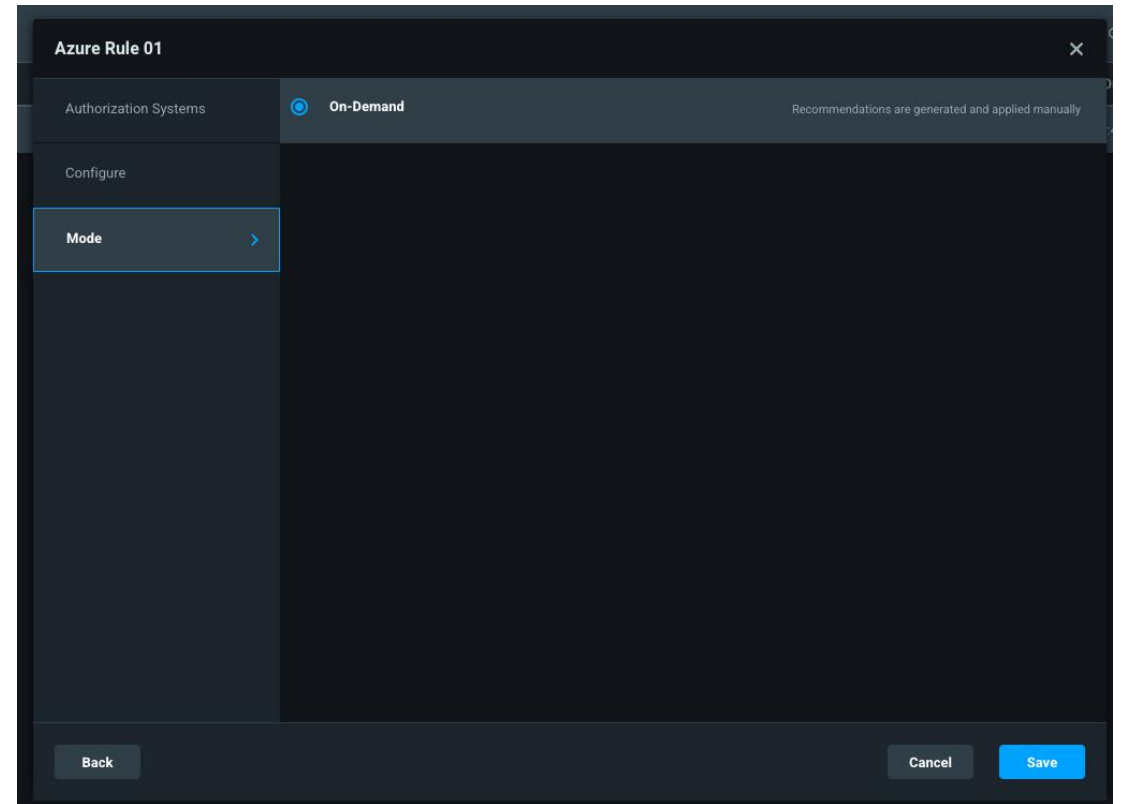


- Choose the rule's inactivity timer threshold



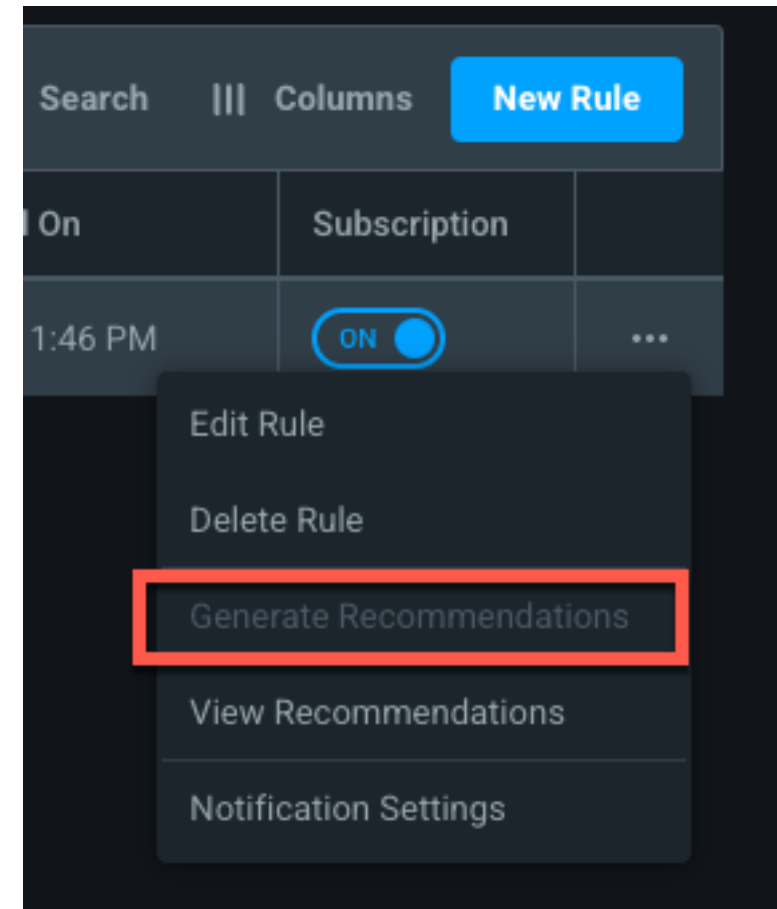
Recommended Autopilot Rule

- Choose the mode, typically on-demand
- Click Save
- Repeat process for other authorization systems of same type or different types
 - Autopilot rules are slightly different between AWS, Azure, and GCP, but fundamentally do similar things



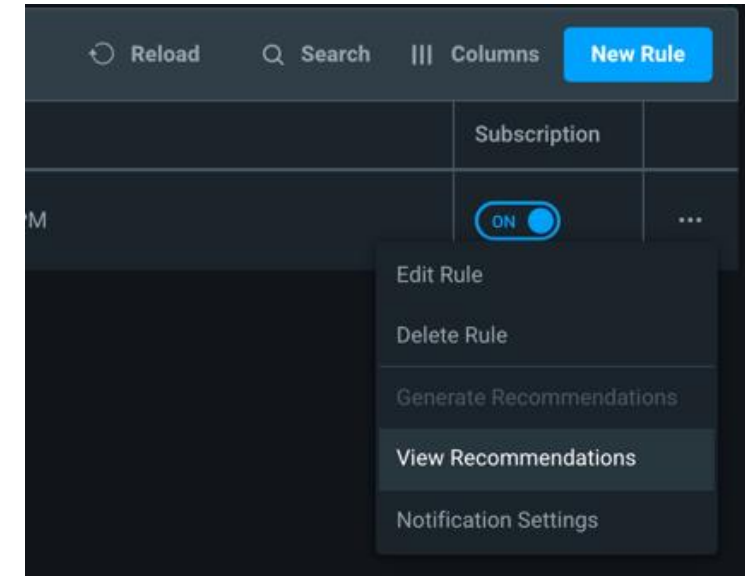
Recommended Autopilot Rule

- Click the Generate Recommendations button on the 3 dots menu to kick off the recommendations process
- If you onboarded EPM recently then no recommendations may be available for 30/60/90 days, depending on how you configured the Autopilot rule



View Auto Pilot Recommendations

- Click the View Recommendations button on the 3 dots menu.
- The recommendations for that rule will be shown.
 - Example below these are the apps whose permissions would be removed



Azure Autopilot: Remove Permissions For Unused Applications/Managed Identities ⓘ

Generated Jun 26, 2023, 7:24 PM

Generate Recommendations Apply Recommendations Unapply Recommendations

Authorization System Type: Azure Authorization System: All State: All Apply Reset Filter

Roles						Export
Roles^	State	Authorization System	Last Used On	Created On	Cross Account Role	
Cloud Infrastructure Entitlement Management	Generated		Never	-	No	
Microsoft Defender for Cloud Servers Scanner Resource Provider	Generated		Never	-	No	

Apply Recommendations

- After confirming the changes, check the box to which recommendation you want to apply, then hit "Apply" button on bottom
- Note: A Controller will need to be setup to be able to make changes in the Authorization System

Generate Recommendations **Apply Recommendations** Unapply Recommendations

Authorization System Type: Azure Authorization System: All State: All **Apply** [Reset Filter](#)

Roles

<input type="checkbox"/> Roles ^	State	Authorization System	Last Used On	Created On	Cross Account Role
<input type="checkbox"/> Cloud Infrastructure Entitlement Management	Generated		Never	-	No
<input type="checkbox"/> Microsoft Defender for Cloud Servers Scanner Resource Provider	Generated		Never	-	No

Next Steps



Where do we go from here?

- Finish remediating the most critical items found in the POC
- SOC leverage data and alerts for investigation of incidents
- JIT Privilege Elevation for critical resource access
- Start to remediate most over permissioned users/groups/apps
- Monitor PCI Score, did it go up or down?
- Continue to use Entra Permissions Management
 - We'll follow up in about 3 weeks
 - What did you like?
 - What needs to be improved?
 - What else did you find?
- Would a roadmap conversation be helpful?

Thank you!



