Microsoft Entra Permissions Management

Remediation & Permissions Creep Index

<Name>

<Job role>

Agenda

- Planning Phase
- Remediation Phase
  - Day 0
    - Immediate actions
  - Day 30
    - Baselining
    - Review Findings
    - Implement JIT/JEA
    - Permissions Creep Index (PCI)
      - What is it?
      - What does it identify?
      - PCI heat map

Planning Phase

Reminder on Zero Trust

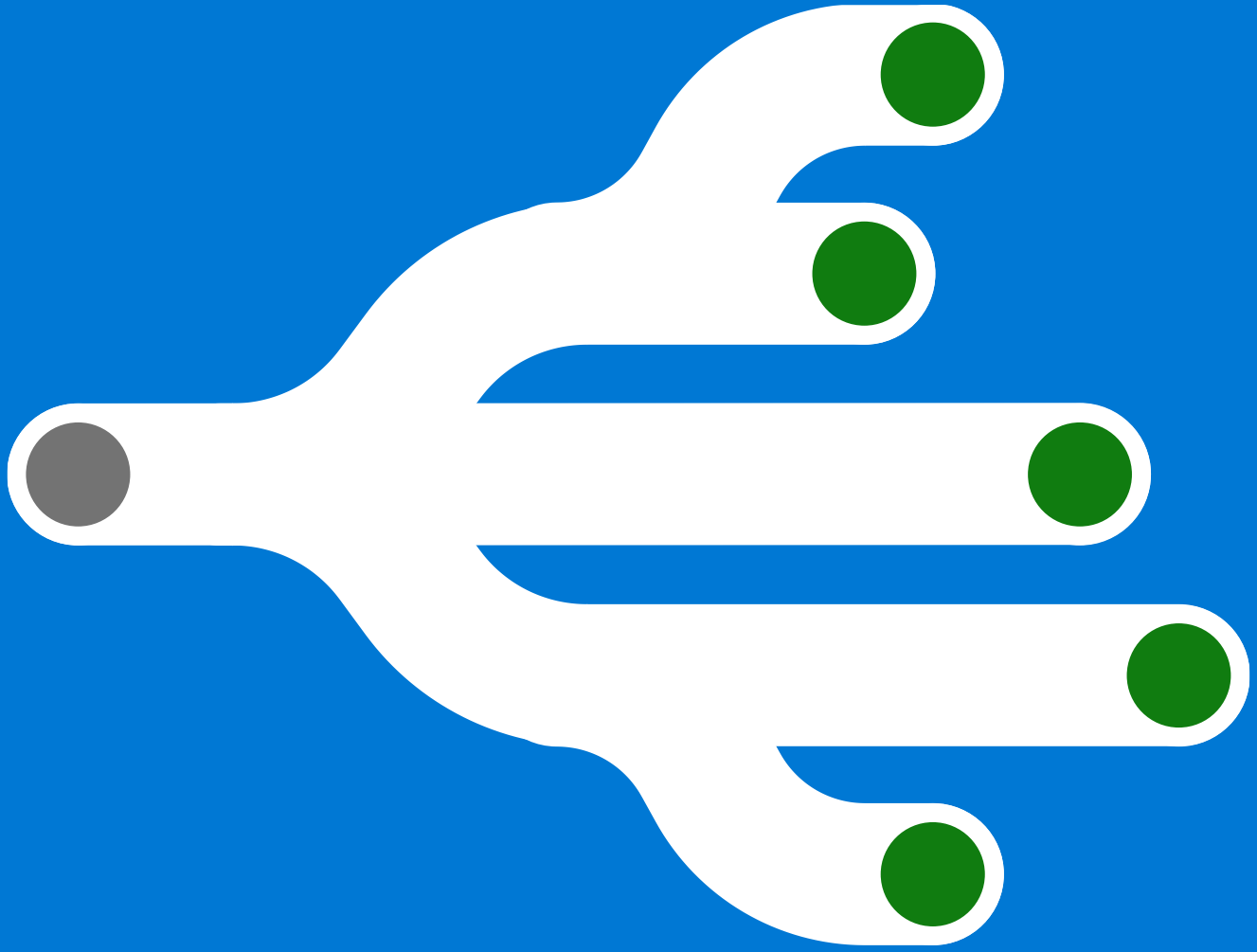
Least privilege best practices

- Right-sizing permissions assignments
  - Assign least privilege roles and continuously review assignments and historical usage to adjust over time
- Avoid direct assignment of users to high-risk roles
  - Implement permissions-on-demand (just-in-time) elevation of privileges for high risk tasks in GCP and AWS
  - Implement PIM for Groups or EPM permissions-on-demand elevation of privileges for high risk tasks in Azure
- Carefully design access to production environment!

Remediation plan

- Prioritize and triage - some tasks are more immediately important than others:
  - Day 0: Immediate attention needed
    - Critical ports open to the Internet (e.g. 22 – SSH, 3389 – RDP, 1433 – SQL Server, 3306 – MySQL Server, etc.)
    - Data exposed externally/publicly from blob storage
  - Day 30: Getting to an improved baseline - this phase aims to create a baseline with most of the findings remediated
    - Enable Controller Mode on Authorization Systems
    - Evaluate other EPM Findings, formulate a plan for which can be right-sized
    - Execute on plan to right-size roles/permissions identified for users, groups, and service accounts / apps based on initial EPM findings
    - Define the policies and establish process for permissions on demand flows.
  - Day 60: Plan and Alert – "Stop the Bleeding"
    - Capture your current state using PCI Dashboard
    - Configure Alerting so you know if any new findings are springing up
    - Continue remediation activities from findings
  - Day 90: Leverage Automation
    - Implement autopilot rules
    - Operationalize SOC processes around alerts
    - Force users to leverage permissions on demand
    - Report on progress using PCI Dashboard – are you seeing improvements you can show to management?

Remediation Phase

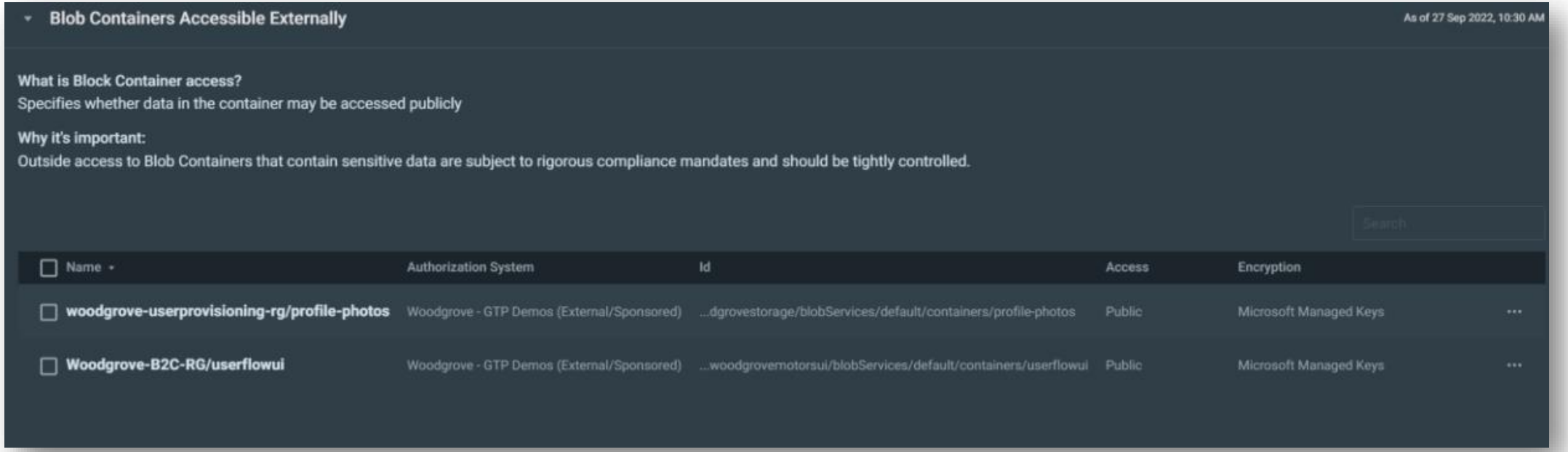


Day 0 Remediations: Fix the immediate problems

Immediate action: Data that is accessible externally

- **Risk:** Carefully review all findings for data that is exposed publicly (Azure Blob storage, AWS S3 buckets, GCP Storage buckets)

- **Action:** Using the permissions analytics report, identify those storage accounts (S3 Buckets, Storage buckets) and make sure to configure the right access and exposure level.



Immediate action: Open network security groups

- Network security groups can have critical ports open for inbound connections from the Internet
  - Ports like 22 (SSH), 3389 (RDP), 1433 (SQL Server), 3306 (MySQL Server) and others must be protected from direct Internet access.
  - **Action:** Close completely these ports from Internet. Typically done via a policy tool, such as Azure Security Center or AWS security group rules.

- Network security groups with no resources behind them create future hidden risks
  - **Action:** Identify owners and review those network security groups. Remove those that are not needed anymore.

Day 30 Remediations: Get to a Baseline

Getting to baseline tips

- Find the right stakeholders and verify before taking action
  - Most resources in an environment are used by different teams within a company. Before changing permissions first identify the stakeholders and discuss the findings
- Be aware of seasonal access, especially for application identities
  - Verify if read-only access is enough
  - After assigning read-only access, test the application
- Entra Permissions Management reports are most accurate about 60 days after first onboarding of an authorization system
  - By initial onboarding only data over the last 30 days is available
  - Depending on the type of authorization system (Azure, AWS, GCP) read operations might not be tracked. Consider this information when reviewing “inactive” identities – they might need read only access
- Future projects (landing zones) could require more permissions than the baseline

Review super identities

- It is expected to have “super” identities
  - Users, Groups, Apps / Service Principals, Serverless Functions
- It is NOT expected to have excessive numbers of super identities
  - Generally want 5 or fewer User and/or Group super identities per authorization system
  - App / service principal / service accounts should be very limited in number and reasoning for permissions documented
- Recommendation:
  - Move permissions for super users and groups to JIT (PIM for Azure, EPM JIT for AWS, GCP, and Azure)
    - PIM for Groups is very standard for Azure RBAC role-management. Many of the benefits of EPM JIT are already in place if you are already using PIM for Groups
    - EPM JIT extends similar Just-in-Time concepts to AWS and GCP quickly and easily

JIT / JEA

Privilege Management at Scale

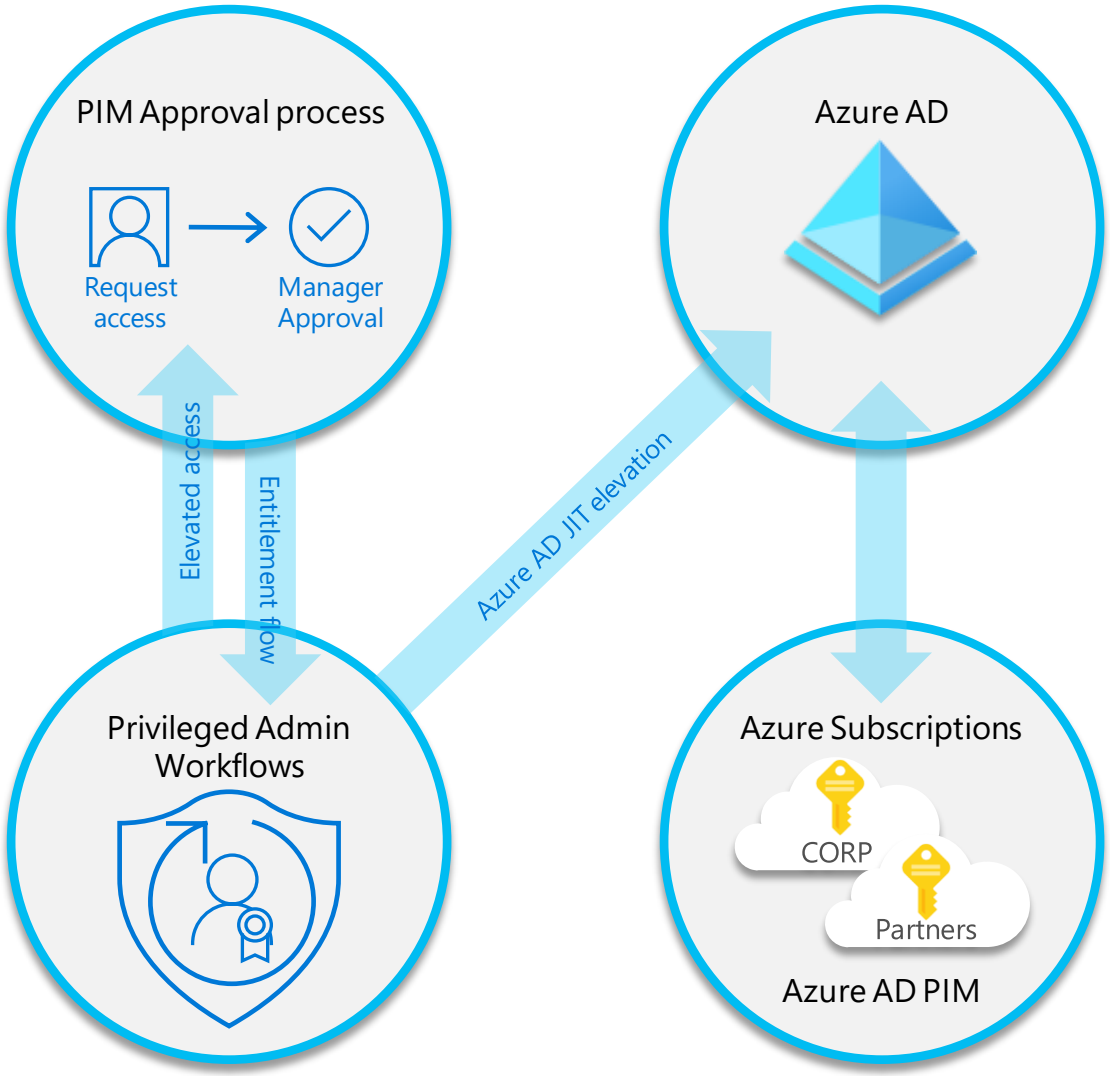
Leverage JIT/JEA controls for Tier 0 roles, expand to other roles as well.

No Persistent Elevated Access

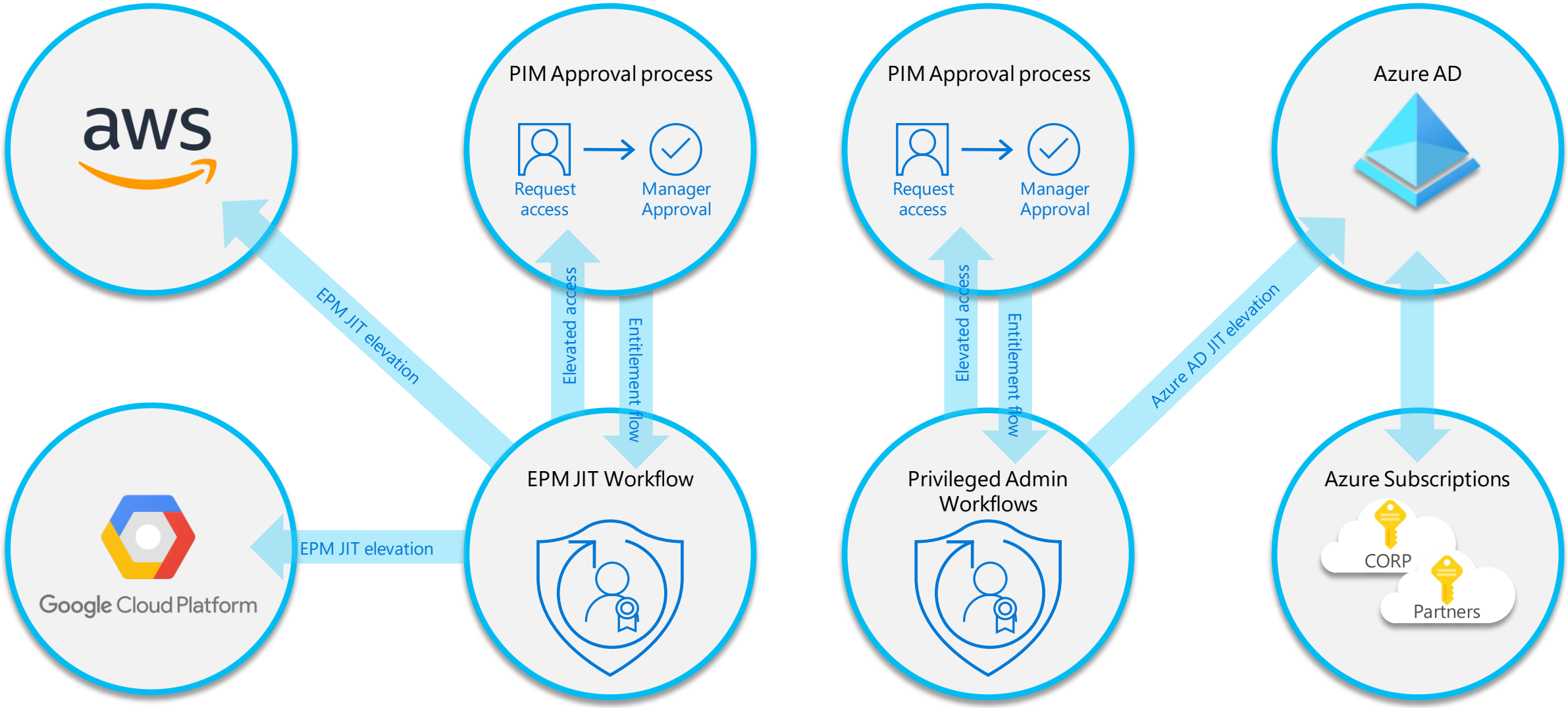
Do not allow persistent elevated access on-premises or in the cloud.

Reduce Surface Area

Significantly lower blast radius if identity is compromised.

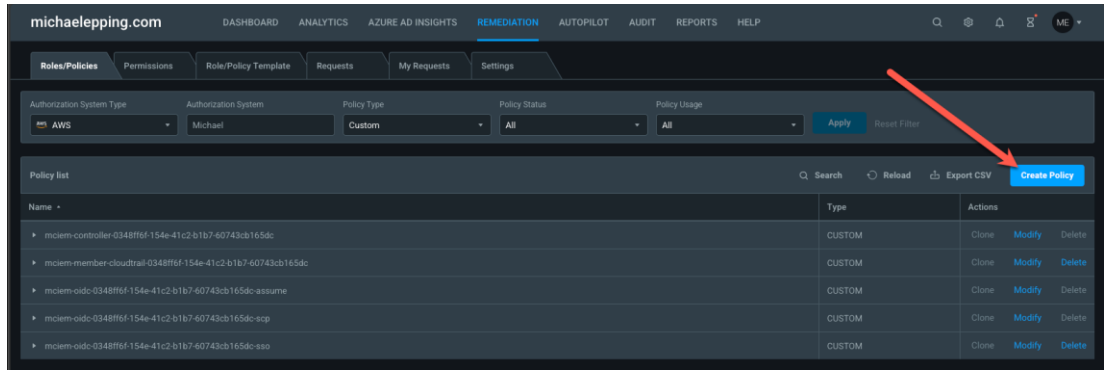


JIT / JEA

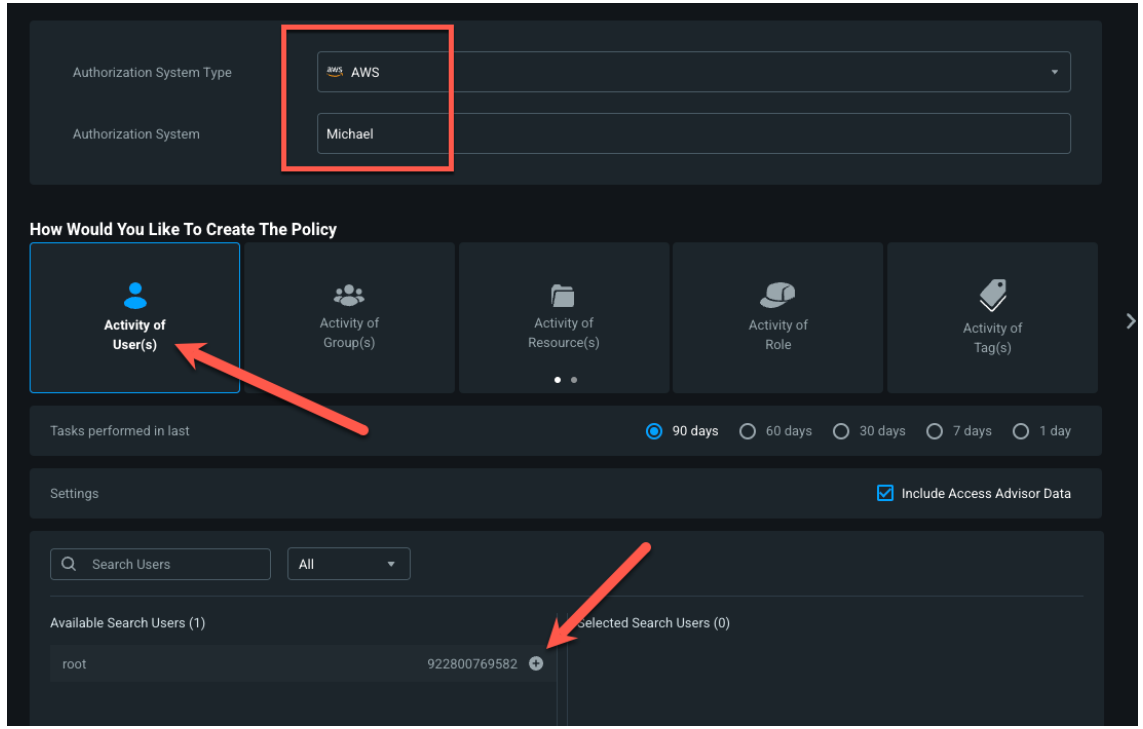

aws
PIM Approval process
Request access
Manager Approval
PIM Approval process
Request access
Manager Approval
Azure AD
EPM JIT elevation
Elevated access
Entitlement flow
Elevated access
Entitlement flow
Azure AD JIT elevation
Google Cloud Platform
EPM JIT elevation
EPM JIT Workflow
Privileged Admin Workflows
Azure Subscriptions
CORP
Partners

Configuring EPM JIT for Super Identities

- Navigate to Remediation → Roles/Policies → Create Policy

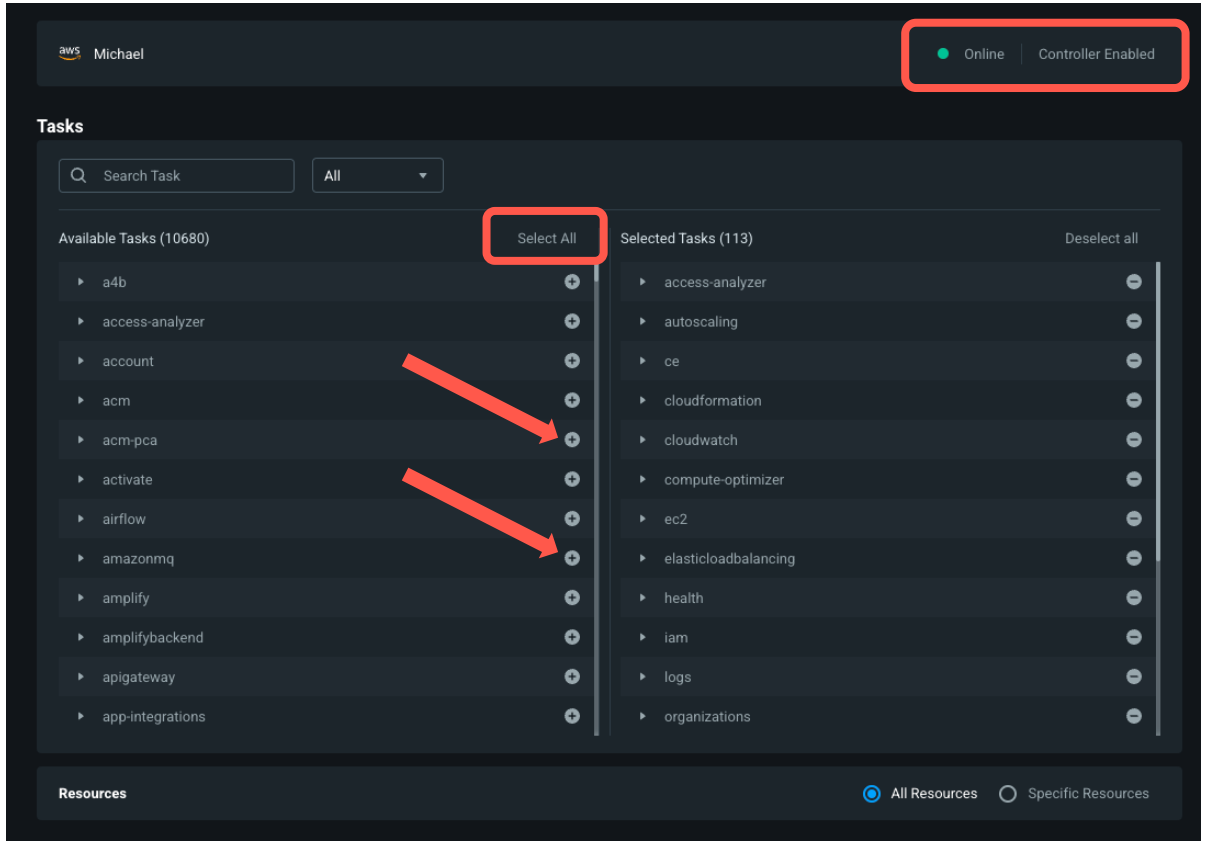


- Select your Authorization System Type and Authorization System
- Select Activity of User(s) and choose the Super Identities you're converting to JIT access



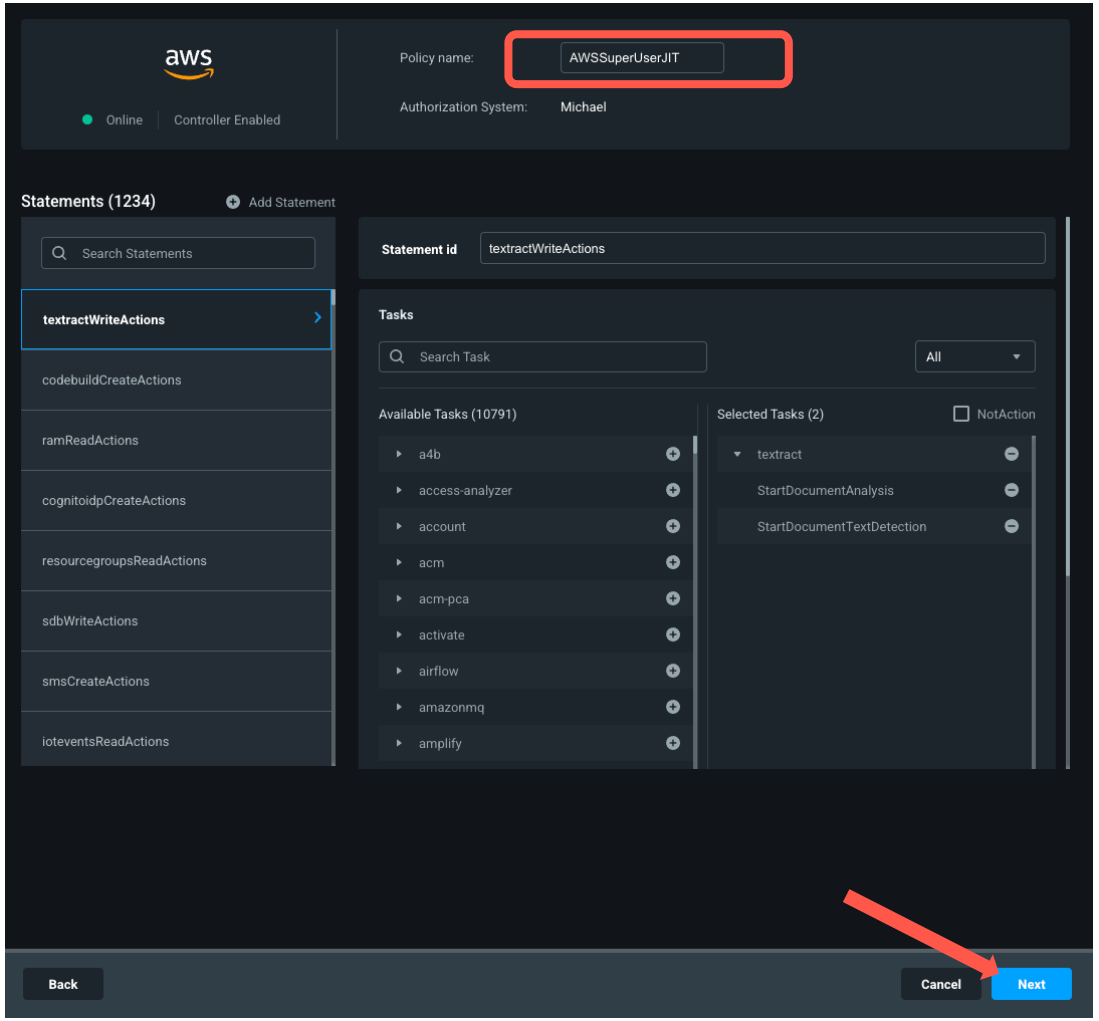
Configuring EPM JIT for Super Identities

- Validate that the authorization system shows Controller Enabled
  - Without Controller Enabled, EPM cannot manage JIT access for users
- The pre-selected tasks on the right will be the tasks that EPM has detected your Super Identity has used recently
  - Since super identities may need all permissions, you can optionally choose to add more
  - Choose Select All or individual permissions



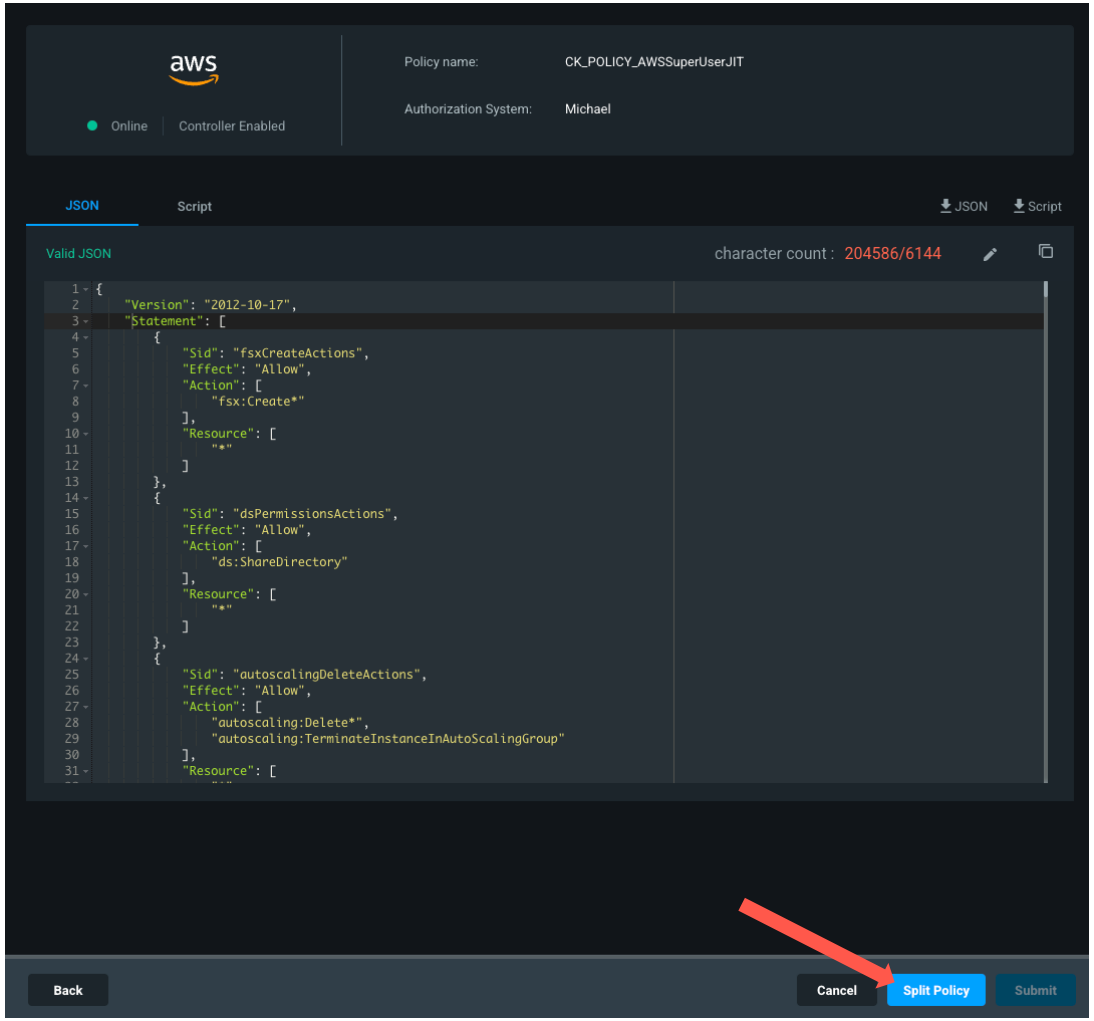
Configuring EPM JIT for Super Identities

- Provide a policy name (AWS) or role name



Configuring EPM JIT for Super Identities

- If the policy is very large then you'll need to create it using the Split Policy option:
- Finally, click Submit
- It will take several minutes for the policies to be created

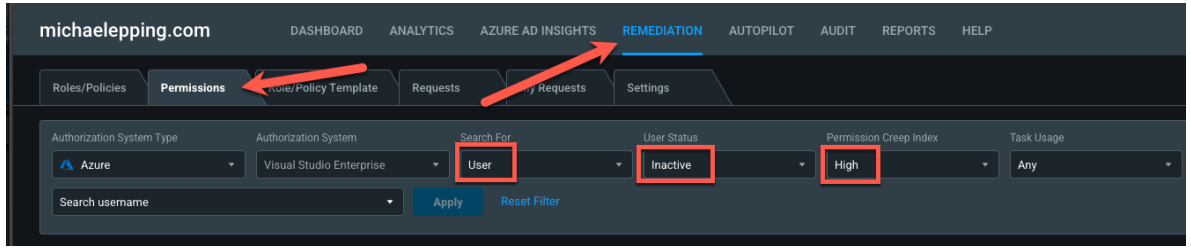


Review inactive identities

- Identities with granted, but not used privileges create imminent risk to your environment
- Review if any identities need to retain permissions, but just use them sparingly, such as break glass accounts or apps
  - Filter these out of your alerts when you set them up later
- Revoke all permissions for unused identities
  - Alternatively, revoke all write permissions for those identities
  - Start with High PCI, then Medium PCI, then Low PCI identities

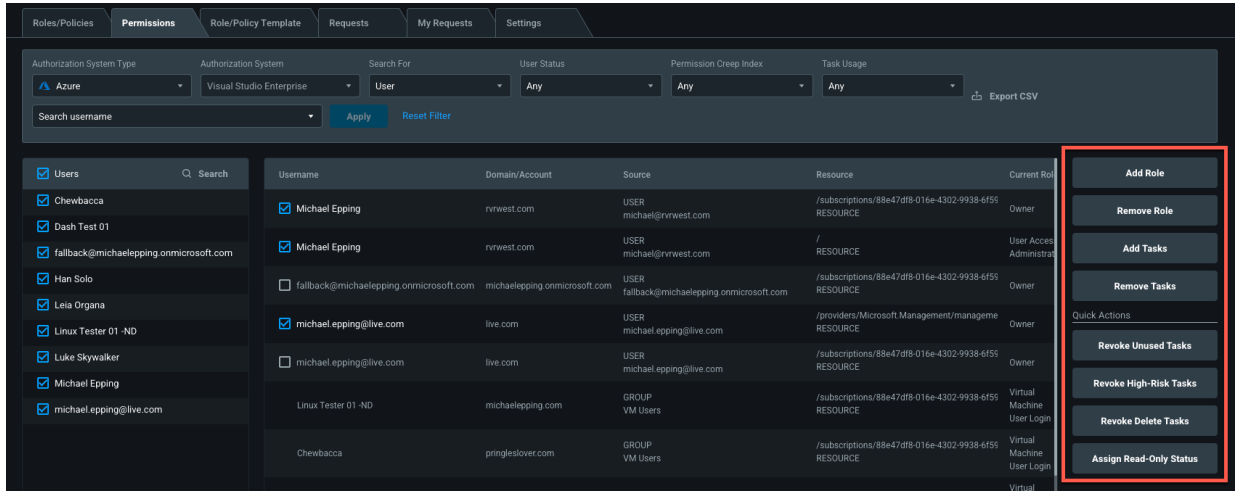
Remediating Inactive Identities

- Navigate to Remediation → Permissions
- Choose your Authorization System and filter
  - Filter for User, Group, Application, etc.
  - Filter User Status as “Inactive”
  - Filter for the PCI risk level, typically starting with High



Remediating Inactive Identities

- Choose the inactive identities that you would like to remediate
- Choose the proper action on the right hand side. Recommended Actions:
  - Revoke Unused Tasks
  - Revoke High-Risk Tasks
  - Revoke Delete Tasks
- Validate identities are truly inactive before invalidating permissions/tasks

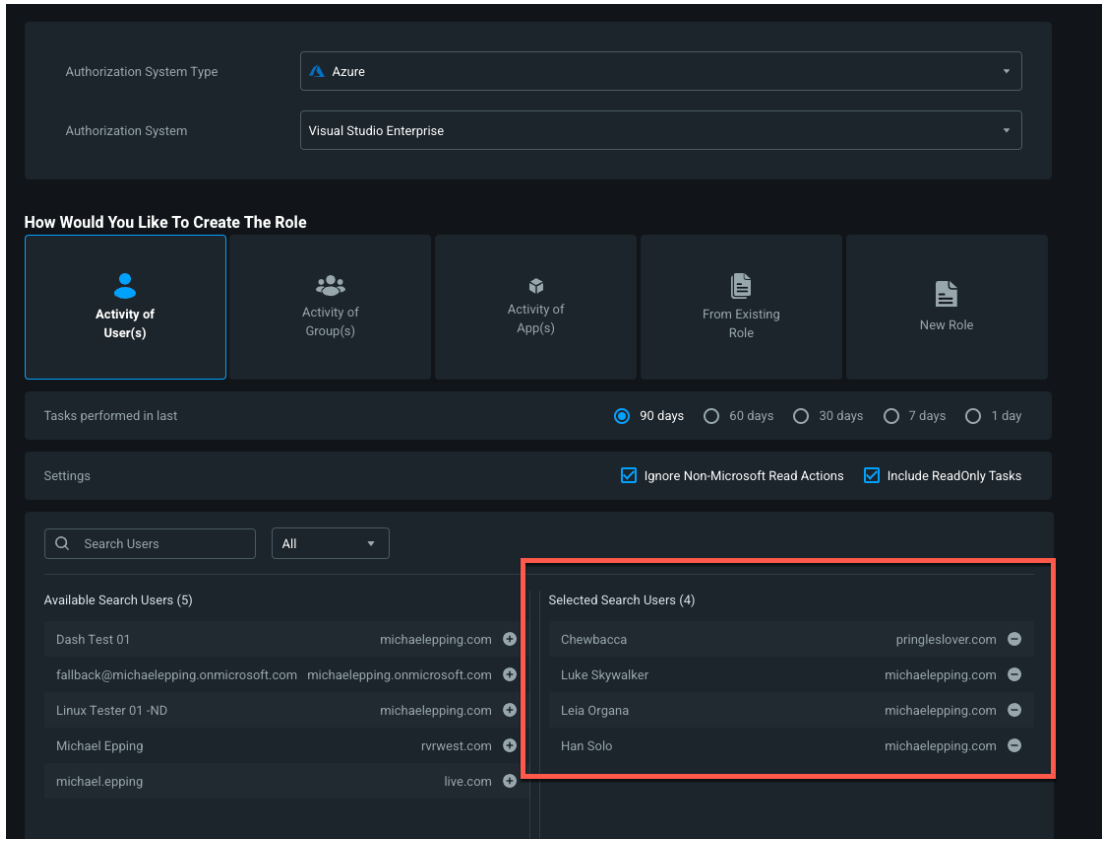


Right-size active identity permissions (overprovisioned active identities)

- Identify patterns for permissions and create custom roles if needed
- Assign those baseline roles to overprovisioned identities
- Start with identities that have a High PCI score

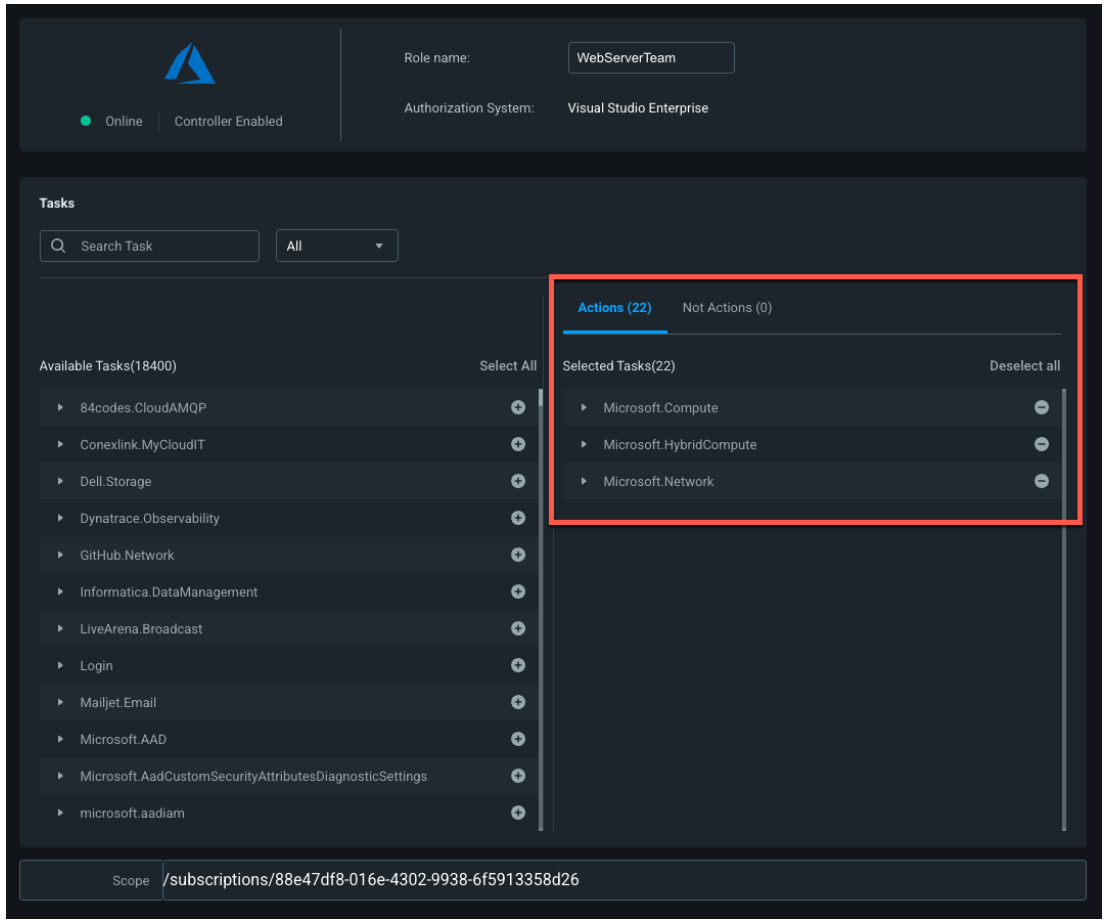
Right-size active identity permissions (overprovisioned active identities)

- Identify a team or group of users you want to right-size permissions for. For example, the admins/devs for a web service
- Recommended approach:
  - Create a new role based on what the team currently does
  - Go to Remediation → Roles/Policies → Create Role/Policy
  - Select the users from the team you're working with:



Right-size active identity permissions (overprovisioned active identities)

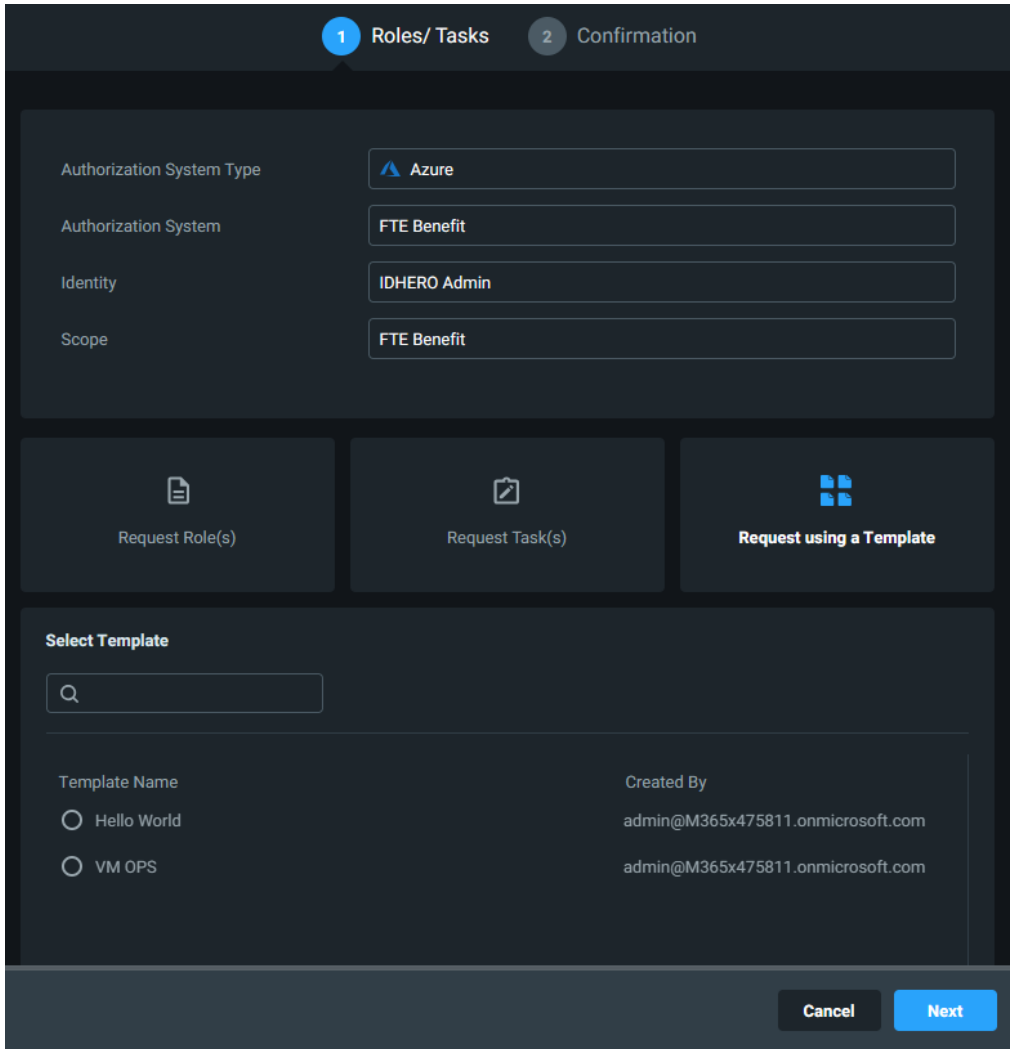
- Validate the permissions in the new role
- Add any missing permissions the team may need
- Create the new role
- Revoke existing permissions from the team
- Going forward, these users should request the now right-sized permissions via EPM



Improving baseline: Just-in-time privilege elevation

Elevation of permissions can be based on a built-in or custom role, preconfigured permissions template, or even specific granular permissions.

Best practice: Configure Just-in-time for all privileged roles

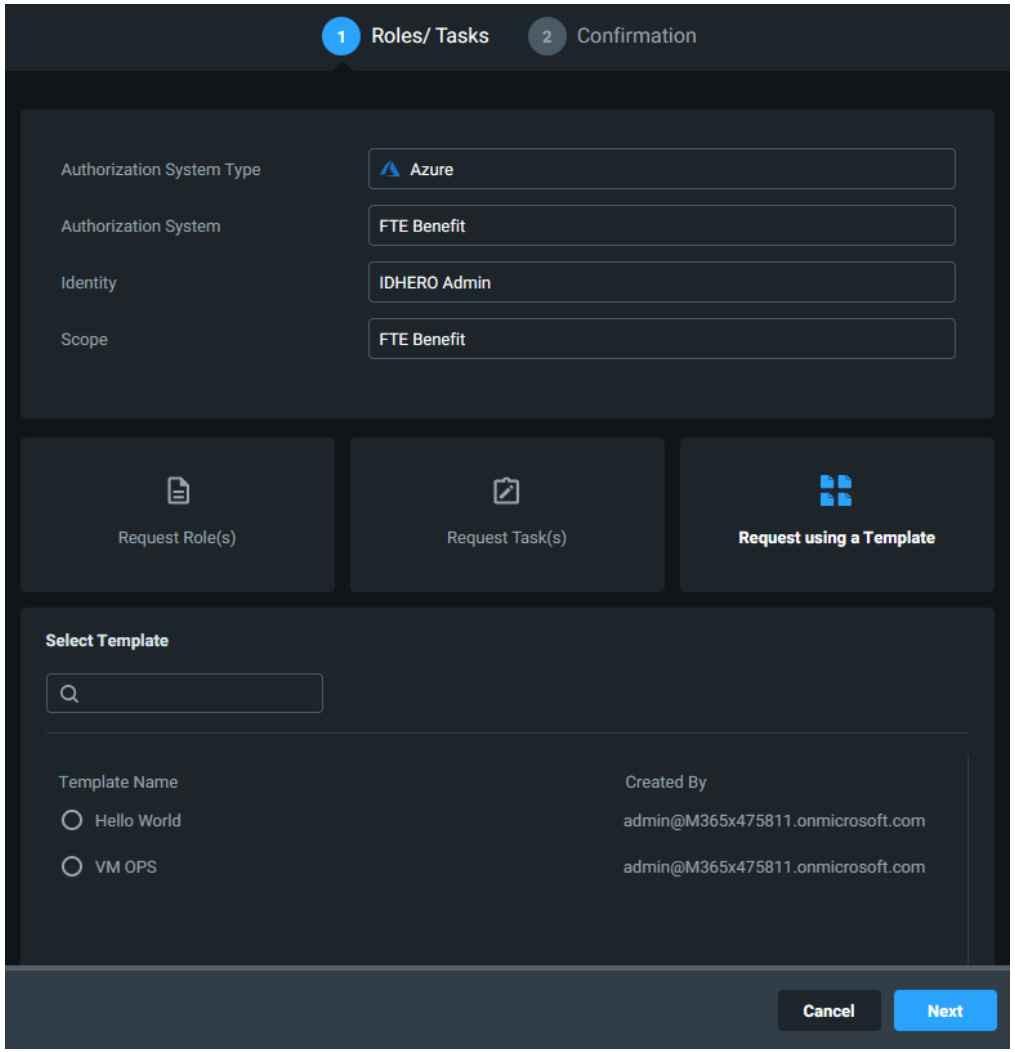


Implement Permissions On-Demand

Elevation of permissions can be based on a built-in or custom role, preconfigured permissions template, or even specific granular permissions.

- Suggested Guiding Principles:
  - No user shall have delete permissions unless they explicitly request them, they are approved, and they are time-bound
  - High privileged access is only granted through just enough permissions and just-in-time access
  - Users may request recurring daily, weekly, or monthly permissions that are time-bound with approval
  - Use Templates where possible

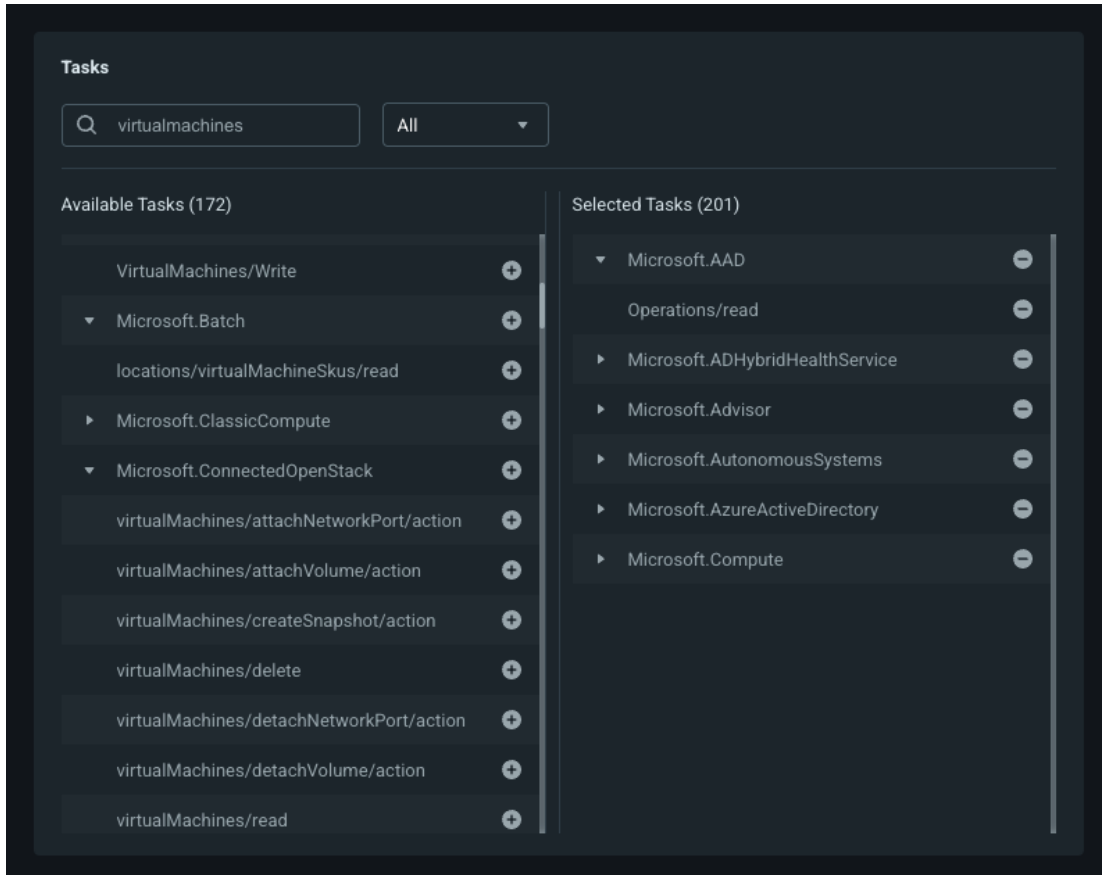
Best practice: Configure Just-in-time for *all* privileged roles



Implement Permissions On-Demand

Create templates

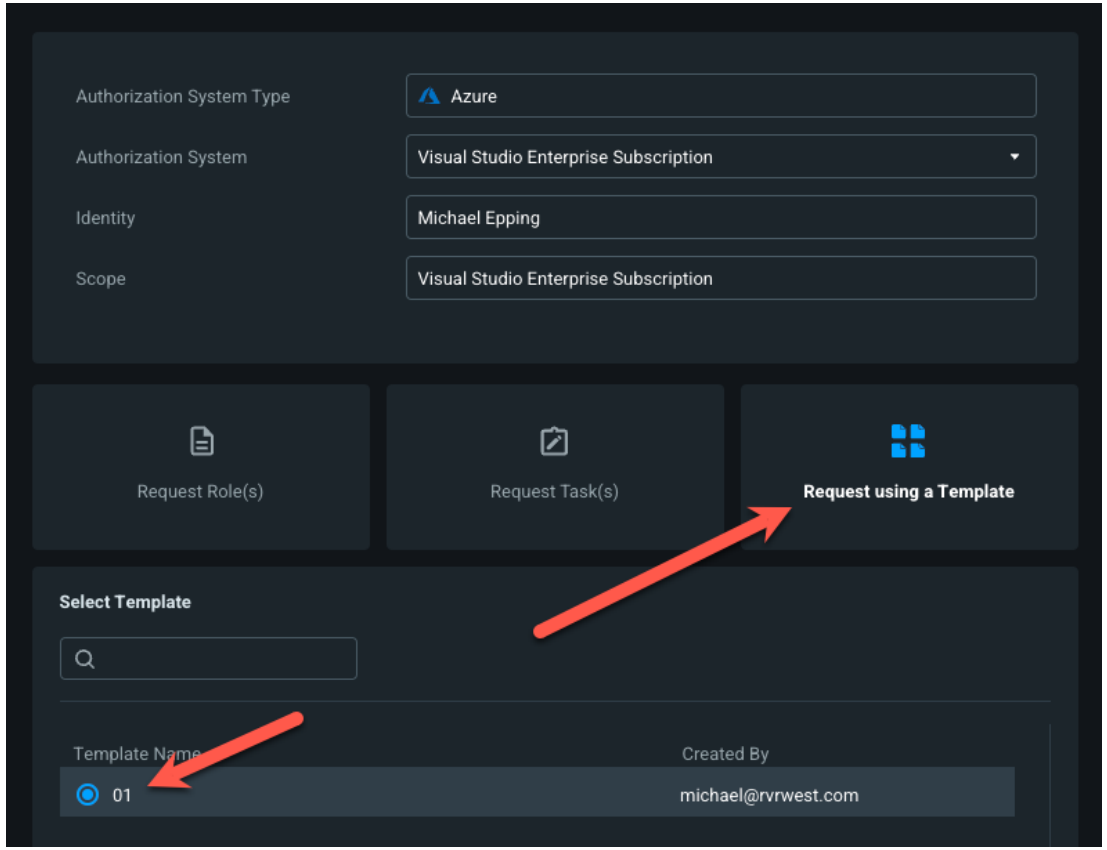
- Templates let you create sets of permissions for users to request
- For example, VM Admins in Azure may need to request multiple permissions within Microsoft.Compute, so configure a template with that set of permissions and any others they may want to request:



Implement Permissions On-Demand

Request Permissions

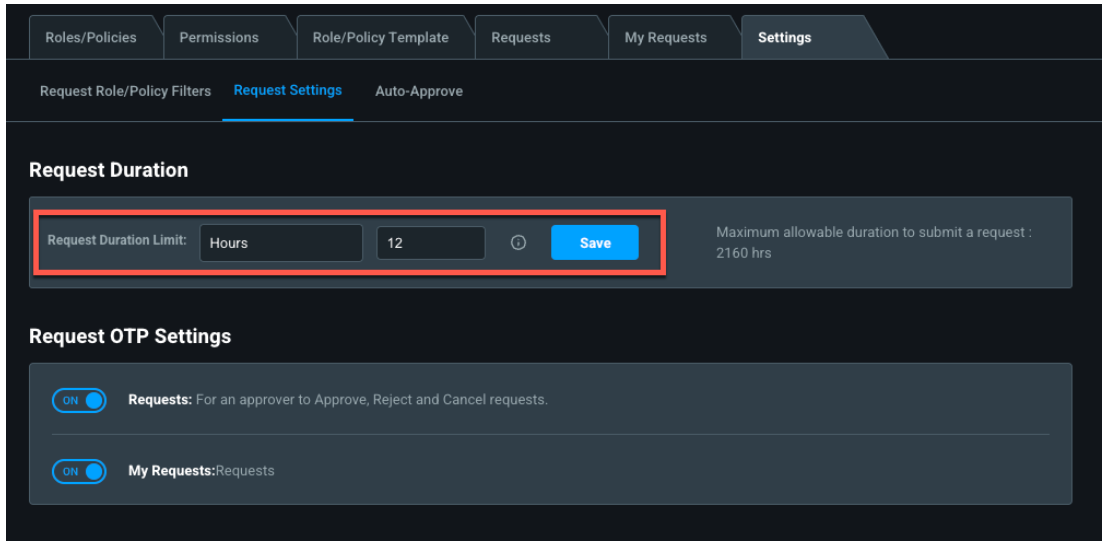
- When the VM Admin goes to request permissions they can do so using the template
  - This reduces the need for them to need to know which individual permissions they may need



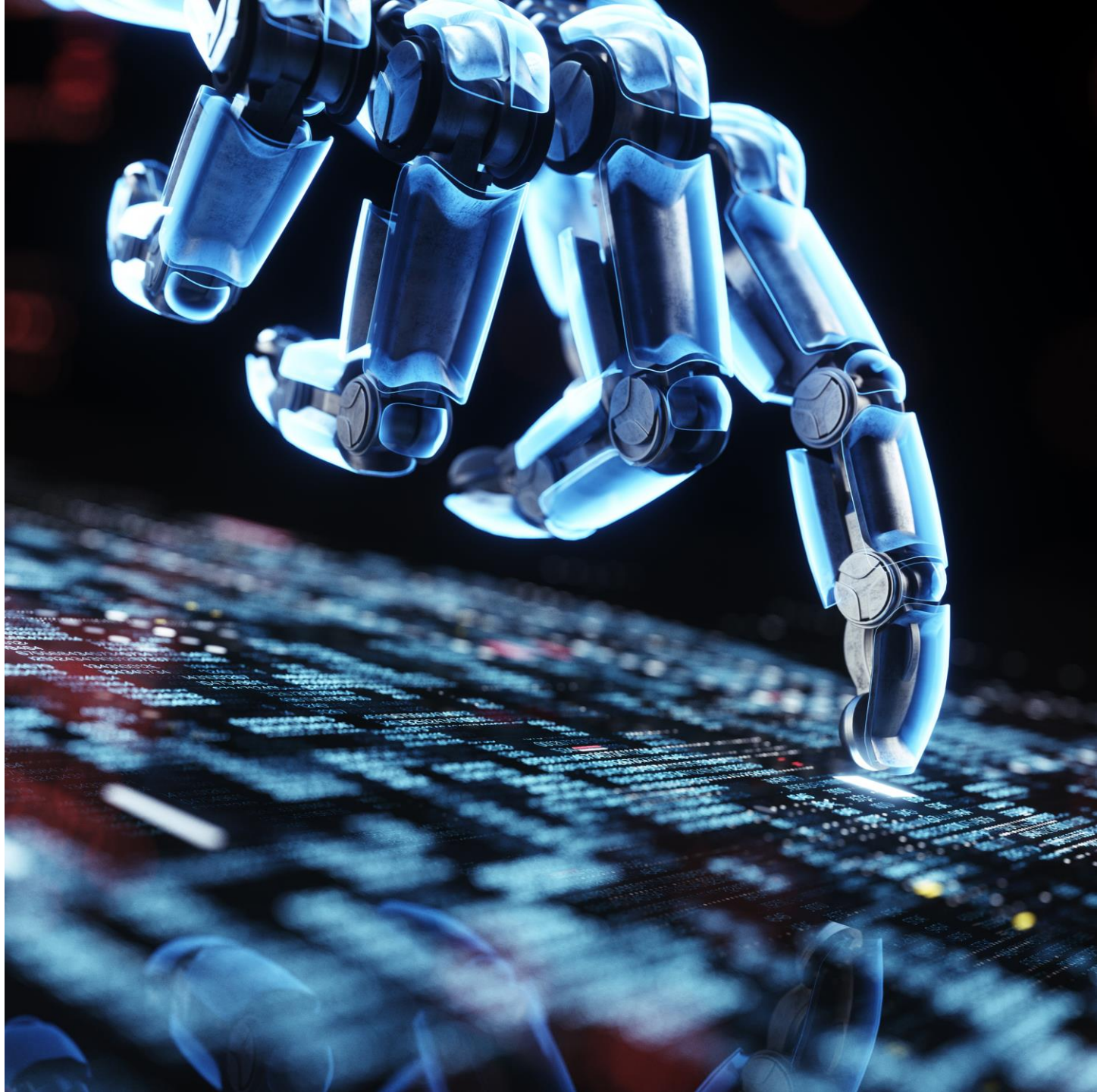
Implement Permissions On-Demand

Configure Request Settings

- Recommended:
  - Configure a maximum request duration that aligns with your longest change window(s)

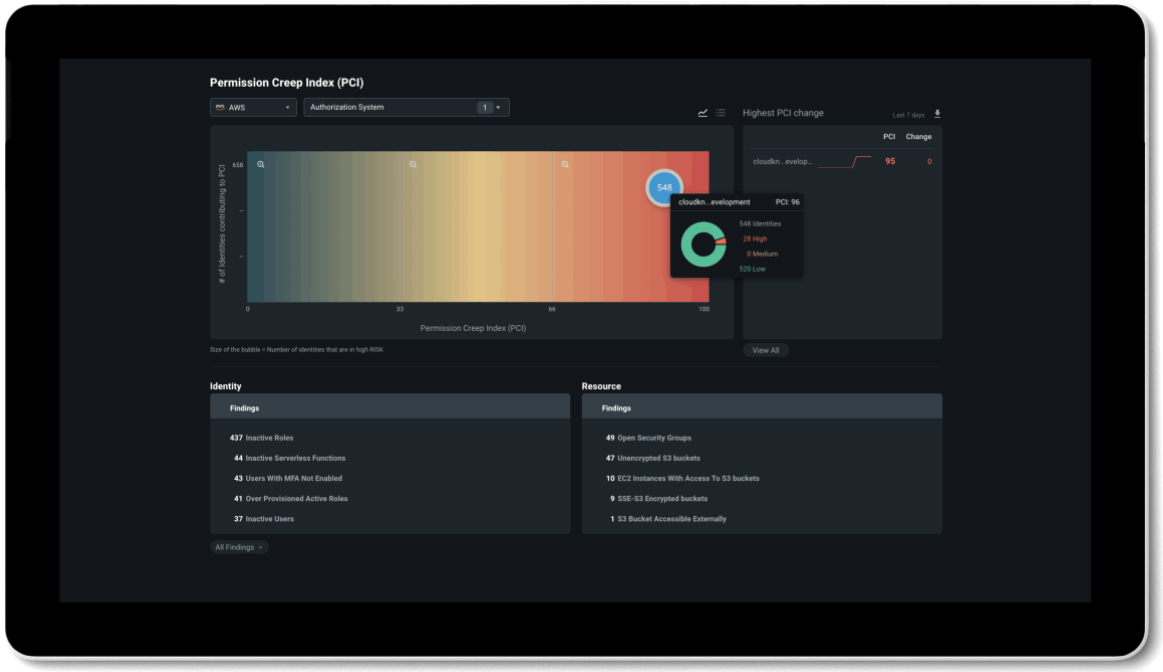


Day 60 Remediations: Permissions Creep Index



Permission Creep Index (PCI):

A single metric that evaluates the gap between permissions granted and permissions used.



What does PCI (Permission Creep Index) identify?

- The number of identities (human and non-human) who have been granted high-risk permissions but aren't using them.

- The number of identities who contribute to the permission creep index (PCI) and where they are on the scale.

The PCI heat map (1/2)

The Permission Creep Index heat map shows the overall calculated permissions gap created by high-risk permissions given to identities but not used. It shows:

- Identities who were given access to high-risk permissions but aren't actively using them. High-risk permissions include the ability to modify or delete information in the authorization system.
- The number of resources an identity has access to, otherwise known as resource reach.
- The high-risk permissions coupled with the number of resources an identity has access to, produce the score seen on the chart. The PCI Trend graph shows you the historical trend of the PCI score over the last 90 days.

The PCI heat map (2/2)

Permissions are classified as high, medium, and low.

High (displayed in red) - The score is between 68 and 100. The identity has access to many high-risk permissions they aren't using and has high resource reach.

Medium (displayed in yellow) - The score is between 34 and 67. The identity has access to some high-risk permissions that they use or have medium resource reach.

Low (displayed in green) - The score is between 0 and 33. The identity has access to few high-risk permissions. They use all their permissions and have low resource reach.

The PCI Trend graph shows you the historical trend of the PCI score over the last 90 days.

Each bubble displays the number of identities that contribute to the PCI score. *High-risk* refers to the number of identities that have permissions which exceed their normal or required usage.

Understanding the data

- View identity findings
  - The Identity section below the heat map on the left side of the page shows all the relevant findings about identities, including inactive, overprovisioned active, serverless functions and other.

- View resource findings
  - The Resource section below the heat map on the right side of the page shows all the relevant findings about your resources. For example, data that is publicly accessible, or an open network security group.

Common Identity findings

- Inactive Identities
  - Identities that haven't performed any* action during the last 90 days**.
- Super Identities
  - Identities that have been given access equivalent to "root".
- Inactive serverless functions
- Inactive groups

* Azure Resource Manager does not track read operations
** Given Entra Permissions Management was running for at least 60 days

Common resource findings

- Open network security groups
- Data exposed publicly to the Internet (Azure Blob Storage, AWS S3 Bucket or GCP Storage Bucket)
- Data encrypted with provider managed keys only (not customer managed keys)

Recommendations

- Set aside time to regularly look at PCI
- Capture the current state of the PCI score so you can compare it when we're done with the POC
- Use PCI to determine identities with biggest blast radius, target those first

Where do we go from here?

- Continue onto Part 5, Automation and Alerts

Thank you!

Microsoft Security