# Microsoft Entra Permissions Management

**Introduction**

**<Name>**

**<Job role>**

Microsoft Security

# Brilliant at the Basics

Triage the most critical items

Goal: Fix in under 30 days

# Investigation Areas

- Internet accessible storage
- Internet exposed ports
- Privileged Accounts
- Privilege Escalation
- Identities that can access secret information/Security Tools (AWS only)
- Inactive Users
- Inactive Apps/Functional accounts
- Inactive Groups

# Critical Investigation Areas

- Internet Accessible
- Most Permissive Accounts
- Inactive Objects

# Storage Accounts, S3 Buckets, GCP Storage

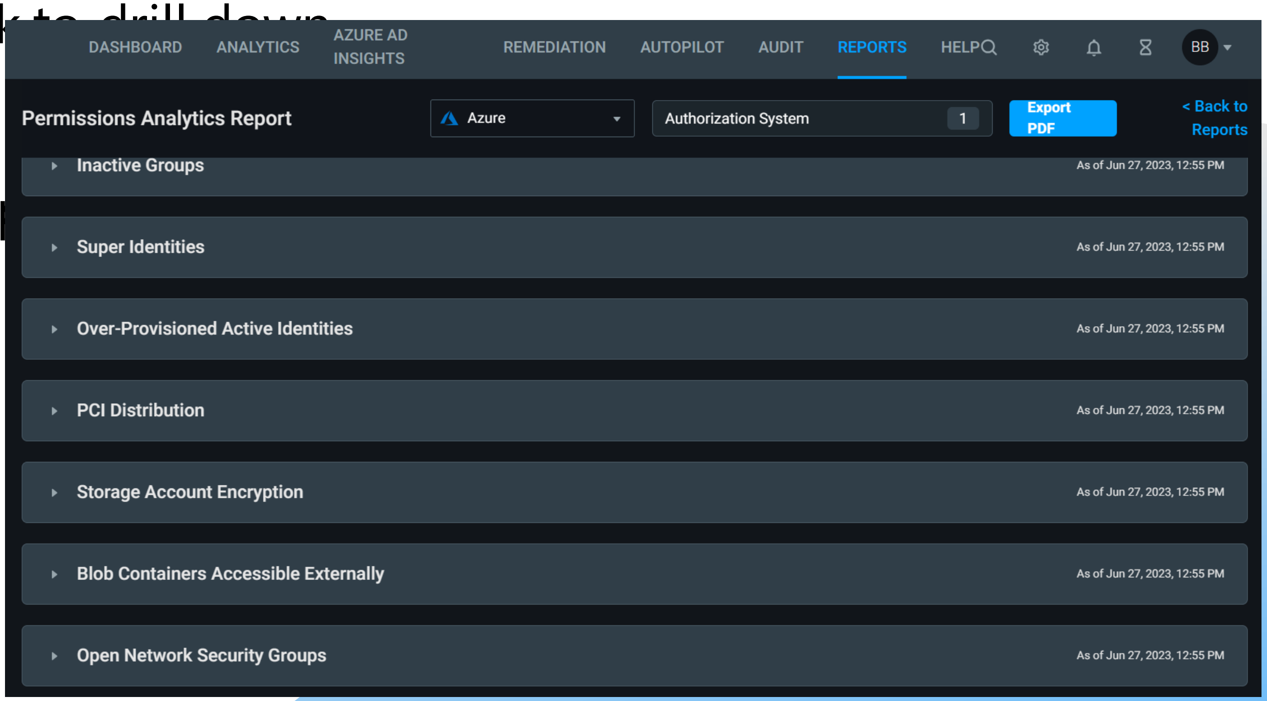
- **Anyone** can access the data in this storage container
- Default off for some time
- Real Life Examples: Numerous (Booz Allen, Dow Jones, Verizon, Time Warner, etc)
- What is your org's policy? Never allowed? Allowed with approval?
  - What processes are in place for creation of these?
  - What processes are in place for monitoring/scanning for these?
- Report-Permissions Analytics Report
- Remediation-Immediately if unexpected, possible IR depending on data exposed

# Azure Storage Account

- Dashboard -> Select Azure as Authorization Systems -> Resources section
  - Blob Containers Accessible External, click to drill down
- Reports -> Permissions Analytics Report
  - Select Azure in the drop down in the upper right
- Remediation steps

# Azure Storage Account

- Dashboard -> Select Azure as Authorization Systems -> Resources section
  - Blob Containers Accessible External, click to drill down
- Reports -> Permissions Analyt
  - Select Azure in the drop down in the up
- Remediation steps



Permissions Analytics Report

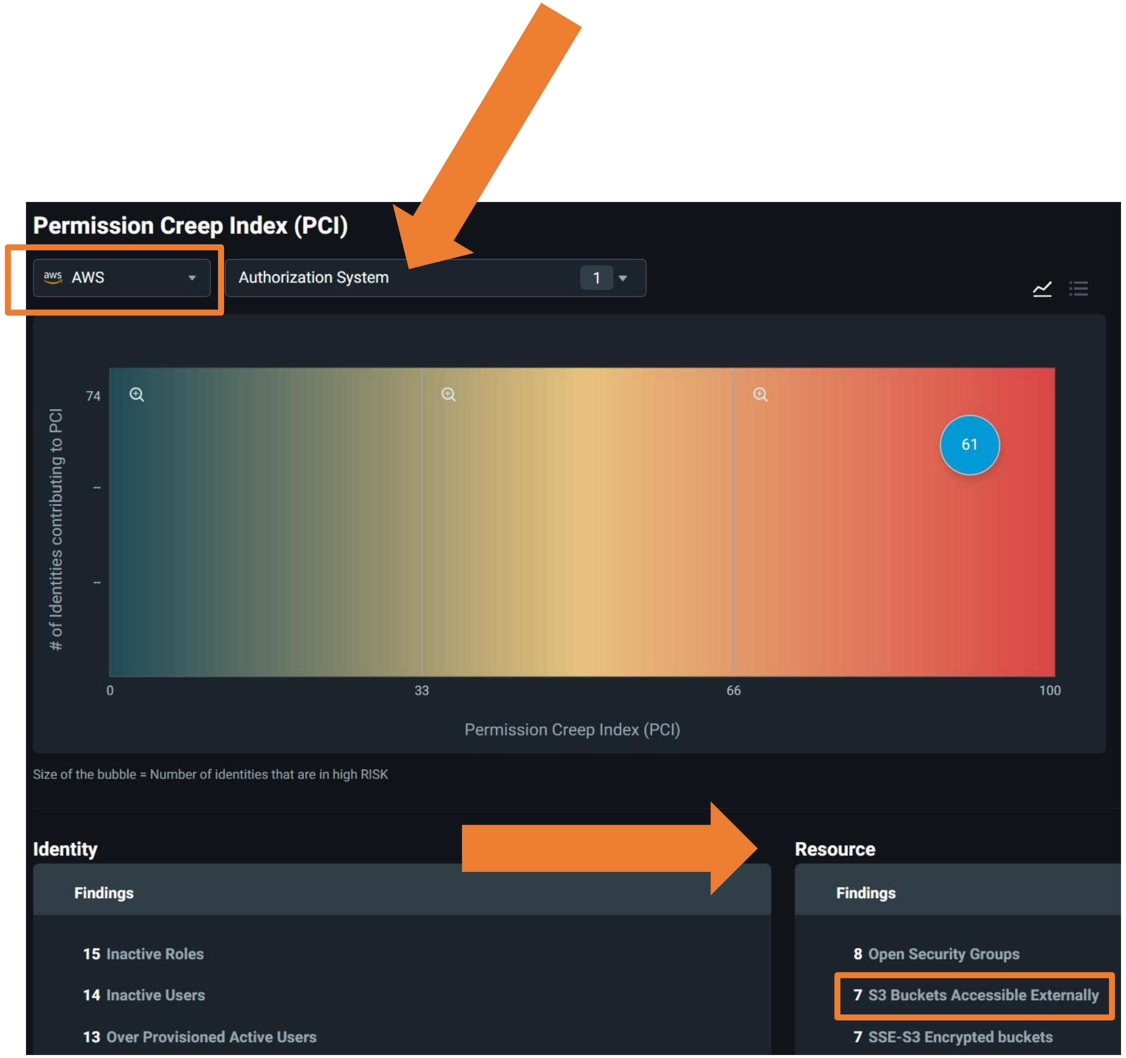
Azure

Authorization System 1

- Inactive Groups — As of Jun 27, 2023, 12:55 PM
- Super Identities — As of Jun 27, 2023, 12:55 PM
- Over-Provisioned Active Identities — As of Jun 27, 2023, 12:55 PM
- PCI Distribution — As of Jun 27, 2023, 12:55 PM
- Storage Account Encryption — As of Jun 27, 2023, 12:55 PM
- Blob Containers Accessible Externally — As of Jun 27, 2023, 12:55 PM
- Open Network Security Groups — As of Jun 27, 2023, 12:55 PM

# AWS S3

- Dashboard -> Select AWS as Authorization Systems -> Resources section
  - S3 Buckets Accessible Externally, click to drill down



Permission Creep Index (PCI)

AWS

Authorization System 1

74
0
33
66
100
61
# of Identities contributing to PCI
Permission Creep Index (PCI)

Size of the bubble = Number of identities that are in high RISK

**Identity**

**Findings**

15 Inactive Roles

14 Inactive Users

13 Over Provisioned Active Users

**Resource**

**Findings**

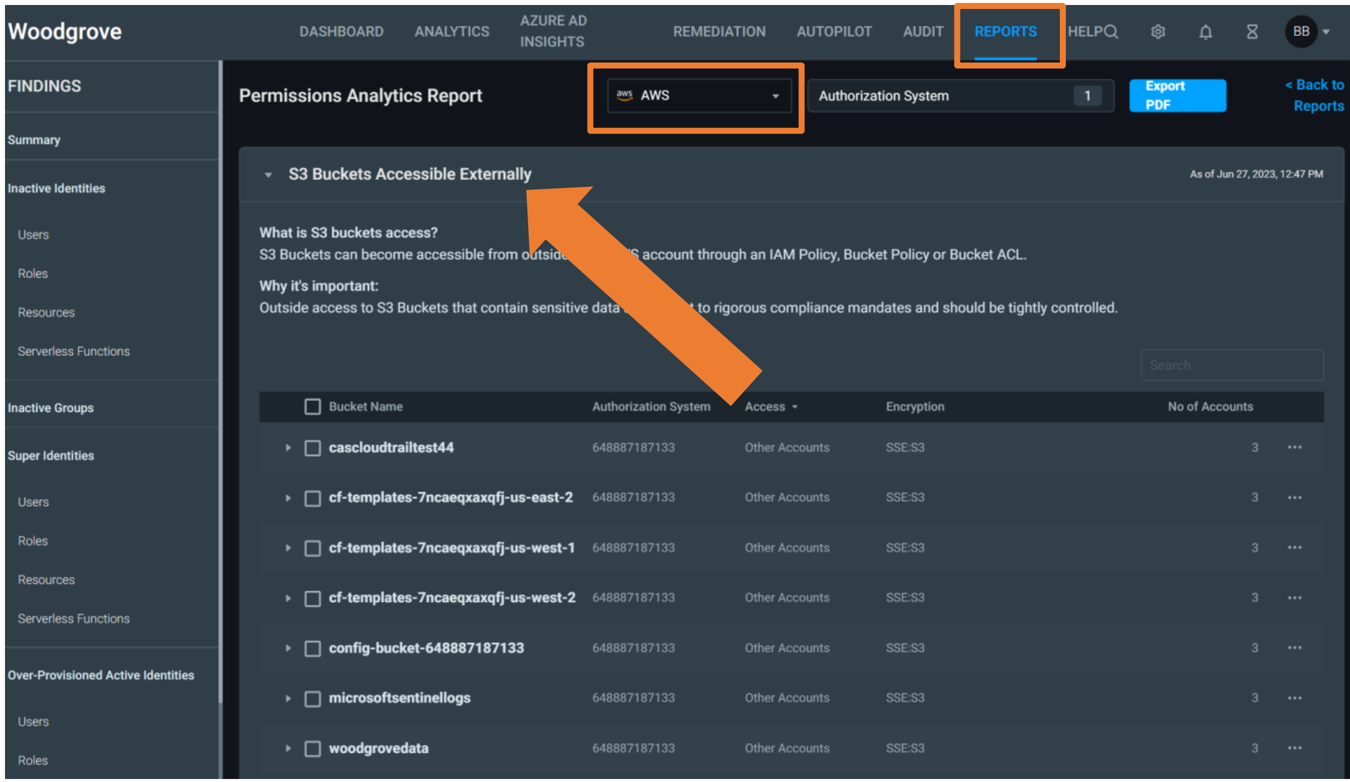
8 Open Security Groups

7 S3 Buckets Accessible Externally

7 SSE-S3 Encrypted buckets

# AWS S3

- After clicking you'll be taken to the following page.
- You can also manually go Reports -> Permissions Analytics Report
  - Select AWS in the drop down in the upper right
  - Scroll to S3 Buckets Accessible Externally



Permissions Analytics Report

AWS

Authorization System 1

S3 Buckets Accessible Externally

As of Jun 27, 2023, 12:47 PM

**What is S3 buckets access?**
S3 Buckets can become accessible from outsid S account through an IAM Policy, Bucket Policy or Bucket ACL.

**Why it's important:**
Outside access to S3 Buckets that contain sensitive data t to rigorous compliance mandates and should be tightly controlled.

| Bucket Name | Authorization System | Access | Encryption | No of Accounts |
|---|---|---|---|---|
| cascloudtrailtest44 | 648887187133 | Other Accounts | SSE:S3 | 3 |
| cf-templates-7ncaeqxaxqfj-us-east-2 | 648887187133 | Other Accounts | SSE:S3 | 3 |
| cf-templates-7ncaeqxaxqfj-us-west-1 | 648887187133 | Other Accounts | SSE:S3 | 3 |
| cf-templates-7ncaeqxaxqfj-us-west-2 | 648887187133 | Other Accounts | SSE:S3 | 3 |
| config-bucket-648887187133 | 648887187133 | Other Accounts | SSE:S3 | 3 |
| microsoftsentinellogs | 648887187133 | Other Accounts | SSE:S3 | 3 |
| woodgrovedata | 648887187133 | Other Accounts | SSE:S3 | 3 |

# AWS S3

- Remediation steps

# GCP Storage

- Dashboard -> Select GCP as Authorization Systems -> Resources section
  - ??, click to drill down
- Reports -> Permissions Analytics Report
  - Select GCP in the drop down in the upper right
- Remediation steps

# Open Network Security Groups, Open Security Groups, GCP VPC Firewall

- **Any IP** can access the resources behind on these ports
  - Foothold, exploit, lateral movement concerns
- Real Life Examples: Scanning, phase 2 of any pentest (paid or free), nmap, Shodan
- What is your org's policy? Never allowed? Allowed with approval?
  - What processes are in place for creation of these?
  - What processes are in place for monitoring/scanning for these?
  - What is the decommission process or these resources?
- Report-Permissions Analytics Report
- Remediation-Immediately if unexpected, most likely IR process

# Azure Open Network Security Groups

- Dashboard -> Select Azure as Authorization Systems -> Resources section
  - Open Network Security Groups -> click to drill down
- Reports -> Permissions Analytics Report
  - Select Azure in the drop down in the upper right
- Remediation steps
  - Close ports if not needed
  - JIT for ports that are needed especially mgmt. ports

# AWS S3

- Dashboard -> Select AWS as Authorization Systems -> Resources section
  - S3 Buckets Accessible Externally, click to drill down
- Reports -> Permissions Analytics Report
  - Select AWS in the drop down in the upper right
- Remediation steps

# GCP VPC Firewall

- Dashboard -> Select GCP as Authorization Systems -> Resources section
  - ??, click to drill down
- Reports -> Permissions Analytics Report
  - Select GCP in the drop down in the upper right
- Remediation steps

# Azure AD Insights

- Portal -> Azure AD Insights
- Reports -> ?
- Remediation steps

# Azure AD Insights

- Privileged Roles in Azure AD must be minimized for human and non-human identities
- Real Life Examples: Tier 0 resource
- What is your org's policy?
  - Are these break glass accounts?
  - How do we handle privilege accounts?
- Report-Permissions Analytics Report
- Remediation-Immediately if unexpected possible IR

# Super Identities

- Human and non-human accounts with equivalent permissions of GA (Azure), Root (AWS), GCP (Super Admin)
- Real Life Examples: Least privilege prevents a bad breach from being even worse.
- What is your org's policy?
  - Human-What is their authentication methods (AAL3/2/1)?
  - Non-Human-What is their authentication methods (MSI/Cert/Shared Secret)?
    - How frequently are these rotated?
  - What processes are in place for creation/deletion of these?
  - What processes are in place for monitoring for these?
  - How do you implement least privilege practices?
- Report-Permissions Analytics Report
- Remediation-Immediately if unexpected possible IR

# Azure Super Identities

- Reports -> Permissions Analytics Report
  - Select Azure in the drop down in the upper right
  - Scroll to “Super Users” section
    - Inspect with customer Users, Service Principles, Serverless Functions
- Remediation steps

# AWS Super Identities

- Reports -> Permissions Analytics Report
  - Select AWS in the drop down in the upper right
  - Scroll to “Super Users” section
    - Inspect with customer Users, Service Principles, Serverless Functions
    - NOTE: Resources is AWS specific. **TO DO Examples***

- Remediation steps

# GCP Super Identities

- Reports -> Permissions Analytics Report
  - Select Azure in the drop down in the upper right
  - Scroll to “Super Users” section
    - Inspect with customer Users, Service Principles, Serverless Functions
- Remediation steps

# Privilege Escalation

- Misconfigured IAM policy or configuration oversight will allow elevated access to other permissions or resources
- Real Life Example: Numerous (ProxyNotShell (Exchange), AnyConnect, vCenter)
- What is your org's policy?
  - Toxic combination?
  - What processes are in place for monitoring for these?
- Report-Permissions Analytics Report
- Remediation-Immediately if unexpected possible IR

# Azure Privilege Escalation

- Reports -> Permissions Analytics Report
  - Select Azure in the drop down in the upper right
  - Scroll to “Privilege Escalation” section
    - Inspect with customer Users, Service Principles, Serverless Functions
- Remediation steps

# AWS Privilege Escalation

- Reports -> Permissions Analytics Report
  - Select AWS in the drop down in the upper right
  - Scroll to “Privilege Escalation” section
    - Inspect with customer Users, Service Principles, Serverless Functions
    - NOTE: Resources is AWS specific. **TO DO Examples***

- Remediation steps

# GCP Privilege Escalation

- Reports -> Permissions Analytics Report
  - Select Azure in the drop down in the upper right
  - Scroll to “Privilege Escalation” section
    - Inspect with customer Users, Service Principles, Serverless Functions
- Remediation steps

# Identities that can access secret information/Security Tools (AWS)

- Identities that have privilege to read/modify/delete secrets, or make changes to security tools
- What is your org's policy?
  - How do you rotate secrets or protect them?
  - What processes are in place for monitoring for actions on these secerets?
  - Change management process?
- Report-Permissions Analytics Report
- Remediation-Immediately if unexpected possible IR

# Identities that can access secret information/Security Tools (AWS)

- Reports -> Permissions Analytics Report
  - Select AWS in the drop down in the upper right
  - Scroll to “Identities that can access secret information/security tools” sections
    - Inspect with customer Users, Roles, Serverless Functions
    - NOTE: Resources is AWS specific. **TO DO**8

- Remediation steps

# Inactive Users

- Human identity that haven’t performed a write action in last 90 days
- Real Life Example: Account take over, possibly no MFA.
- What is your org's policy?
  - Removal of stale accounts?
  - What processes are in place for monitoring for activity on these accounts?
- Report-Permissions Analytics Report
- Remediation-Immediately clean up

# Azure Inactive Users

- Dashboard -> Select Azure as Authorization Systems -> Findings section
  - Inactive users
- Reports -> Permissions Analytics Report
  - Select Azure in the drop down in the upper right
  - Scroll down to Inactive Identities
- Remediation steps

# AWS Inactive Users

- Dashboard -> Select AWS as Authorization Systems -> Findings section
  - Inactive Users , click to drill down
- Reports -> Permissions Analytics Report
  - Select AWS in the drop down in the upper right
    - Scroll down to Inactive identities
    - Inspect with customer Users, Service Principles, Serverless Functions
    - NOTE: Resources is AWS specific. **TO DO Examples***
- Remediation steps

# GCP Inactive Users

- Dashboard -> Select GCP as Authorization Systems -> Identity section
  - Inactive Users, click to drill down
- Reports -> Permissions Analytics Report
  - Select GCP in the drop down in the upper right
  - Scroll down to Inactive Identities
- Remediation steps

# Inactive Apps/Functional Accounts

- Non-human identity that haven’t performed an action in last 90 days
- Real Life Example: Account take over and NO MFA!
- What is your org's policy?
  - Removal of stale service accounts?
  - What processes are in place for monitoring for activity on these accounts?
- Report-Permissions Analytics Report
- Remediation-Immediately clean up

# Azure Inactive Apps/Functional Accounts

- Dashboard -> Select Azure as Authorization Systems -> Findings section
    - Inactive Apps/Functional Accounts Reports ->
- Reports -> Permissions Analytics Report
    - Select Azure in the drop down in the upper right
    - Scroll down to Inactive Identities
- Remediation steps

# AWS Inactive Apps/Functional Accounts

- Dashboard -> Select AWS as Authorization Systems -> Findings section
    - Inactive Users , click to drill down
- Reports -> Permissions Analytics Report
    - Select AWS in the drop down in the upper right
        - Scroll down to Inactive identities
        - Inspect with customer Service Principles, Serverless Functions
        - NOTE: Resources is AWS specific. **TO DO Examples***
- Remediation steps

# GCP Inactive Apps/Functional Accounts

- Dashboard -> Select GCP as Authorization Systems -> Findings section
  - Inactive Service Accounts, click to drill down
- Reports -> Permissions Analytics Report
  - Select GCP in the drop down in the upper right
  - Scroll down to Inactive Identities
- Remediation steps

# Inactive Groups

- Members that haven’t performed any action on any resource in the last 90 days
- What is your orgs policy?
  - What resources do groups have access to?
  - How is membership governed to these groups and resources?
- Report-Permissions Analytics Report
- Remediation-Immediately clean up

# Azure Inactive Groups

- Dashboard -> Select Azure as Authorization Systems -> Findings section
  - Inactive Groups, click to drill down
- Reports -> Permissions Analytics Report
  - Select Azure in the drop down in the upper right
  - Scroll down to Inactive Groups
- Remediation steps

# AWS Inactive Groups

- Dashboard -> Select AWS as Authorization Systems -> Findings section
  - Inactive Groups, click to drill down
- Reports -> Permissions Analytics Report
  - Select AWS in the drop down in the upper right
  - Scroll down to Inactive Groups
- Remediation steps

# GCP Inactive Groups

- Dashboard -> Select GCP as Authorization Systems -> Findings section
  - Inactive Groups, click to drill down
- Reports -> Permissions Analytics Report
  - Select GCP in the drop down in the upper right
  - Scroll down to inactive groups
- Remediation steps

# Thank you!

Microsoft Security