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

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
- Automation/Alerting-?
- Remediation-Immediately if unexpected, possible IR depending on data exposed

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
- Automation/Alerting-?
- Remediation-Immediately if unexpected, most likely IR process

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
- Automation/Alerting-?
- 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
- Automation/Alerting-?
- Remediation-Immediately if unexpected possible IR

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
- Automation/Alerting-?
- Remediation-Immediately if unexpected possible IR

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

- Identities that have privilege to read/modify/delete secrets, or make changes to security tools
- **Find Breach Example**
- 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
- Automation/Alerting-?
- Remediation-Immediately if unexpected possible IR

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
- Automation/Alerting-?
- Remediation-Immediately clean up

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
- Automation/Alerting-?
- Remediation-Immediately clean up

Inactive Groups

- Members that haven’t performed any action on any resource in the last 90 days
- **Find Breach Example**
- 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
- Automation/Alerting-?
- Remediation-Immediately clean up

Thank you!

Microsoft Security