Entra Permissions Management Dashboard

PCI Distribution

● Max of Human Count ● Max of Non-human Count

Y-axis: Human vs Non-Human count (0, 10, 20)
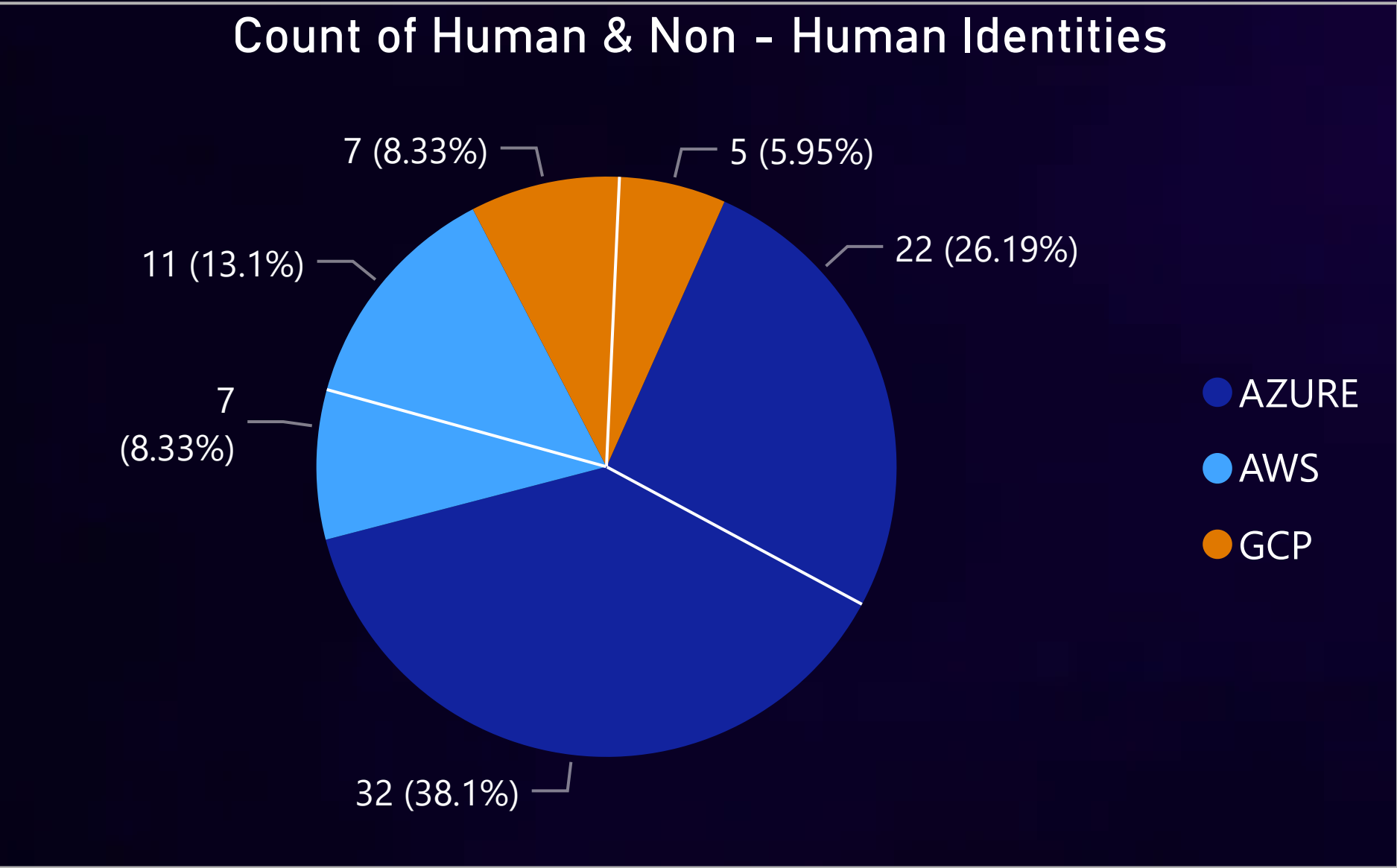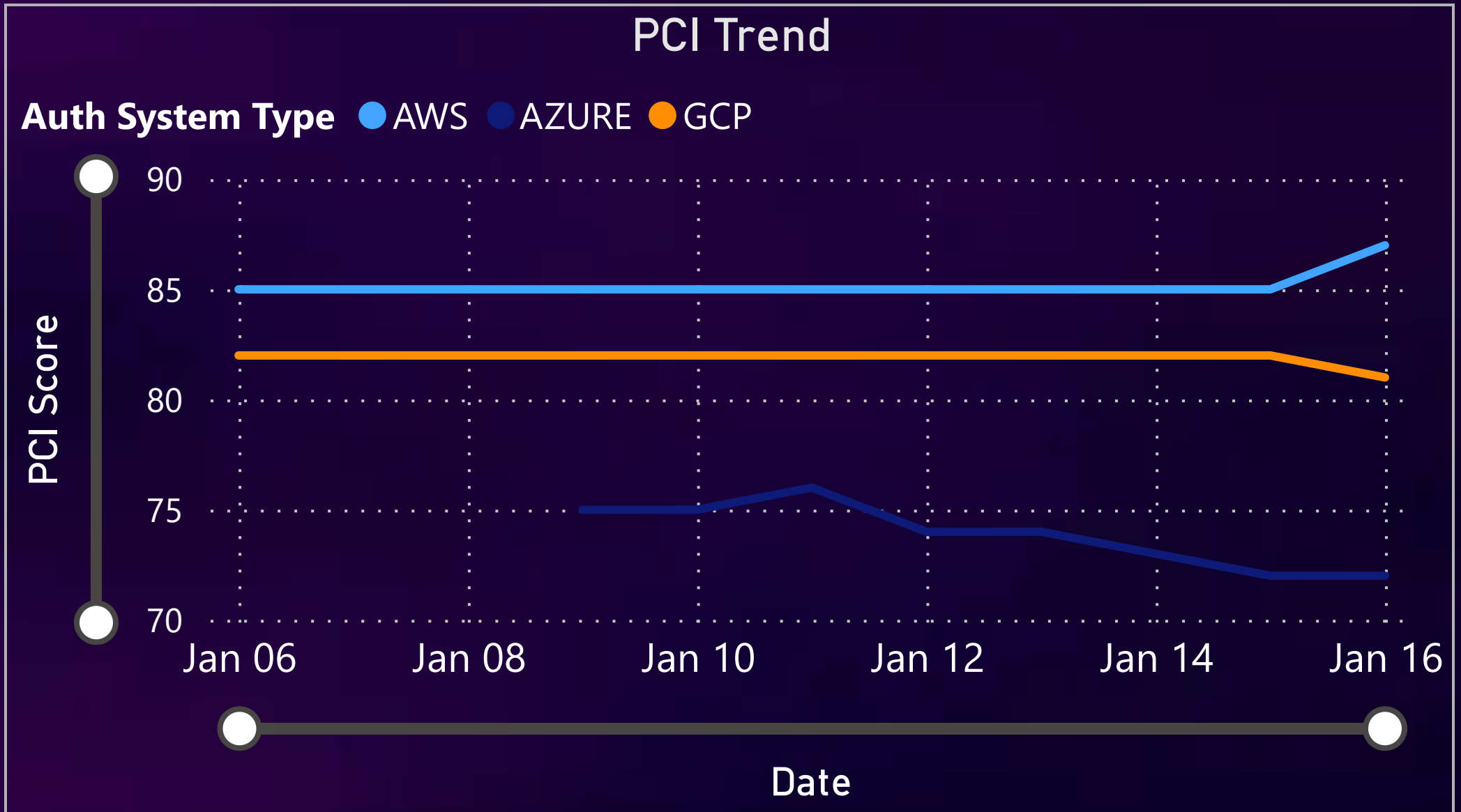X-axis: Cloud — AWS, AZURE, GCP
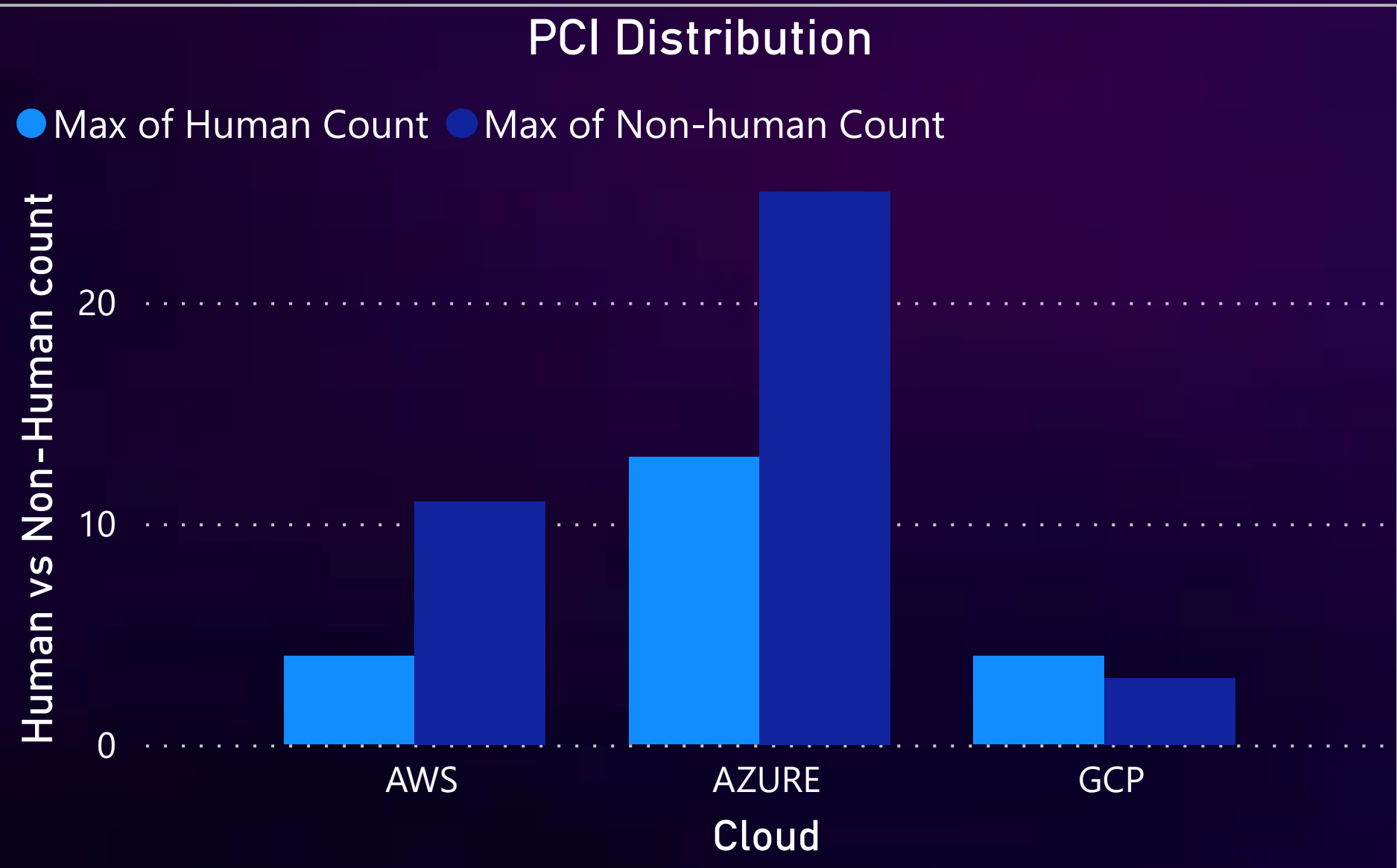
PCI Health Status

Cloud provider	PCI Status
AWS	HIGH
AZURE	HIGH
GCP	HIGH

Cloud

- ☐ AWS
- ☐ AZURE
- ☐ GCP

PCI Trend

Auth System Type ● AWS ● AZURE ● GCP

Y-axis: PCI Score (70, 75, 80, 85, 90)
X-axis: Date — Jan 06, Jan 08, Jan 10, Jan 12, Jan 14, Jan 16

Count of Human & Non - Human Identities

- 7 (8.33%)
- 5 (5.95%)
- 22 (26.19%)
- 11 (13.1%)
- 7 (8.33%)
- 32 (38.1%)

● AZURE
● AWS
● GCP

Access Key Entitlement - GCP

47
Resources With Access

4624
Tasks Granted

0
Tasks Used

82
Risk Score

gsuite
Service Account Name

221

Group Entitlements And Usage

Group Name	Authorization System	Risk Score	Tasks Gra
Azure ML Data Scientist	AZURE	1	
Azure ML Data Scientist	AZURE	1	
epmtest_usergroup	AWS	7	
epmtest_usergrp2	AWS	7	
epmtest_usergrp2	AWS	7	
Security_Admins	AZURE	2	
Security_Admins	AZURE	2	
Security_Admins	AZURE	2	
Sentinel_Automation_Contributors	AZURE	0	
Sentinel_Automation_Contributors	AZURE	0	
Sentinel_Contributors	AZURE	2	
Sentinel_Contributors	AZURE	2	
Sentinel_Contributors	AZURE	2	
Sentinel_Contributors	AZURE	2	
Sentinel_Contributors	AZURE	2	
Sentinel_Contributors	AZURE	2	
Sentinel_Contributors	AZURE	2	
Sentinel_Contributors	AZURE	2	

Application Access Key Entitlement - Azure

Key Id	Key Name	Key Type	Risk Score	# Resources With Access	# Tasks Granted	# Tasks Used	A
###########565676	Qradar	ACCESS_KEY	1	361	5067	0	

Permission Analytics Dashboard

8
Users with Priv. Escalations

539
Total # of Tasks Used

898K
Total # Tasks Granted

435K
Permission Gap (Unused ...

Top 3 Risky Identities

epm_testuse...	AWS
Name	Cloud
100	
PCI	

epm_testuse...	AWS
Name	Cloud
100	
PCI	

| epm_testuse... | AWS |

Details of Identities with Privilege Escalations

Name	# of Escalations	PCI	Category
epm_testuser1	8	100	Users - Privil
epm_testuser3	3	17	Users - Privil
epm_testuser4	7	100	Users - Privil
epm_testuser5	8	100	Users - Privil
epm_testuser6	7	7	Users - Privil
epm_testuser7	7	7	Users - Privil
mciem-collection-role	3	1	Roles - Privil

Permission Analytics Filter

Category
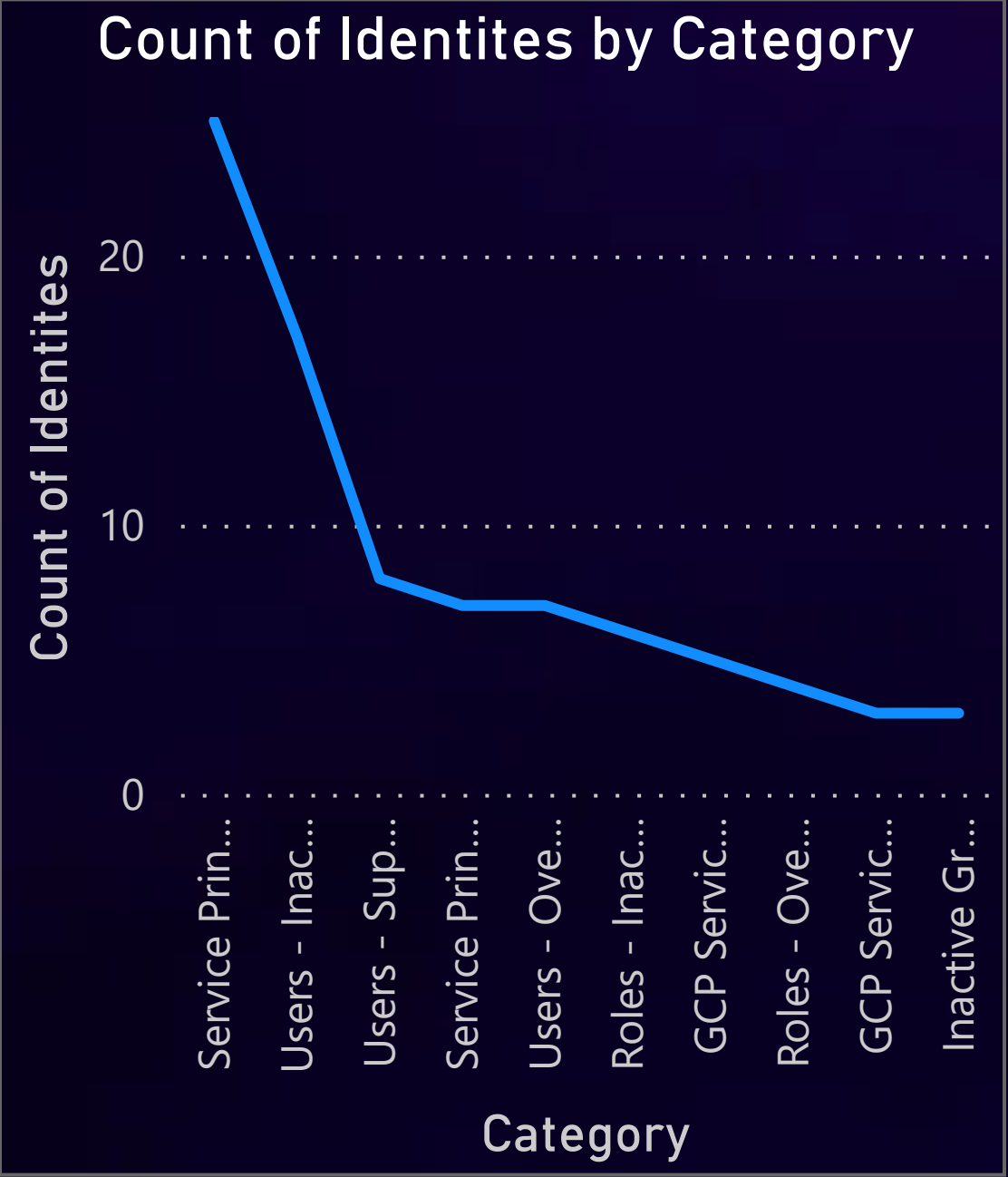
- ☐ (Blank)
- ☐ GCP Service Accounts - Inactive
- ☐ GCP Service Accounts - Super Id
- ☐ Inactive Groups
- ☐ Roles - Inactive Identities
- ☐ Roles - Over-Provisioned Active
- ☐ Service Principals - Inactive

Count of Identites by Category

Name	PCI	Type	Tasks Used	Tasks Max	Ta
ActionsOnMachine	2	MANAGED_IDENTITY	0	12670	
Add-HostToWatchlist-IncidentTrigger	58	MANAGED_IDENTITY	0	12670	
Add-IPToWatchlist-IncidentTrigger	1	MANAGED_IDENTITY	0	12670	
Add-UserToWatchlist-IncidentTrigger	1	MANAGED_IDENTITY	0	12670	
AmazonEKSNodeRole	0		0	10786	
ap	0	ED	0	12670	
AutoResponder-Playbook	0	MANAGED_IDENTITY	0	12670	
AWS-MDCSetup-HostMgmtRole-ap-south-1	1		0	10786	
Azure Information Protection	19	APP	0	12670	
Azure Security Insights	0	APP	0	12670	
Azure Sentinel Content Deployment App	1	APP	0	12670	

Entitlement Usage Dashboard

Total # of identities considered

7

# of Users with MFA e...

11 (12.79%)
8 (9.3%)
67 (77.91%)
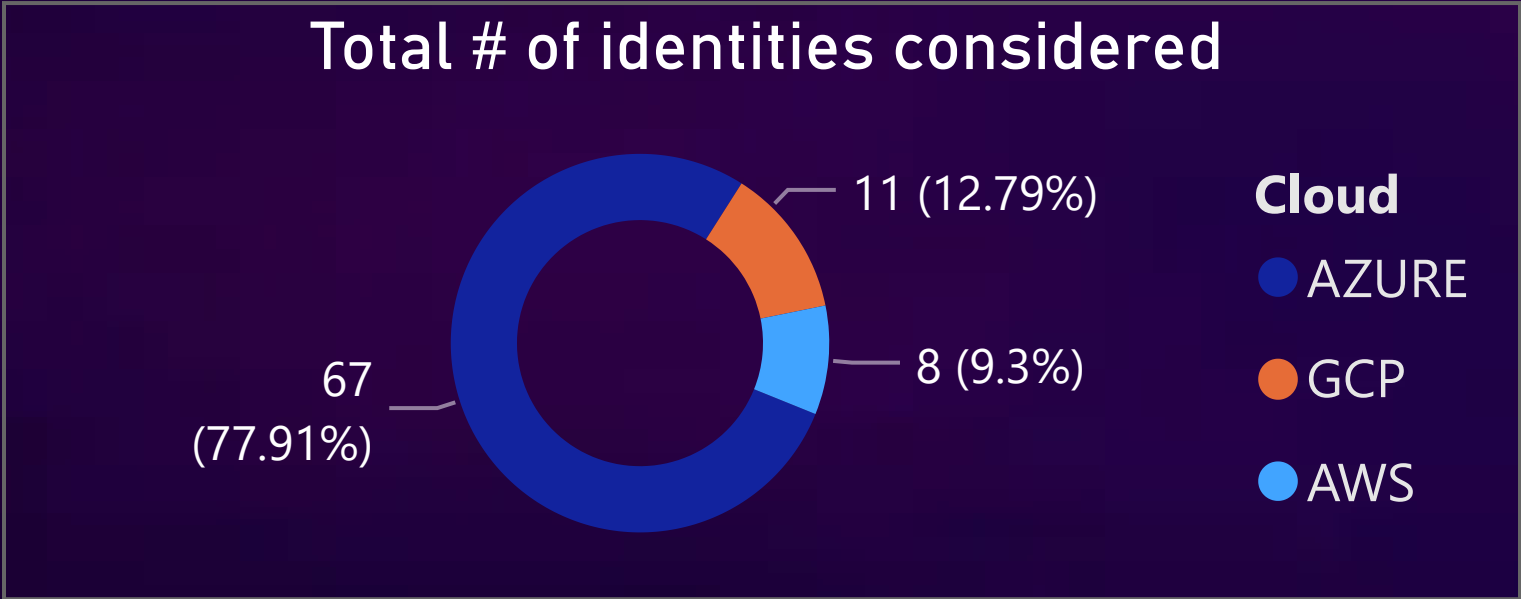
Cloud
- AZURE
- GCP
- AWS

Identity Type
- [ ] APPLICATION
- [ ] MANAGED_IDENTITY
- [ ] SERVICE_ACCOUNT
- [ ] USER

Cloud
- [ ] AWS
- [ ] AZURE
- [ ] GCP

Users with access to Critical services

3 (50%)   3 (50%)

Category
- Users - Sec...
- Users - Sec...
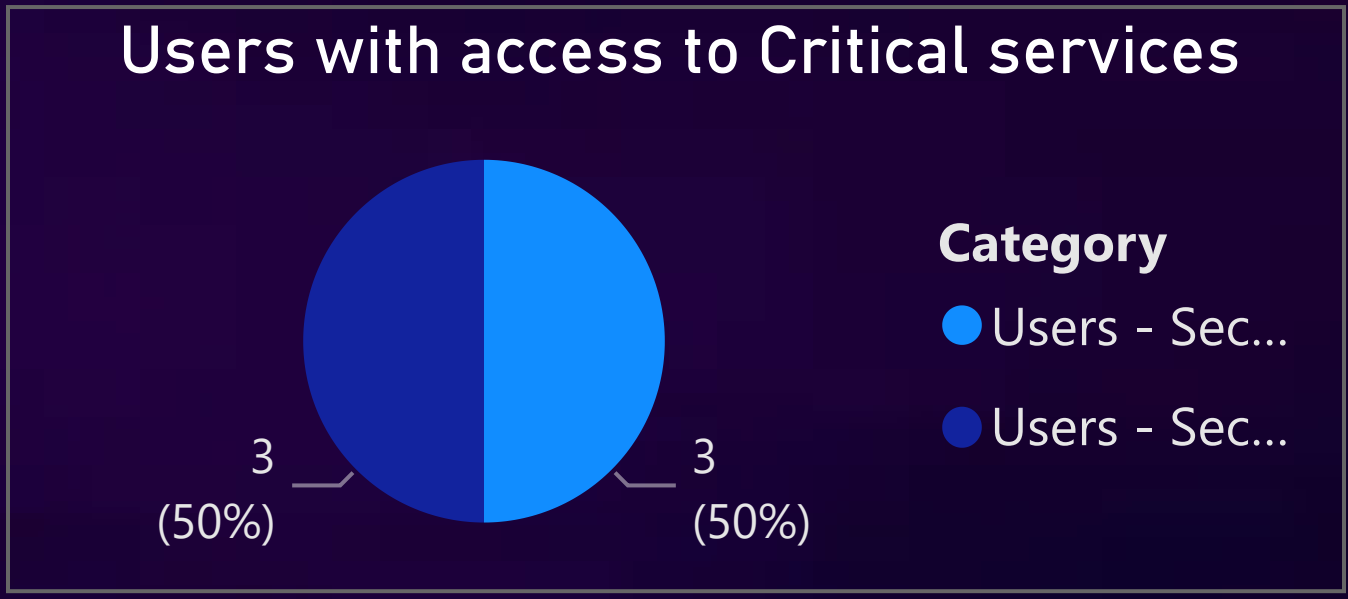
Open Security Groups

Name	Inbound Ports	# of Virtual Machines	Authorization System
Sentinel_RG/nsg1	22,514,80,80	1	Azure Sub Name
Sentinel_RG/nsg2	22,50,514,514	0	Azure Sub Name
Sentinel_RG/nsg3	3389	0	Azure Sub Name

All permissions for identity

Identity Type	Resource/Policy Name	Resource/Policy Type	Role Nam
APPLICATION	Azure Sub Name	RESOURCE	Monitorin
APPLICATION	Azure Sub Name	RESOURCE	Reader
APPLICATION	Azure Sub Name	RESOURCE	User Acce
APPLICATION	Azure Sub Name	RESOURCE	VM Scann
APPLICATION	cloud-shell-storage-southeastasia	RESOURCE	Microsoft
APPLICATION	Qradar	RESOURCE	Monitorin
APPLICATION	Qradar	RESOURCE	Monitorin
APPLICATION	RG	RESOURCE	Logic App
APPLICATION	RG	RESOURCE	Microsoft
APPLICATION	RG	RESOURCE	Microsoft

User Entitlements and Usage

Authorization System ● AWS ● AZURE ● GCP ○ Sum of Tasks Used

Sum of Tasks Granted (left axis): 0K, 50K, 100K
Sum of Tasks Used (right axis): 0, 100, 200, 300, 400

Type: USER, MANAGED_IDENTI..., APPLICATION, SERVICE_ACCOUNT, ROLE

Role Status

0.1K (3.87%)
2.46K (96.13%)

Role S...
- UN...
- ASS...

of roles assigned under each role type

Count of Role Type: 0K, 2K

Role Type: SYSTEM, CLOUDK..., CUSTOM, INLINE, RESOURCE