Azure Cloud Security

Posture Assessment and Improvement Project

Jeremy Duong

Mentor

Keith Wingate

Agenda

- ☑ Project Overview
- ☑ Purpose & Objectives
- ☑ Scope
- ☑ Tools Usage
- ☑ Key Findings
- ☑ Recommendations & Level of Effort
- ☑ Risks
- ☑ Success Criteria
- ☑ Lessons Learned

Project Overview

- **What it is** 🔒
- 10-week Azure Cloud Security Posture Assessment
- Goal: Evaluate current security posture and recommend improvements
- **What I did** ⚙️
- Resource inventory (AD, VMs, Storage, Key Vaults, NSGs, Firewall)
- Baseline security review (Azure Security Score)
- Automated scans (ScoutSuite) + manual checks
- **What came out** 📑
- Prioritized findings with severity levels
- Remediation recommendations with Level of Effort (quick wins vs long-term fixes)
- Final report & presentation to the Cloud Security Team

Goals

Objective

- Gain hands-on experience with Azure security tools and policies
- Document and quantify findings
- Evaluate and improve Azure cloud security posture
- Identify misconfigurations and risks
- Provide actionable recommendations aligned with the CIS Benchmarks and Microsoft best practices

In Scope

- User accounts & access (Azure AD, MFA, roles)
- Virtual Machines
- Data Storage (Storage accounts, key vaults)
- Applications (App Services)
- Network security (NSGs, Azure Firewall)
- Security tools (ScoutSuite, Defender for Cloud)

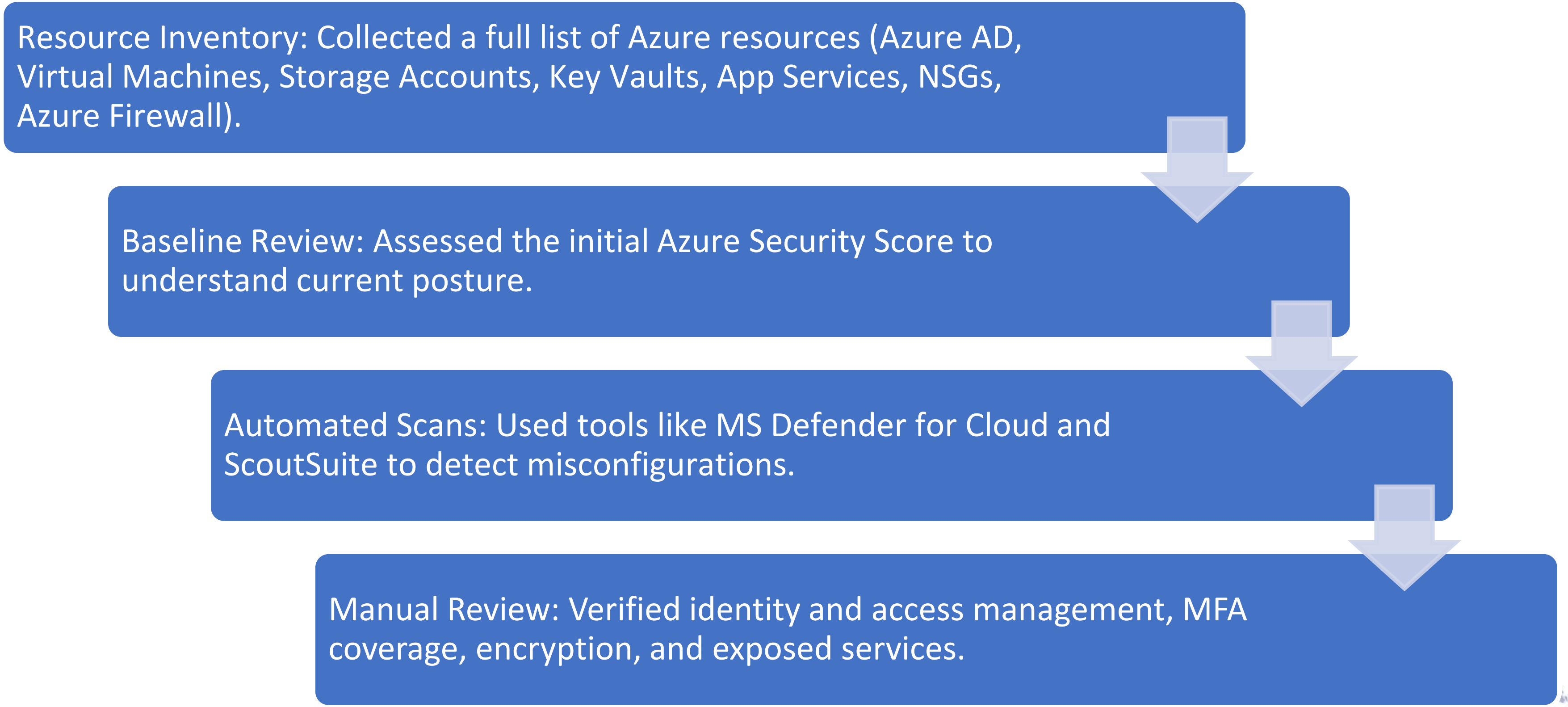
Out of Scope

Direct production changes

On-premises/hybrid systens

Critical OT systems (unless supervised)

Key Activities



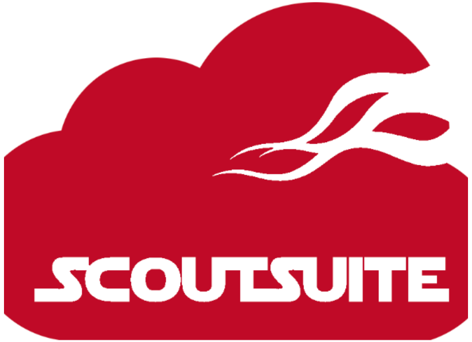
Resource Inventory: Collected a full list of Azure resources (Azure AD, Virtual Machines, Storage Accounts, Key Vaults, App Services, NSGs, Azure Firewall).

Baseline Review: Assessed the initial Azure Security Score to understand current posture.

Automated Scans: Used tools like MS Defender for Cloud and ScoutSuite to detect misconfigurations.

Manual Review: Verified identity and access management, MFA coverage, encryption, and exposed services.

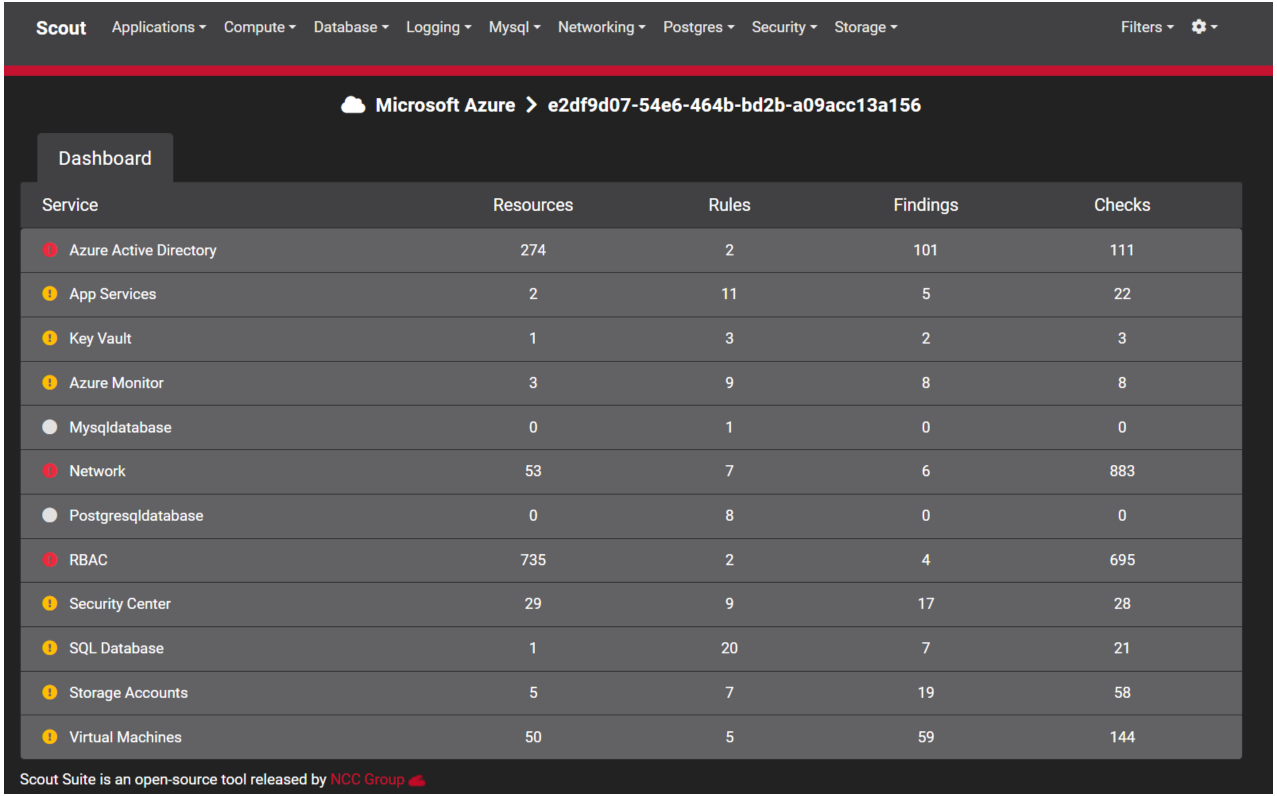
Tools Usage



ScoutSuite 🛠️

- Open-source cloud security auditing tool
- Scanned Azure resources for misconfigurations
- Helped identifying risks in identity, storage, network, and VM setups
- Gave a structured report for analysis and prioritization

ScouteSuite Overview



Microsoft Azure > e2df9d07-54e6-464b-bd2b-a09acc13a156

Dashboard

Service	Resources	Rules	Findings	Checks
Azure Active Directory	274	2	101	111
App Services	2	11	5	22
Key Vault	1	3	2	3
Azure Monitor	3	9	8	8
Mysqldatabase	0	1	0	0
Network	53	7	6	883
Postgresqldatabase	0	8	0	0
RBAC	735	2	4	695
Security Center	29	9	17	28
SQL Database	1	20	7	21
Storage Accounts	5	7	19	58
Virtual Machines	50	5	59	144

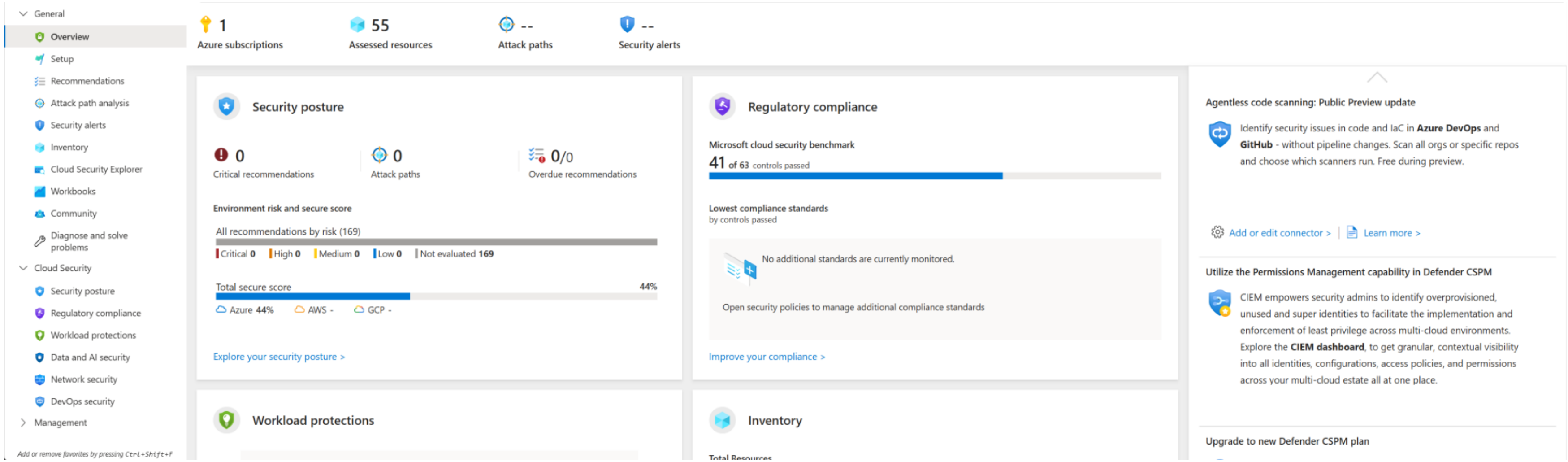
Scout Suite is an open-source tool released by NCC Group

Tools Usage

Microsoft Defender for Cloud 🔒

- Built-in Azure security monitoring tool
- Provided a baseline security score
- Highlighted vulnerabilities, missing protections, and compliance gaps
- Helped track overall security posture over time

Microsoft Defender for Cloud Overview



1 Azure subscriptions | 55 Assessed resources | -- Attack paths | -- Security alerts

Security posture

0 Critical recommendations | 0 Attack paths | 0/0 Overdue recommendations

Environment risk and secure score

All recommendations by risk (169)

Critical 0 | High 0 | Medium 0 | Low 0 | Not evaluated 169

Total secure score 44%

Azure 44% | AWS - | GCP -

Explore your security posture >

Regulatory compliance

Microsoft cloud security benchmark

41 of 63 controls passed

Lowest compliance standards
by controls passed

No additional standards are currently monitored.

Open security policies to manage additional compliance standards

Improve your compliance >

Agentless code scanning: Public Preview update

Identify security issues in code and IaC in **Azure DevOps** and **GitHub** - without pipeline changes. Scan all orgs or specific repos and choose which scanners run. Free during preview.

Add or edit connector > | Learn more >

Utilize the Permissions Management capability in Defender CSPM

CIEM empowers security admins to identify overprovisioned, unused and super identities to facilitate the implementation and enforcement of least privilege across multi-cloud environments. Explore the **CIEM dashboard**, to get granular, contextual visibility into all identities, configurations, access policies, and permissions across your multi-cloud estate all at one place.

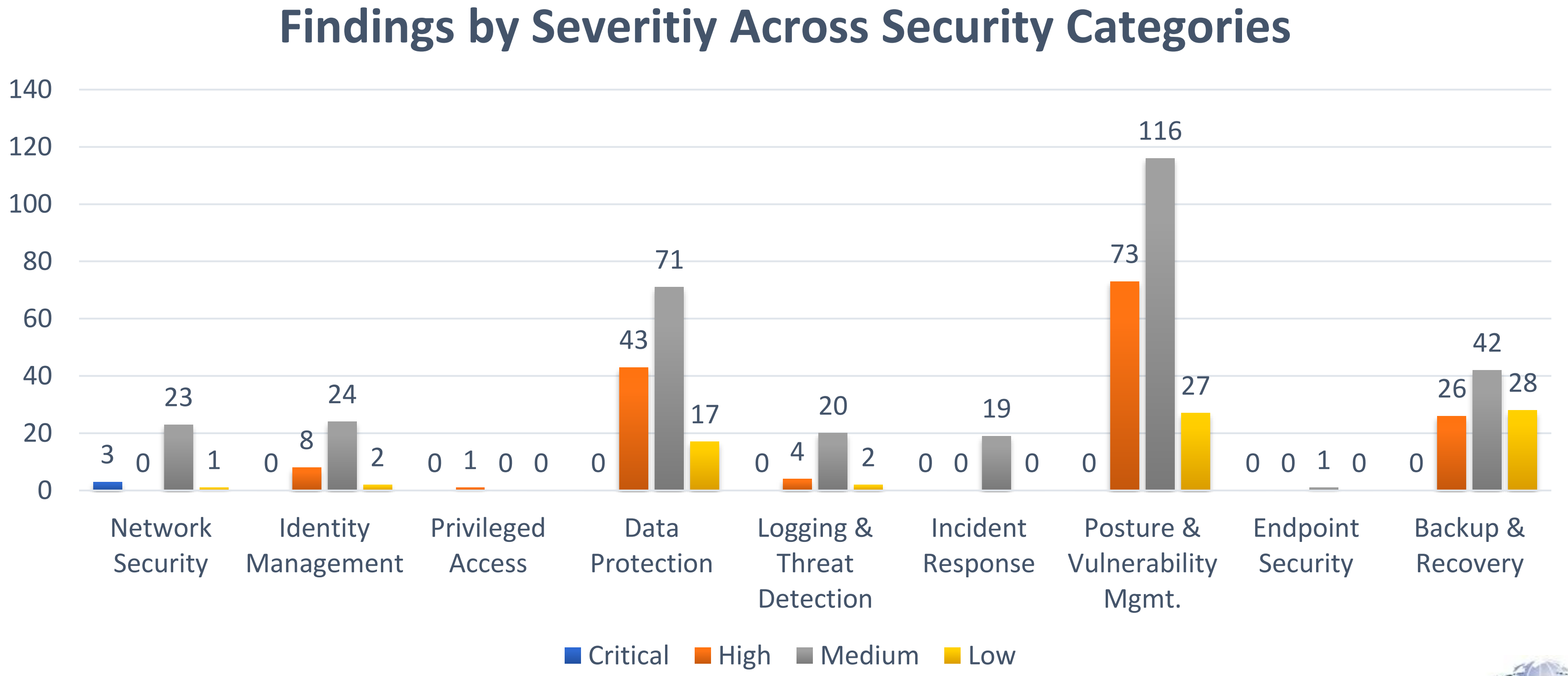
Upgrade to new Defender CSPM plan

Workload protections

Inventory

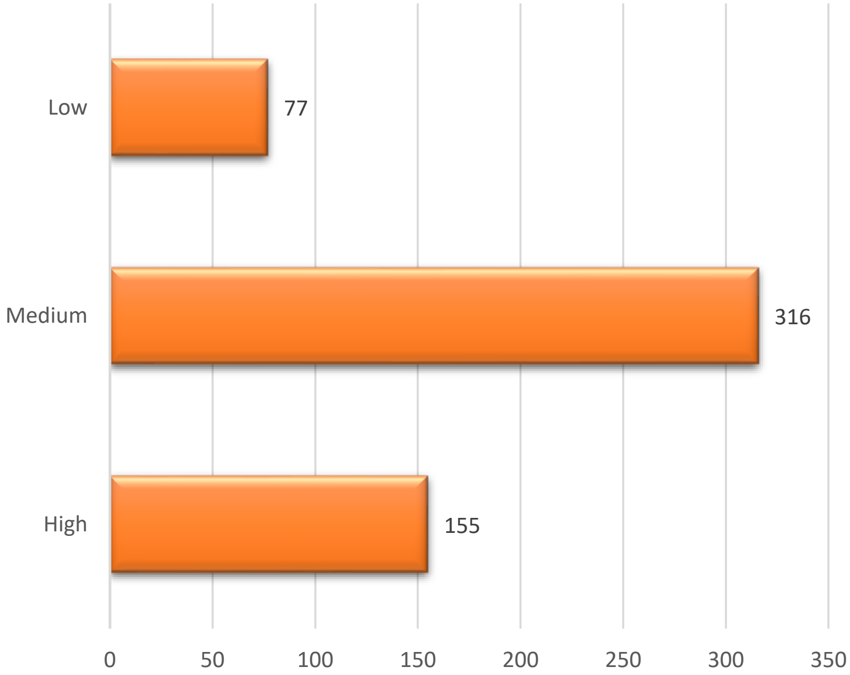
Total Resources

Findings by Severity Across Categories

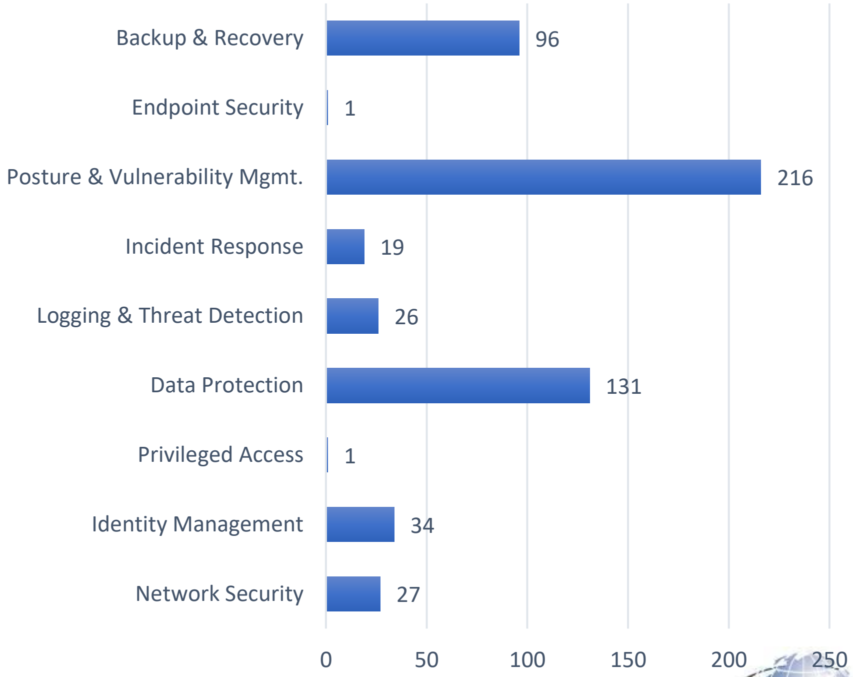


Severity Risks Findings

Total Number of Findings



Total Number of Findings By Category



Key Findings

(High Severity 🔴)

These are the most urgent issues that could put the company at serious risk if left unchecked:

- Some storage accounts allowed **public access** → there is a possibility that anyone on the internet could reach data.
- **MFA not fully enforced** → user accounts more vulnerable to attacks.
- Some Virtual Machines had **no disk encryption** → risk if data is stolen.
- **Key Vault access too wide** → secrets could be reached by more accounts than necessary.

Key Findings

(Medium & Low Severity 🟠 🟢)

- Key Vault **logging not fully enabled** → harder to detect suspicious activity.
- Virtual Machines missing **endpoint protection/antimalware** → risk of malware infection.
- App Services allowed **older TLS versions** → weaker encryption for web traffic.
- Shared accounts/roles had **too many permissions** → not aligned with least privilege.
- Some storage accounts lacked **advanced threat protection** → missing extra monitoring.

Recommendations (Quick Wins – Low Effort)

These fixes are **easy to implement** but have **high security impact**:

- **Enforce MFA** for all users → quick policy change, reduces account takeover risk.
- **Block public access** to storage accounts → configuration update, protects sensitive data.
- **Update TLS to 1.2+** for App Services → small setting change, strengthens encryption.

Recommendations (Medium & High Effort 🚀)

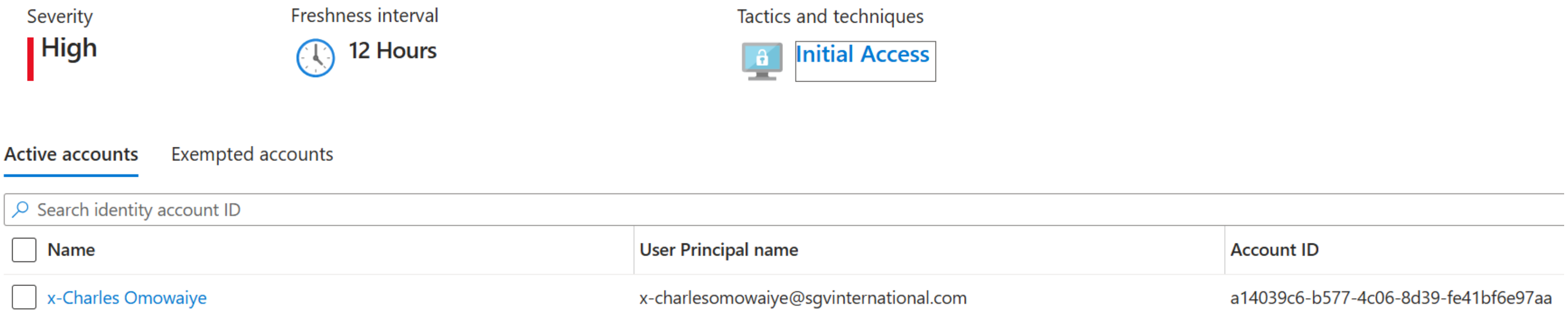
These fixes are **a bit harder to implement**:

- **Medium Effort (planned fixes):**
- Enable **Key Vault logging** → configure diagnostics + storage.
- Add **endpoint protection** on VMs → install + test security agents.
- Restrict **shared account permissions** → assign proper RBAC roles.

- **High Effort (longer-term):**
- Apply **disk encryption** to older VMs → may require downtime/migration.
- Re-architect **NSG rules** → needs planning/testing to avoid outages.

Example Of High Severity – Low Effort

- Disabled accounts with read & write permission on Azure resources should be removed.



Severity
High

Freshness interval
12 Hours

Tactics and techniques
Initial Access

Active accounts Exempted accounts

Search identity account ID

□ Name	User Principal name	Account ID
□ x-Charles Omowaiye	x-charlesomowaiye@sgvinternational.com	a14039c6-b577-4c06-8d39-fe41bf6e97aa

This user is no longer here; we can delete it.

Project Risks

1. Limited Access

- I didn’t have full access to every production system.
- **Why it’s a risk:** Some problems could have been hidden since I couldn’t check everything directly.
- **How I handled it:** I used test/staging environments to safely review settings without touching live systems.

2. Incomplete Inventory

- Azure has many resources spread across different areas.
- **Why it’s a risk:** If something was missed, it might stay unsecured.
- **How I handled it:** I used Defender for Cloud and Azure Resource Graph to make sure I found as many resources as possible.

3. Time Constraints

- The project lasted only 10 weeks.
- **Why it’s a risk:** There wasn’t enough time to fix every single problem.
- **How I handled it:** I focused on creating a clear report with recommendations so the team can take action later.

Lessons Learned

RIGHT TOOLS HELP UNCOVER HIDDEN ISSUES

PRIORITIZATION IS KEY (FOCUS ON BIGGEST RISKS FIRST)

CLEAR COMMUNICATION MAKES FINDINGS ACTIONABLE

TIME LIMITS MEAN FOCUS ON QUICK WINS

COLLABORATION IMPROVES OVERALL RESULTS

Thank You!