

Richard M. Okhai

# Technical Portfolio

Cybersecurity | Data Science | Technology & Engineering

# Table of Content

Summary .....	3
Domain 1: Cybersecurity .....	4
Subdomain 1: Incident Response and Malware Forensics .....	5
Subdomain 2: Process Automation – Cybersecurity .....	13
Domain 2: Data Science – Competitive Intelligence .....	16
Subdomain 1: Market Prediction – Supply Chain .....	17
Domain 3: KeyVault (In Development) .....	21
Subdomain 1: Save Credentials .....	22
Subdomain 2: Retrieve Credentials .....	23
Subdomain 3: Generate Credentials .....	24
Domain 4: Cloud Integration .....	25
Appendix .....	30

# Summary

Sourcing and utilizing systems data in cybersecurity is becoming more popular as technology grows to become more sophisticated.

With modernization of security solutions, enhanced with powerful capabilities to draw an in-depth mathematical analysis of a security event with KPI's to gauge the effectiveness of the overall process for continuous and proactive security hygiene.

This portfolio has been designed to outline similar process with homegrown program written in Python and some sample dataset:

## Threat Hunt and Malware Analysis: “Homegrown Python Program”

- Dataset: Firewall and proxy block event report.
- Objective: Combating persistent common ICT threats on managed host.
- Solution: Detective/investigative control process.

## Process Automation – Host Discovery Scan and Risk Assessment

- Dataset: Quarterly scan results of network boundary.
- Objective: Risk assessment for host with misconfiguration and open ports.
- Solution: Technical/administrative control process.

## Competitive Intelligence – Supply Chain & Program Modernization

- Dataset: Kaggle.
- Objective: Supply chain product for sales prediction.
- Solution: Sales prediction program.

# Domain 1: Cybersecurity/Information Security

- Incident Response and Malware Analysis:
  - Threat-Hunt Tool:
    - Scenario: Detect & respond to a phishing attack.
    - Action Plan: Correlate a persistent “Blocked” traffic of a security event on a known endpoint.
    - Validation: Utilize global threat intelligence | Utilize KPI to preview malware event overtime.
    - Continuous Monitoring: Preview news update artifacts for news article pertaining to IOC.
- Process Automation – Cybersecurity:
  - Host Discovery Scan and Risk Assessment Tool:
    - Scenario: OS fingerprint and vulnerable port identification.
    - Action Plan: NMAP scan of network boundary.
    - Continuous Monitoring: Dashboard of quarterly risk overview.



# 1.0: Incident Response & Malware Forensics

```
[Threat Hunt - Detection and Analysis]

User Interactive Mode

Quick Hunt Category:

[0]: Threat Event Correlation Database ← Detect
[1]: Detection Over 90 Days by Malware Category
[2]: Top 5 Most-Recent Detection by Malware Category
[3]: Global Threat Hunt (i.e. Common ICT Threats)
[4]: Global URL Verdict (i.e. Threat Intelligence Info Gathering) ↓
[5]: IOC Data Retention
[6]: Image Forensics (i.e. JPG, PNG)
[7]: Threat Event Dashboard ← Malware event overtime - KPI
[8]: Cybersecurity News Artifacts ↑ Artifacts from news article

Enter ':q' to quit

Select Category (e.g., 0) or ':q' to terminate session: |
```

**Objective:** Daily proxy report shows a persistent threat on a host from a previous security event from a firewall detection.

**IOC Retained:** IP Address & URL.

# 1.1: Incident Response & Malware Forensics

```
User Interactive Mode

Quick Hunt Category:
[0]: Threat Event Correlation Database ← IOC Correlation from Proxy Event
[1]: Detection Over 90 Days by Malware Category
[2]: Top 5 Most-Recent Detection by Malware Category
[3]: Global Threat Hunt (i.e. Common ICT Threats)
[4]: Global URL Verdict (i.e. Threat Intelligence Info Gathering)
[5]: IOC Data Retention
[6]: Image Forensics (i.e. JPG, PNG)
[7]: Threat Event Dashboard
[8]: Cybersecurity News Artifacts

Enter ':q' to quit

Select Category (e.g., 0) or ':q' to terminate session: 0

IOC Database Tailored to Threat-Hunt Process for diverse use-case.
Information Contained is retained in Database.
Dataset include but not limited to:
- Proxy Event Report.
- Email Threat Detection Report
- Firewall Sinkhole Report
Enter IOC Value to lookup in Database (e.g., email@secureline.com): https://www.polyfill.io/
You have hit a match ← IOC Match found with similar IOC with 20 offense count

IOC_Type          IOC_Value Date_Detected      Description Severity_Level Offense_Count
Malware_Category URL   2024-02-17    Blocked proxy event     Medium           20
CnC              https://www.polyfill.io/
```

- **Action Plan** – Correlate IOC from proxy with IOC Database for previous event detected.
  - **Provided IOC:** URL.
  - **Provided Source:** Proxy Daily Report.

# 1.2: Incident Response & Malware Forensics

```
Quick Hunt Category:  
[0]: Threat Event Correlation Database ← IOC correlation with IP from proxy event  
[1]: Detection Over 90 Days by Malware Category  
[2]: Top 5 Most-Recent Detection by Malware Category  
[3]: Global Threat Hunt (i.e. Common ICT Threats)  
[4]: Global URL Verdict (i.e. Threat Intelligence Info Gathering)  
[5]: IOC Data Retention  
[6]: Image Forensics (i.e. JPG, PNG)  
[7]: Threat Event Dashboard  
[8]: Cybersecurity News Artifacts  
  
Enter ':q' to quit  
  
Select Category (e.g., 0) or ':q' to terminate session: 0  
  
IOC Database Tailored to Threat-Hunt Process for diverse use-case.  
Information Contained is retained in Database.  
Dataset include but not limited to:  
- Proxy Event Report.  
- Email Threat Detection Report  
- Firewall Sinkhole Report  
Enter IOC Value to lookup in Database (e.g., email@secureline.com): 10.30.4.1 ← IOC Value  
  
You have hit a match | Match criteria from a CnC event from a firewall report on 02/17  
  
Malware_Category      IOC_Type    IOC_Value        Date_Detected   Description  Severity_Level  Offense_Count  
CnC                  IP Address  10.30.4.1  2024-02-17 00:00:00  CNC Detection  Critical           5
```

- **Further Action Plan:**  
Correlation of destination IP address from proxy event with IOC Database.
- **IOC Type:** IP address

# 1.3: Incident Response & Malware Forensics

```
PS C:\Users\Richard Mahmud Okhai\Desktop\Cybersecurity & Data Science\Personal Capstone\Threat Hunt>
[Threat Hunt - Detection and Analysis]

User Interactive Mode

Quick Hunt Category:
[0]: Threat Event Correlation Database
[1]: Detection Over 90 Days by Malware Category
[2]: Top 5 Most-Recent Detection by Malware Category
[3]: Global Threat Hunt (i.e. Common ICT Threats)
[4]: Global URL Verdict (i.e. Threat Intelligence Info Gathering)
[5]: IOC Data Retention
[6]: Image Forensics (i.e. JPG, PNG)
[7]: Threat Event Dashboard
[8]: Cybersecurity News Artifacts

Enter ':q' to quit

Select Category (e.g., 0) or ':q' to terminate session: 4 ← Quick Hunt Category Selected
Please enter the URL to scan: https://www.polyfill.io/ ← URL/IOC Scanned
Boolean expression: False equals to No
"URL is not clean"
Viruses Found Website Response Code Threat Type
Clean Verdict None ← according to response code 0 UnableToConnect
False
```

**Verdict:** After analyzing the PCAP data. It was seen in most host running an obsolete version of Mozilla Firefox with the JS Framework embedded into these versions of Mozilla Firefox(s).

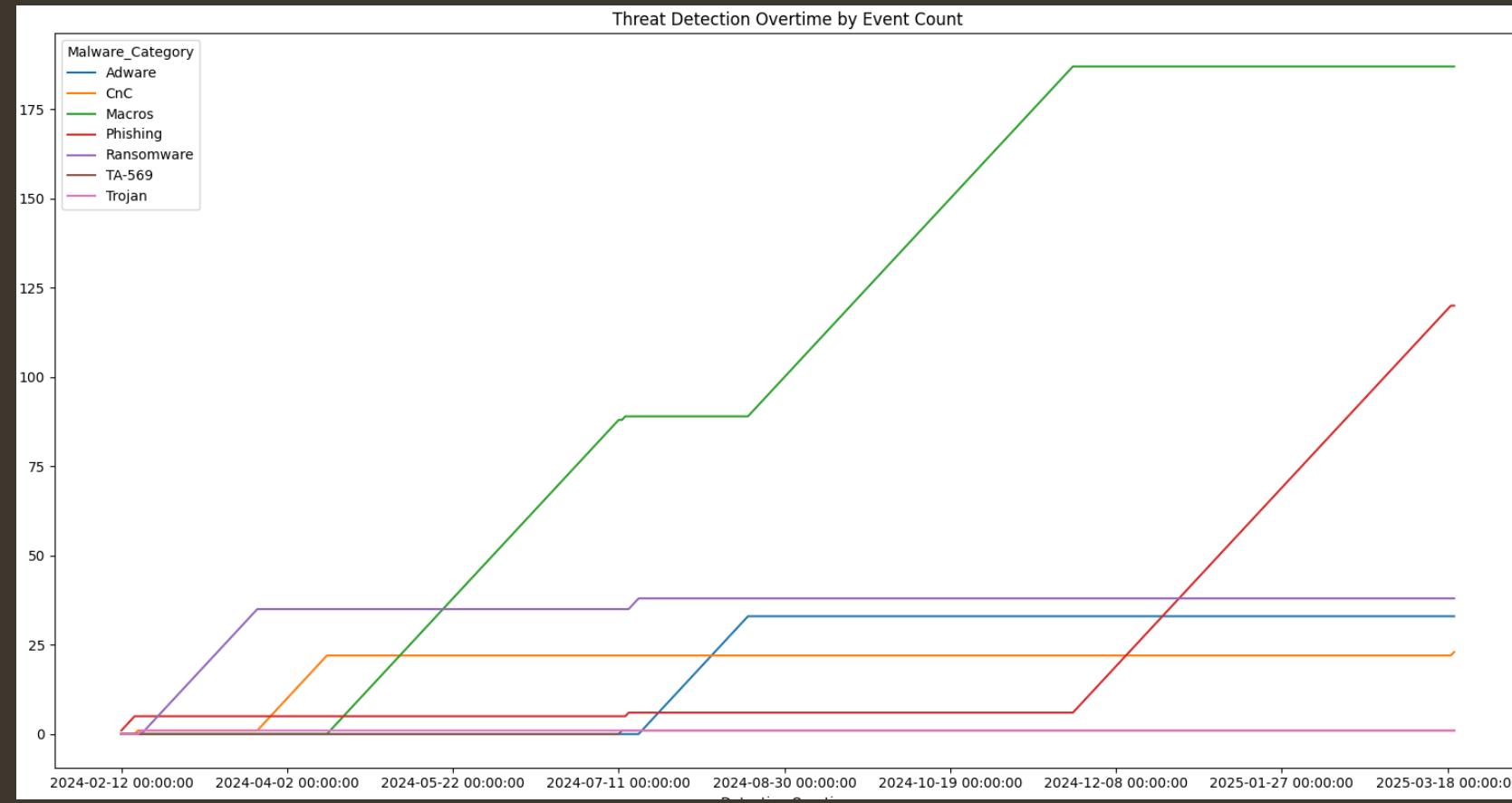
**Correlation with Global Threat Intelligence:** Shows result as False (Clean? "No").

# 1.4: Incident Response & Malware Forensics

- Dashboard Report Analysis: Top 10 Detection Overview | Event Correlation: None existent.

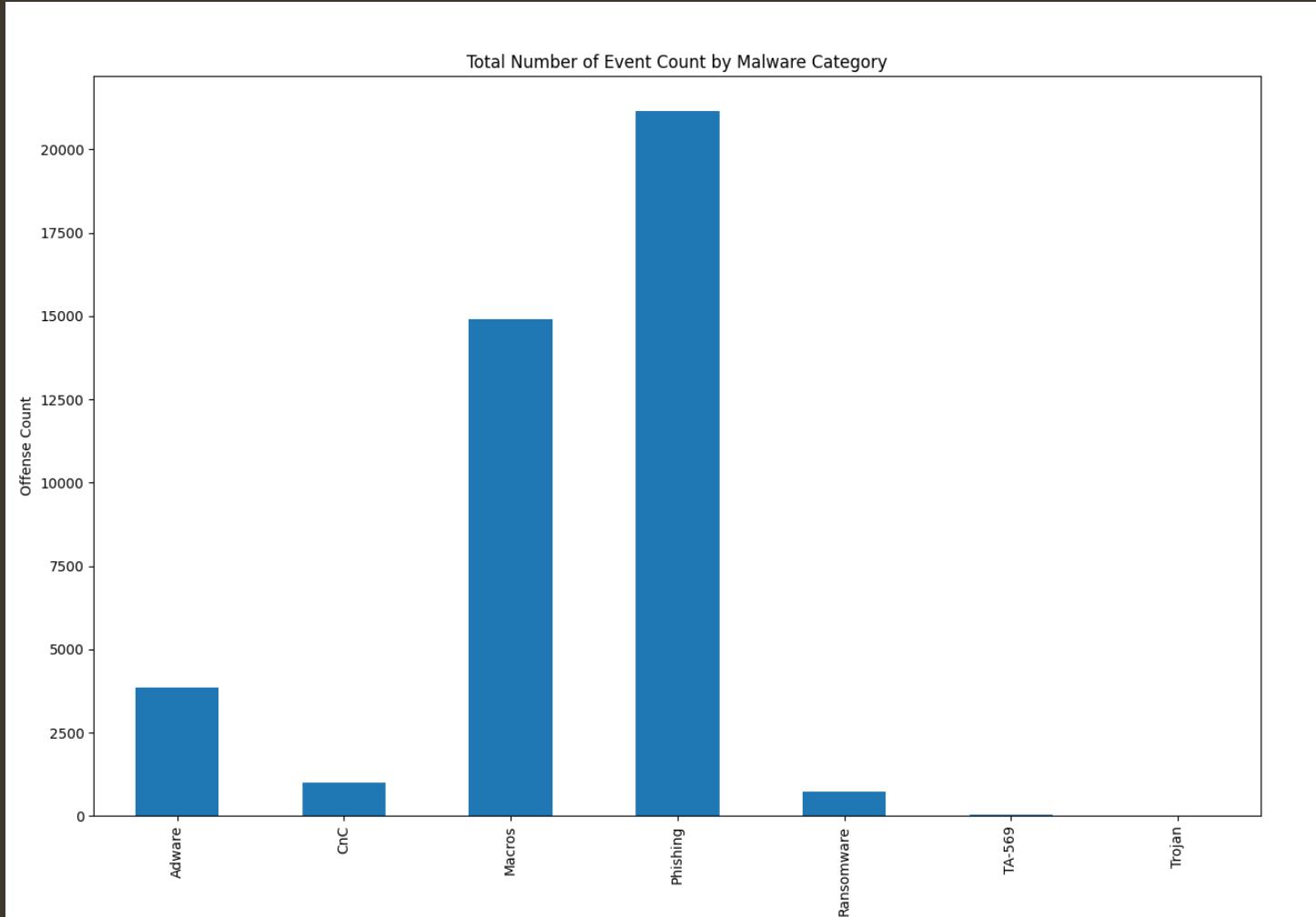
Threat Overview - Top 10 Detection by Event Count							
Malware_Category	IOC_Type	IOC_Value	Date_Detected	Description	Severity_Level	Offense_Count	
Phishing	URL	druknr1.pl	2025-02-11 00:00:00	Known phishing domain	Medium	640	
Phishing	URL	breakthroughenergy.org	2025-02-04 00:00:00	Known phishing domain	Medium	640	
Phishing	URL	shellbefehle.de	2025-01-18 00:00:00	Known phishing domain	Medium	640	
Phishing	URL	linius.com	2025-01-11 00:00:00	Known phishing domain	Medium	640	
Phishing	URL	pharmacie-hanbury.voila.net	2024-12-25 00:00:00	Known phishing domain	Medium	640	
Phishing	URL	prep.ac.th/	2024-12-18 00:00:00	Known phishing domain	Medium	640	
Phishing	URL	akopos.lt	2024-12-01 00:00:00	Known phishing domain	Medium	640	
Phishing	URL	picayunekatrina.blogspot.com/	2025-01-31 00:00:00	Known phishing domain	Medium	576	
Phishing	URL	jimmowrer.net	2025-01-30 00:00:00	Known phishing domain	Medium	576	
Phishing	URL	ec2-3-8-141-80.eu-west-2.compute.amazonaws.com	2025-01-29 00:00:00	Known phishing domain	Medium	576	

# 1.5: Incident Response & Malware Forensics



- **Dashboard Report Analysis:** Threat Detection Assessment Overtime by Event Count.

# 1.5: Incident Response & Malware Forensics



- **Dashboard Report Analysis:** Total Number of Event Count by Malware Category.

# 1.6: Incident Response & Malware Forensics

- **Continuous Monitoring:** News Article Correlation to Help Event Verdict

Select Category (e.g., 0) or ':q' to terminate session: 8					
Provide Newsfeed Category to review: ['Phishing email', 'Cyber breach', 'Ransomware', 'Cybersecurity', 'Social Engineering']					
Newsfeed Category:Phishing email					
<hr/>					
<b>Source</b>					
The New York Times	A new book by Scott J. Shapiro, a law and phil...	Don't let the adorable title fool you: As Scot...	https://www.nytimes.com/2023/05/31/books/revie...		2023-05-31
The New York Times	Young artists say they often receive offers by...	Many young artists survive their early careers...	https://www.nytimes.com/2023/03/17/arts/artist...		2023-03-17
The New York Times	A woman's fiancé wants to drag her along. Must...	Rachel writes: My fiancé, Steve, wants me to g...	https://www.nytimes.com/2022/06/23/magazine/ju...		2022-06-23
The New York Times	As pandemic-related scams rise, experts say co...	LONDON — The email from the payroll department...	https://www.nytimes.com/2021/05/13/world/europ...		2021-05-13
The New York Times	The technology giant also confirmed reports th...	WASHINGTON — Chinese hackers are targeting the...	https://www.nytimes.com/2020/06/04/us/politics...		2020-06-04
The New York Times	"Facebook users understood that they had to gi...	Turning Point: Cambridge Analytica, a politica...	https://www.nytimes.com/2018/12/06/opinion/mag...		2018-12-06
The New York Times	Scammers constantly change their tactics to tr...	Q. I got a message asking me to verify a new D...	https://www.nytimes.com/2017/09/14/technology/...		2017-09-14
The New York Times	The band just completed a 13-show run in New Y...	The Popcast is hosted by Jon Caramanica, a pop...	https://www.nytimes.com/2017/08/11/arts/music/...		2017-08-11
The New York Times	Recipients who clicked on the email and follow...	Google said it was investigating an email scam...	https://www.nytimes.com/2017/05/03/technology/...		2017-05-04
The New York Times	Fake messages claiming to be from Amazon are o...	Q. I got an email from Amazon for something I ...	https://www.nytimes.com/2016/11/29/technology/...		2016-11-29
<hr/>					
<b>References</b>					
Reference Article: <a href="https://www.nytimes.com/2017/09/14/technology/personaltech/spotting-the-phish-in-a-sea-of-email.html">https://www.nytimes.com/2017/09/14/technology/personaltech/spotting-the-phish-in-a-sea-of-email.html</a>					
Reference Article: <a href="https://www.nytimes.com/2021/05/13/world/europe/phishing-test-covid-bonus.html">https://www.nytimes.com/2021/05/13/world/europe/phishing-test-covid-bonus.html</a>					
Reference Article: <a href="https://www.nytimes.com/2016/11/29/technology/personaltech/skip-the-phish-on-the-menu.html">https://www.nytimes.com/2016/11/29/technology/personaltech/skip-the-phish-on-the-menu.html</a>					
Reference Article: <a href="https://www.nytimes.com/2017/05/03/technology/personaltech/email-attack-hits-google-what-to-do-if-you-clicked.html">https://www.nytimes.com/2017/05/03/technology/personaltech/email-attack-hits-google-what-to-do-if-you-clicked.html</a>					
Reference Article: <a href="https://www.nytimes.com/2018/12/06/opinion/maggie-shen-king-the-big-phish.html">https://www.nytimes.com/2018/12/06/opinion/maggie-shen-king-the-big-phish.html</a>					
Reference Article: <a href="https://www.nytimes.com/2017/08/11/arts/music/popcast-phish-bakers-dozen.html">https://www.nytimes.com/2017/08/11/arts/music/popcast-phish-bakers-dozen.html</a>					
Reference Article: <a href="https://www.nytimes.com/2023/05/31/books/review/fancy-bear-goes-phishing-scott-shapiro.html">https://www.nytimes.com/2023/05/31/books/review/fancy-bear-goes-phishing-scott-shapiro.html</a>					
Reference Article: <a href="https://www.nytimes.com/2022/06/23/magazine/judge-john-hodgman-on-phish-shows.html">https://www.nytimes.com/2022/06/23/magazine/judge-john-hodgman-on-phish-shows.html</a>					
Reference Article: <a href="https://www.nytimes.com/2023/03/17/arts/artist-email-scam.html">https://www.nytimes.com/2023/03/17/arts/artist-email-scam.html</a>					
Reference Article: <a href="https://www.nytimes.com/2020/06/04/us/politics/china-joe-biden-hackers.html">https://www.nytimes.com/2020/06/04/us/politics/china-joe-biden-hackers.html</a>					

# 1.7: Process Automation – Cybersecurity

```
PS C:\Users\Richard Mahmud Okhai\Desktop\Cybersecurity & Data Science\Personal Capstone\Host Discovery_Risk Assessment>
Disclaimer Message: The process you are about to initiate requires a formal approval from the Asset Owner.
Initiating this scan without a formal approval is a violation of The U.S. Computer Fraud and Abuse Act.

Active Status ...
2024-07-02 21:03:27.942073

Host Discovery Scan & Risk Assessment

[Selection Category]

0: Network Scan Action Plan: OS Fingerprint and Open Port network scan
1: Dashboard - Network Scan
2: Web Scan/Scrapper
3: Dashboard - Web Scan
4: CISA Vulnerability Catalog

Select Category (e.g., 0) or ':q' to quit: 0

Select Quarter Cycle (e.g., Q1, Q2, Q3, Q4): Q2

Enter IP address or subnet (e.g., 192.168.1.0/24): 192.168.1.59

Enter Nmap scan option [e.g., -sP]: -O

Select Scan Speed [e.g., -T4 for faster scans]: -T4

Running command: nmap -O -T4 192.168.1.59

Scan Completed
Result Saved Successfully.. Scan completed and result retained successfully

Select Category (e.g., 0) or ':q' to quit:
```

- Objective: Host discovery scan and risk assessment.
- Ad-hoc Scan: OS Fingerprint.
  - Risk Assessed:
    - Open Ports.
    - Misconfiguration(s).
    - Vulnerabilities.

# 1.8: Process Automation – Cybersecurity

- **Action Plan:** Assess risk with open port and OS fingerprint information:
  - Discovery/Findings: OS Version & Open Port.
    - Vulnerable Justification: After manual test, some services were discovered to be utilizing default credentials.

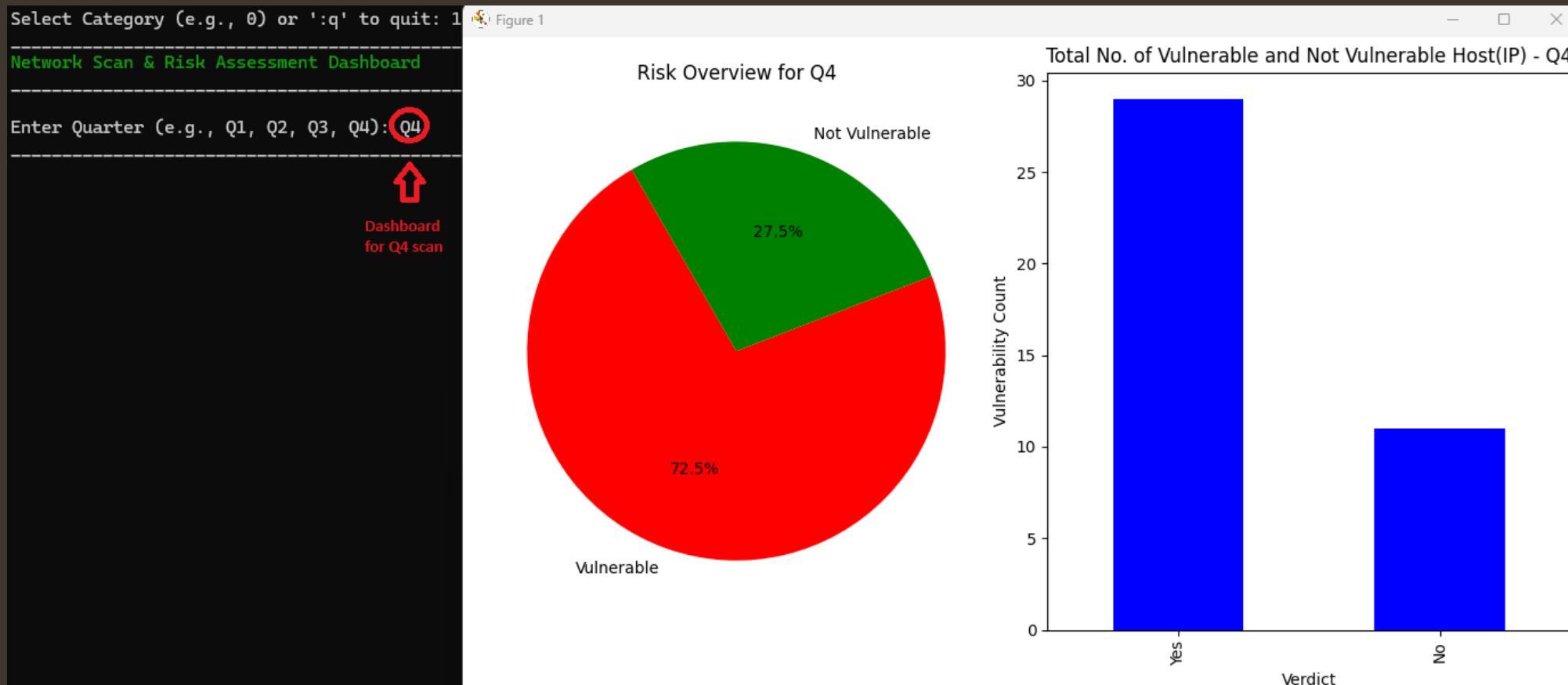
Hostname	OS	Open Ports	Date Scanned	Vulnerable	Not Vulnerable
192.168.1.104	Microsoft Windows 10	135/tcp, 139/tcp, 445/tcp	2024-07-02	Yes	No

Diagram illustrating the flow of data from the scanned host to the report table:

- IP of Host Scanned (192.168.1.104) feeds into the Hostname column.
- OS Version (Microsoft Windows 10) feeds into the OS column.
- Open Ports (135/tcp, 139/tcp, 445/tcp) feeds into the Open Ports column.
- Date Scanned (2024-07-02) feeds into the Date Scanned column.
- The Vulnerable column is determined by a manual test (not shown in the diagram).
- The Not Vulnerable column is also determined by a manual test (not shown in the diagram).

# 1.9: Process Automation – Cybersecurity

- Risk Assessment Dashboard for Process Evaluation:



# Domain 2: Data Science – Competitive Intelligence

- **Data Science:**
  - Objective: Movie App Automation:
    - Business | Use Case: Address customer movie request latency issue.
    - Automation Task: Implement a BOT to retrieve list of movies by search criteria from Movie Database.
    - Resolution: Process/App modernization and API request limit threshold modification.

## 2.3: Movie App Automation

- **Problem:** Reported latency previewing movie genre based on search criteria.
  - Data Science & Security Team Investigated
    - Cause of Action: Security Due Diligence.
      - Justification: API Key blacklisted by third-party web application due to API request.
      - Resolution: Request timeout enacted.
    - Data Science Team
      - Cause of Action: App Modernization.
        - Justification: BOT assistance with new request delay and query limits.
        - Resolution: API data-integration into an automated engine, as a compressed list that provides movie info to viewers based on search criteria.

## 2.4: Movie App Automation - Cybersecurity

- API Security:
  - .ENV Hardcoded into App without revealing API Key to the public.

```
# Set environment variables from the .env in the local environment
load_dotenv()
nyt_api_key = os.getenv("NYT_API_KEY")
tmdb_api_key = os.getenv("TMDB_API_KEY")
type(nyt_api_key)
type(tmdb_api_key)
```

## 2.5: Movie App Automation - Cybersecurity

- Twelve second interval hard-coded into program
  - Twelve seconds delay API Request:

```
response = requests.get(reqst_url)
# Add a twelve second interval between queries to stay within API query limits
time.sleep(12)
# Try and save the reviews to the reviews_list
```

- Request Counter for 50 Requests:

```
#Enumerate method utilized for request counter
for idx, title in enumerate(title_db):
    if idx % 50 == 0 and idx != 0:
        time.sleep(50)
```

# 2.6: Movie App Automation – Data Science

- **Program Modernization:** Bot feature with new request delay.
  - **Movie search, based on keyword and search criteria:**
    - Product Test: Romantic movie search query.

Before:

```
[  
  {  
    "title": "The Attachment Diaries",  
    "genres": [  
      "Drama",  
      "Mystery",  
      "Thriller",  
      "Horror"  
    ],  
    "languages": [  
      "Spanish"  
    ],  
    "countries": [  
      "Argentina"  
    ],  
    "release_date": "2021-10-07",  
    "runtime": 102,  
    "vote_average": 3.0,  
    "vote_count": 4  
  },  
  {  
    "title": "What",  
    "genres": [],  
    "languages": [],  
    "countries": [],  
    ...  
    "vote_average": 6.3,  
    "vote_count": 193  
  }  
]
```

After:

```
Found movie The Attachment Diaries  
Found movie What  
Found movie You Can Live Forever  
Found movie A Tourist  
Found movie Other People  
Found movie One True Loves  
Found movie The Lost Weekend: A Love Story  
Found movie A Thousand and One  
Found movie Your Place or Mine  
Found movie Love in the Time of Fentanyl  
Found movie Pamela, a Love Story  
Found movie In From the Side  
Found movie After Love  
Found movie Alcarràs  
Found movie Nelly & Nadine  
Found movie Lady Chatterley  
Found movie The Sound of Christmas  
Found movie The Inspection  
Found movie Bones and All  
Found movie My Policeman  
Found movie About Fate  
Found movie Waiting for Bojangles  
Found movie I Love My Dad  
Found movie A Love Song  
Found movie Alone Together  
...  
Found movie The Ottoman Lieutenant  
Found movie Love & Taxes  
Found movie Everybody Loves Somebody,  
Found movie Kedi,
```

# Domain 3: KeyVault (In Development)

- **Credential Management:**
  - Objective: Secure/cost effective approach to credential management:
    - Business | Use Case: Approach to Zero Trust Architecture.
    - Automation Task: Application Development.
    - Resolution: Python script | Database (MySQL) | Azure Infrastructure.

## 2.7: Save Credentials

- Credentials Saved in a database table.

```
Active Status: 2025-04-08 07:06:00
-----
Credential Vault
-----
Key Options:
[0]: Retrieve Login Account Credentials
[1]: Save Login Credential
[2]: Generate Password
-----
Enter ':q' to quit
Select Option (e.g., 0) or ':q' to terminate session: 1
-----
Enter Website Name (or ':q' to quit): www.gmail.com
Enter Username (or ':q' to quit): tomapventures
[Enter Password (or ':q' to quit): *****
Credential Logged
-----
Key Options:
[0]: Retrieve Login Account Credentials
[1]: Save Login Credential
[2]: Generate Password
-----
Enter ':q' to quit
Select Option (e.g., 0) or ':q' to terminate session: ■
```

## 2.8: Retrieve Credentials

- Credential Utilized in next login.

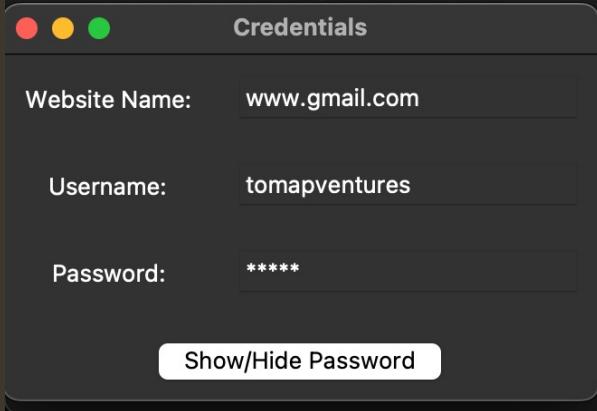
```
Active Status: 2025-04-08 07:08:06

-----
Credential Vault
-----

-----
Key Options:
[0]: Retrieve Login Account Credentials
[1]: Save Login Credential
[2]: Generate Password

Enter ':q' to quit
Select Option (e.g., 0) or ':q' to terminate session: 0

-----
Username: admin
>Password: *****
[Secret Key: *****
Welcome admin
Enter Website Name: www.gmail.com


The screenshot shows a dark-themed application window titled 'Credentials'. It contains three text input fields: 'Website Name' with 'www.gmail.com', 'Username' with 'tmapventures', and 'Password' with '*****'. Below the password field is a 'Show/Hide Password' button. The window has standard OS X-style window controls (red, yellow, green circles).
```

## 2.9: Generate Credentials

- Generate Credentials on a website for future login.

```
Active Status: 2024-07-21 12:12:00
```

```
Credential Vault
```

```
Key Options:
```

```
[0]: Retrieve Login Account Credentials  
[1]: Save Login Credential  
[2]: Generate Password
```

```
Enter ':q' to quit
```

```
Select Option (e.g., 0) or ':q' to terminate session: 2
```

```
Enter length of password (i.e., 7): 10
```

```
Generated Password: q\tgN'seq
```

```
Key Options:
```

```
[0]: Retrieve Login Account Credentials  
[1]: Save Login Credential  
[2]: Generate Password
```

```
Enter ':q' to quit
```

```
Select Option (e.g., 0) or ':q' to terminate session: |
```

# Domain 4: Cloud Integration

- Azure - Infrastructure as a Service | Platform as a Service
- Objective: Web App Implementation
  - **Business|Use Case:** Web accessibility for KeyVault App.
    - **Automation Task:** PowerShell Script – Azure Virtual Machine | Kubernetes Services | Container Registry
    - **Resolution:** Develop and implement a cloud infrastructure for a web application.

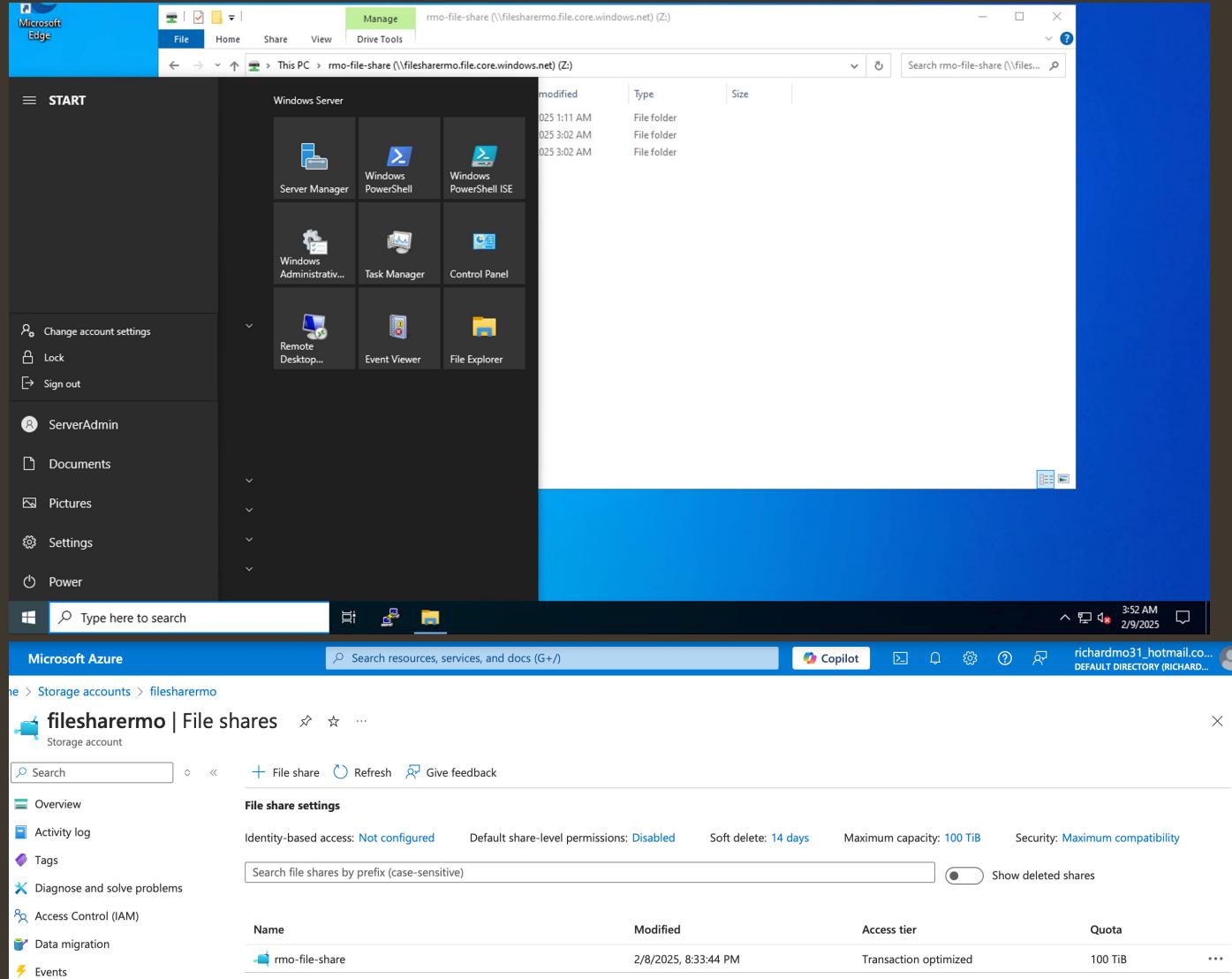
# 3.0: Remote Accessibility – Server Management

- Azure Kubernetes (AKS) Agent Pool – Docker - NGINX in Azure Container Registry (ACR)
- ServerMgmt – Jump server into Web Server and AKS Agent Pool
- Web Server – Data point for website content (Including source code)

The screenshot shows the Microsoft Azure portal interface for managing virtual machines. The top navigation bar includes the Microsoft Azure logo, a search bar, Copilot, and user information. Below the header, the 'Virtual machines' blade is open, showing a list of three VM instances. The table headers are: Name, Subscription, Resource group, Location, Status, Operating system, Size, Public IP address, and Disks. The VM details are as follows:

Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks
aks-agentpool-40532185-0	RichardMO	mc_richardmo_rmoku...	East US	Stopped (deallocated)	Linux	Standard_DS2_v2	-	1
rmoServerMgmt	RichardMO	administrativefunction	East US	Stopped (deallocated)	Windows	Standard_D2s_v3	[REDACTED]	1
rmoWebVM	RichardMO	administrativefunction	East US	Stopped (deallocated)	Windows	Standard_D2s_v3	[REDACTED]	1

# 3.1: File-Share Capability



## - File shared:

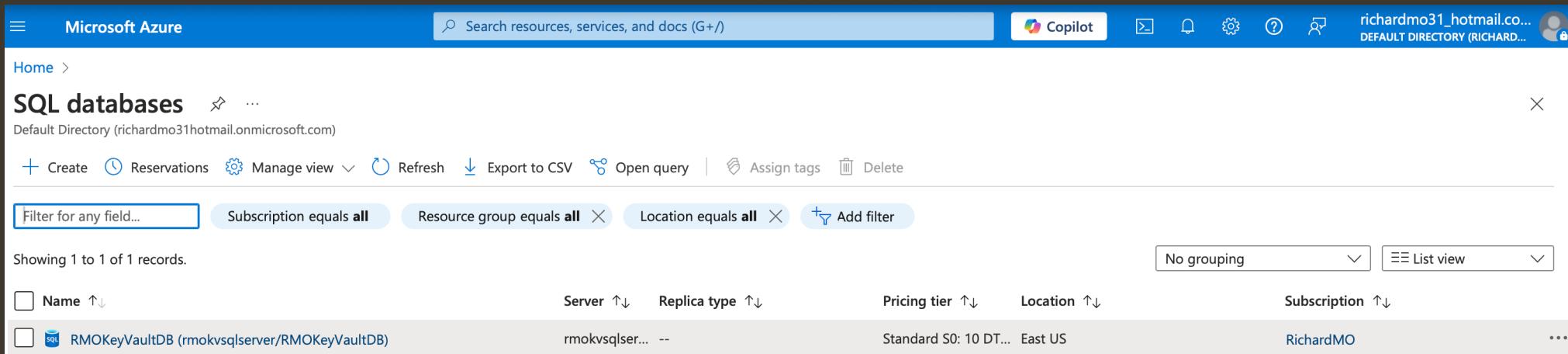
- Development file and codes
- Shared from the local endpoint to AZ VM

## - Connected Endpoint:

- WebVM
- Jump-post

# 3.2: SQL Database & Database Server

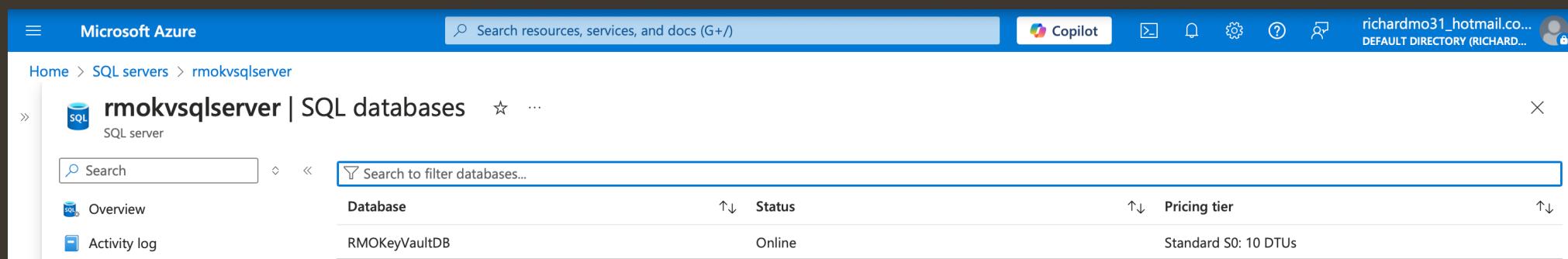
## SQL Database - KeyVault



The screenshot shows the Microsoft Azure portal interface for managing SQL databases. The top navigation bar includes the Microsoft Azure logo, a search bar, Copilot, and user account information. Below the header, the breadcrumb navigation shows 'Home > SQL databases'. The main content area displays a table for 'SQL databases' with one record:

Name	Server	Replica type	Pricing tier	Location	Subscription
RMOKeyVaultDB (rmokvsqlserver/RMOKeyVaultDB)	rmokvsqlser...	--	Standard S0: 10 DT...	East US	RichardMO

## Database Server - KeyVault



The screenshot shows the Microsoft Azure portal interface for managing SQL servers. The top navigation bar includes the Microsoft Azure logo, a search bar, Copilot, and user account information. Below the header, the breadcrumb navigation shows 'Home > SQL servers > rmokvsqlserver'. The main content area displays a table for 'rmokvsqlserver | SQL databases' with one record:

Database	Status	Pricing tier
RMOKeyVaultDB	Online	Standard S0: 10 DTUs

### 3.3: Web/Database Server – ACR | AKS

The terminal window shows the command `kubectl get service nginxexternal` being run, followed by its output:

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP	PORT(S)	AGE
nginxexternal	LoadBalancer	10.0.1.61	52.152.21.129	80:31806/TCP	55s

The browser window displays the Nginx welcome page with the title "Welcome to nginx!" and the message: "If you see this page, the nginx web server is successfully installed and working. Further configuration is required." It also includes links to [nginx.org](http://nginx.org) and [nginx.com](http://nginx.com), and the footer message "Thank you for using nginx."

- Nginx running in a ACR and accessible by an AKS
- Load Balancer for routing
- Server spun up and accessible from an external network with the external IP

# 3.4: Security Control: Microsoft Defender for Cloud

The screenshot shows the Microsoft Defender for Cloud Overview page within the Microsoft Azure portal. The top navigation bar includes the Microsoft Azure logo, a search bar, Copilot, and user information for 'richardmo31@hotmail.co... DEFAULT DIRECTORY (RICHARD...)'. The main content area has a title 'Microsoft Defender for Cloud | Overview' and a subtitle 'Showing subscription 'RichardMO''. A left sidebar under 'General' contains links for Overview, Setup, Recommendations, Attack path analysis, Security alerts, Inventory, Cloud Security Explorer, Workbooks, Community, Diagnose and solve problems, Cloud Security, Security posture, Regulatory compliance, Workload protections, Data security, Firewall Manager, DevOps security, and Management. The main dashboard displays four key metrics: 1 Azure subscriptions, 38 Assessed resources, 1 Attack paths, and -- Security alerts. Below these are sections for 'Security posture' (showing 0 Critical recommendations, 1 Attack paths, and 0/0 Overdue recommendations), 'Environment risk and secure score' (total score 71%, broken down by Azure 71%, AWS, and GCP), and 'Regulatory compliance' (Microsoft cloud security benchmark: 47 of 63 controls passed). On the right side, there are promotional cards for 'Improve code vulnerability analysis with Endor Labs' (describing Endor Labs as a native feature within the Defender for Cloud console) and 'Critical Emerging Vulnerability - PAN-OS (CVE-2024-0012, CVE-2024-9474)' (warning about a critical vulnerability identified in PAN-OS, a commonly used library). There are also links to 'Find impacted VMs', 'Find impacted containers', and 'Read guidance'.

Microsoft Defender  
for Cloud -

- Resources in-scope:
  - Virtual Machines
  - Kubernetes Services
  - Container Registry
  - And Others

# 3.5: Continuous Monitoring – Microsoft Sentinel

The screenshot shows the Microsoft Sentinel Data connectors page. It displays 5 Onboarded Connectors, 2 Connected, and 0 Updates. A search bar, provider filter (Microsoft), data type filter (ThreatIntelligenceIndicator), and status filter (Connected (2)) are present. The table lists two connectors:

Status	Connector name	Content Source	Updates
Connected	Microsoft Defender Threat Intelligence (Preview)	Solution Threat Intelligence	...
Connected	Threat Intelligence Platforms - BEING DEPRECATED (Preview)	Solution Threat Intelligence	...

The screenshot shows the Microsoft Sentinel Analytics page. It displays 0 Active rules. A search bar, rule severity filter (High (1)), and a table of active rules are shown. The table includes columns for Severity, Name, Rule type, Status, Tactics, Techniques, Sub techniques, Source name, and Last modified.

Severity	Name	Rule type	Status	Tactics	Techniques	Sub techniques	Source name	Last modified
High	Advanced Multistage Attack Detection	Fusion	Disabled	Col... +11			Gallery Content	1/27/2025, 8:47...

## Microsoft Sentinel

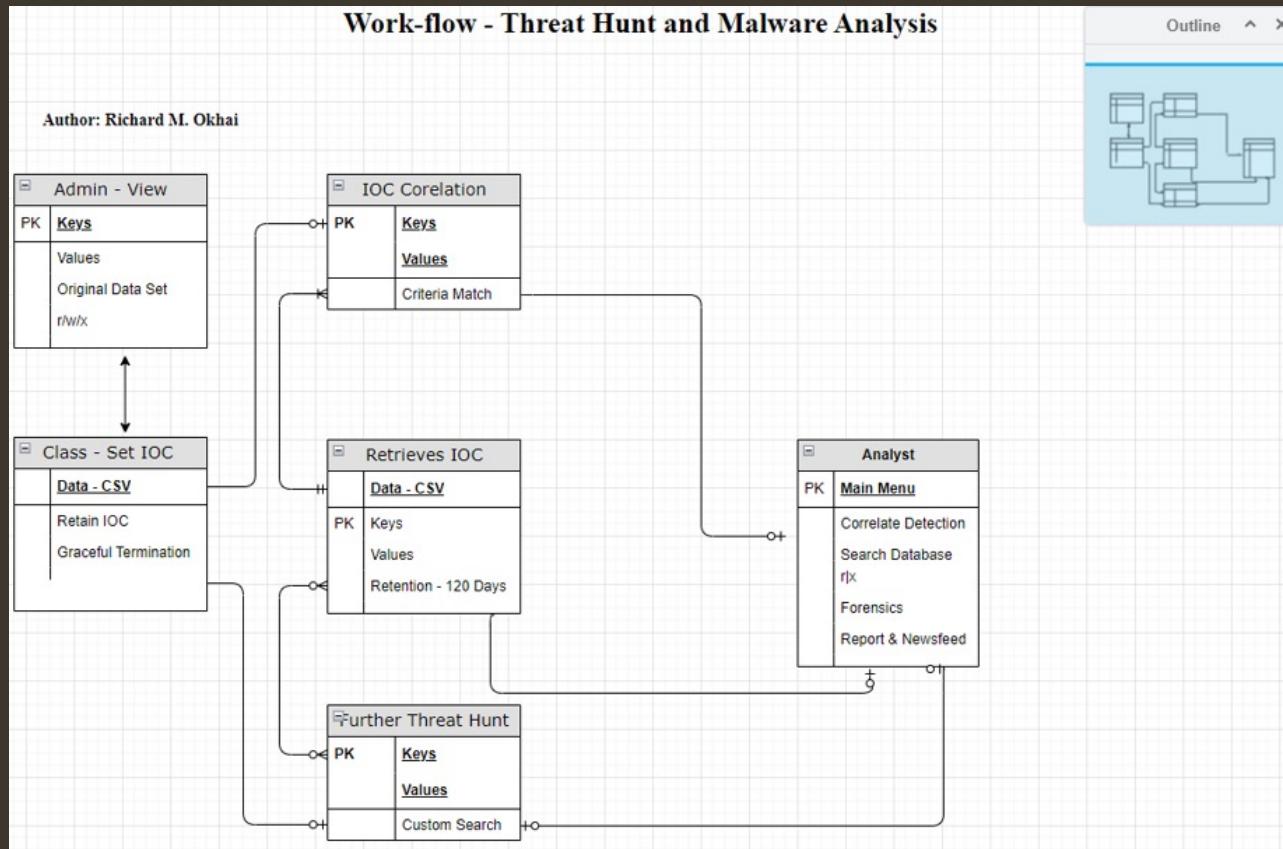
**Log Source:** Data Analytics Workspace

### Connected Log Sources:

- Microsoft Defender Threat Intelligence
- Threat Intelligence Platforms

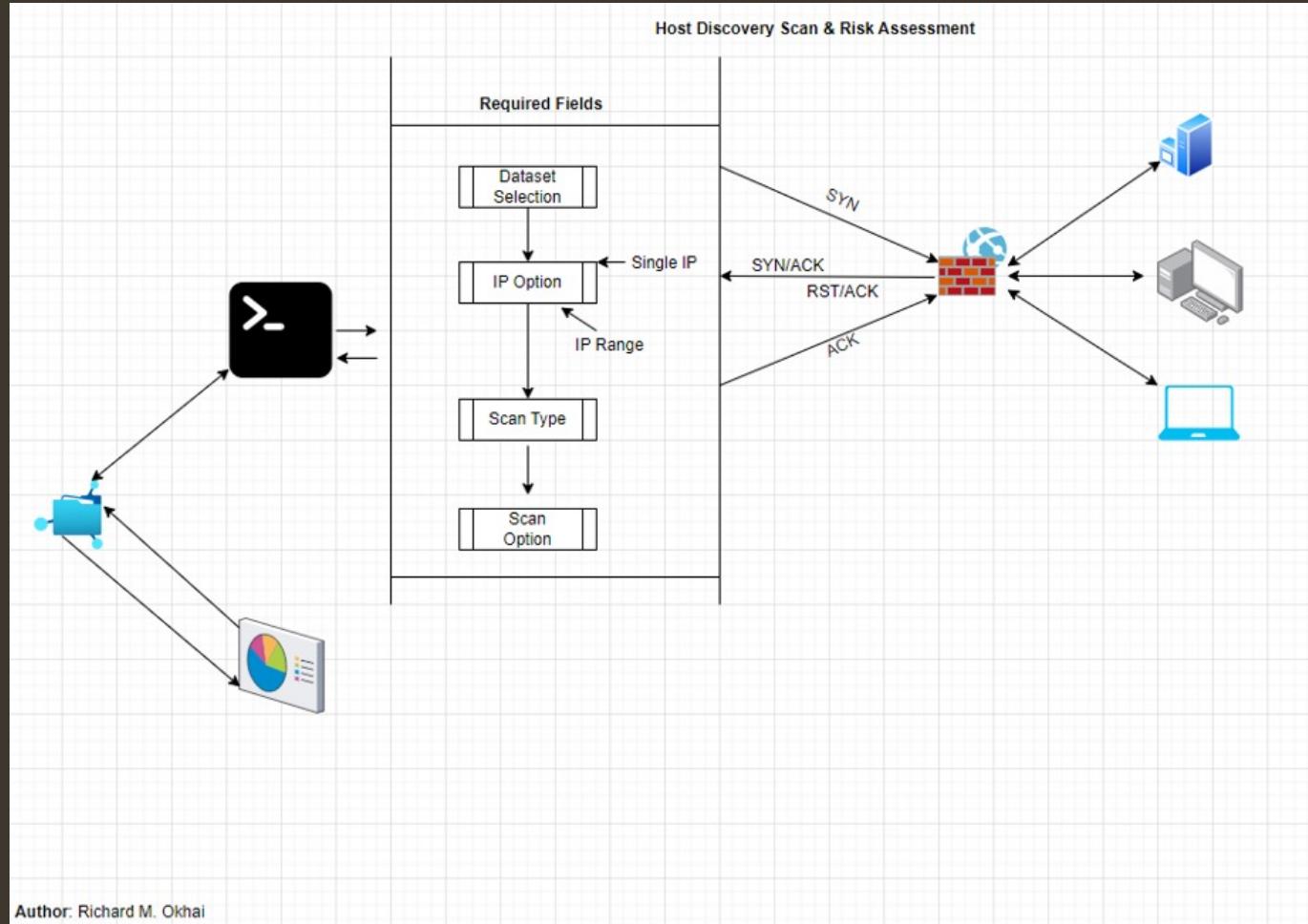
# Appendix

# 1.0: Workflow: Threat-Hunt Tool



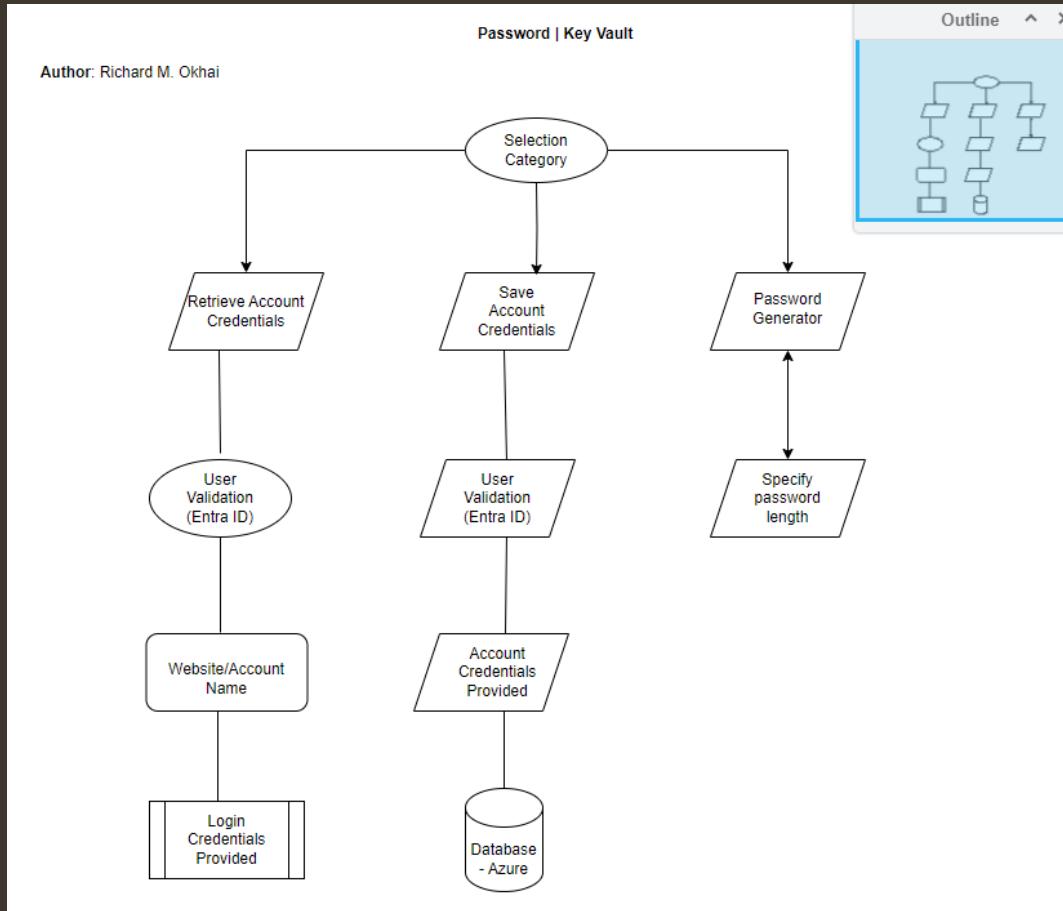
- **Language:** Python
- **Product Type:** Threat-Hunt Tool (Prototype)

# 1.1: Workflow: Host Discovery & Risk Assessment



- **Language:** Python
- **Product Type:** Security Assessment Tool (Prototype)

## 1.2: Workflow: KeyVault



Language: Python  
Product: Credential Management App (In Development)

# 1.3: Network Security Groups for Azure Resources

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

richardmo31@hotmail.co... DEFAULT DIRECTORY (RICHARD...)

Home > Network security groups > rmoNSG

rmoNSG | Inbound security rules

Network security group

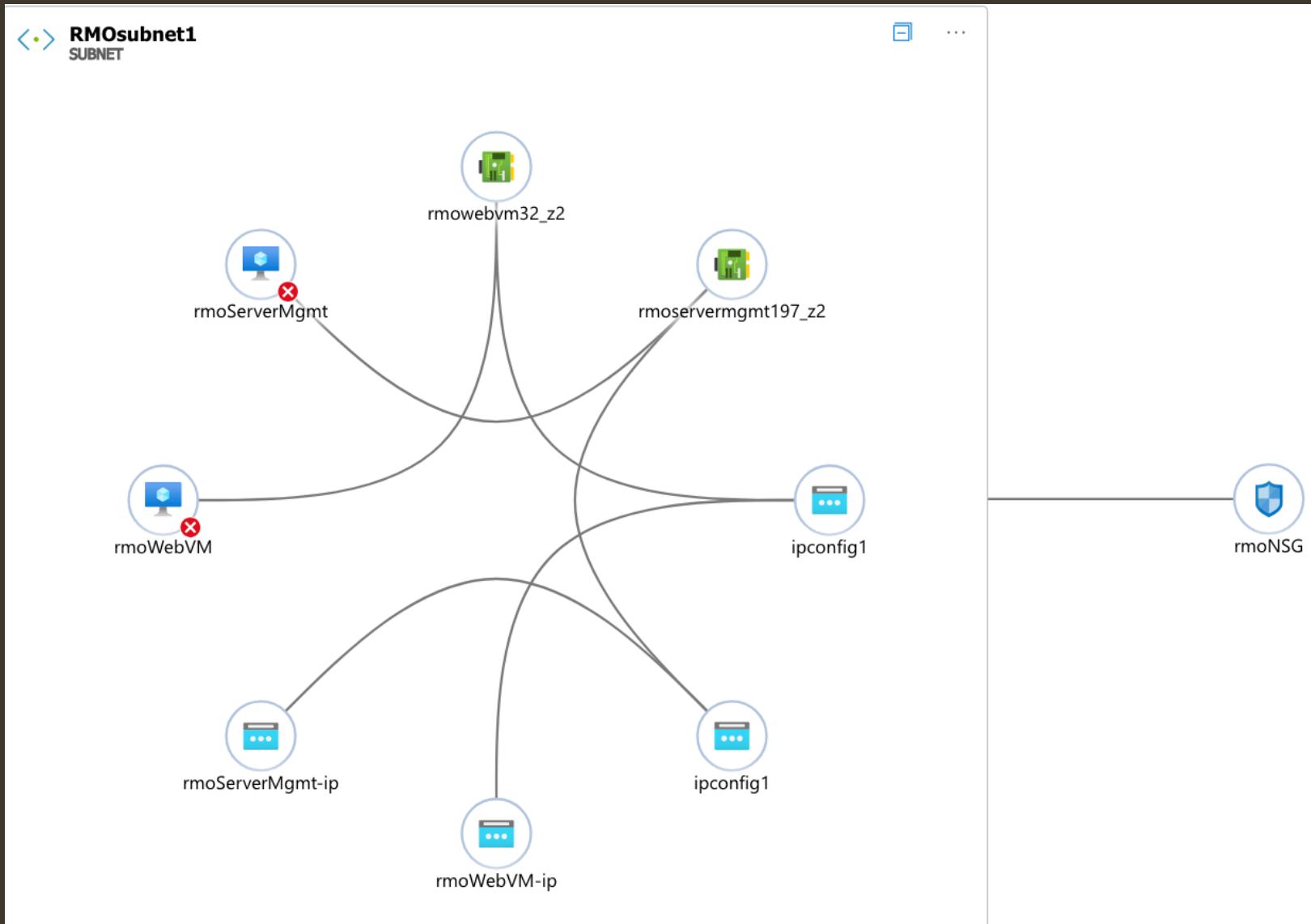
+ Add Hide default rules Refresh Delete Give feedback

Give feedback

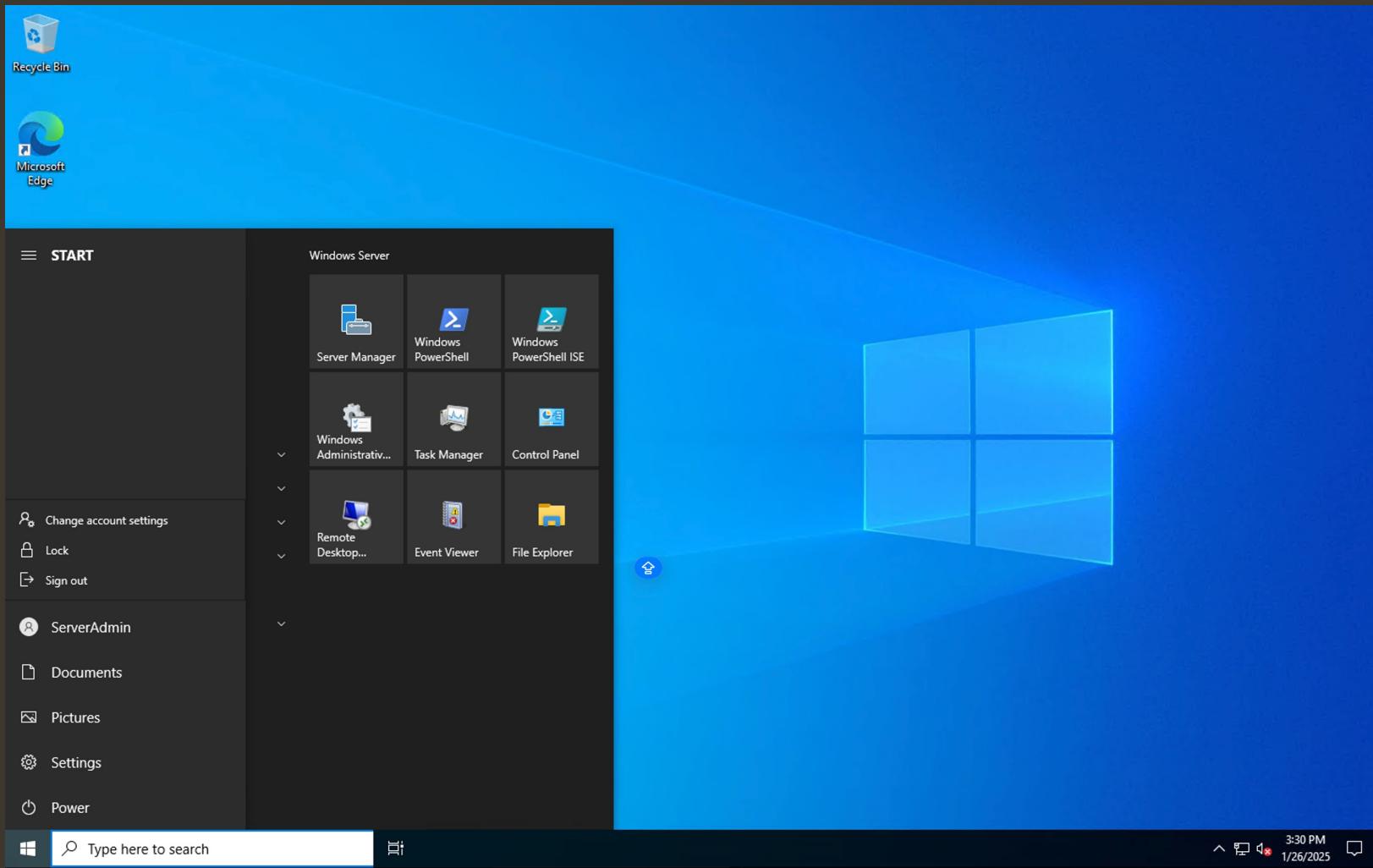
Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Priority ↑	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
100	Allow-Web-All	80,443	TCP	Any	myWebServers	Allow
110	Allow-RDP-All	3389	TCP	[REDACTED]	myMgmtServers	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

# 1.4: Network Architecture – RMO Cloud Instance



# 1.5: Jump-box to Azure Resources



# 1.6: Azure Container Registry



A screenshot of a terminal window with a dark background. The window title bar includes options like "Switch to PowerShell", "Restart", "Manage files", "New session", "Editor", "Web preview", "Settings", and "Help". The main content area displays a JSON object representing an Azure Container Registry. The JSON structure includes fields such as "tier" (set to "Basic"), "status" (null), and "systemData" (containing creation and modification details). The "tags" field is empty, and the "type" is identified as "Microsoft.ContainerRegistry/registries". The "zoneRedundancy" field is set to "Disabled". The command prompt at the bottom shows "richard [ ~ ]\$".

```
"tier": "Basic",
},
"status": null,
"systemData": {
    "createdAt": "2025-01-26T18:02:11.171011+00:00",
    "createdBy": "richardmo31_hotmail.com#EXT#@richardmo31@hotmail.com",
    "createdByType": "User",
    "lastModifiedAt": "2025-01-26T18:02:11.171011+00:00",
    "lastModifiedBy": "richardmo31_hotmail.com#EXT#@richardmo31@hotmail.com",
    "lastModifiedByType": "User"
},
"tags": {},
"type": "Microsoft.ContainerRegistry/registries",
"zoneRedundancy": "Disabled"
}
richard [ ~ ]$
```

# 1.7: Container Build Process

```
Status: Downloaded newer image for nginx:latest
---> 9bea9f2796e2
Successfully built 9bea9f2796e2
Successfully tagged [REDACTED].azurecr.io/sample/nginx:v1
2025/01/26 18:18:58 Successfully executed container: build
2025/01/26 18:18:58 Executing step ID: push. Timeout(sec): 3600, Working directory: '', Network: ''
2025/01/26 18:18:58 Pushing image: [REDACTED].azurecr.io/sample/nginx:v1, attempt 1
The push refers to repository [REDACTED].azurecr.io/sample/nginx]
b57b5eac2941: Preparing
58045dd06e5b: Preparing
541cf9cf006d: Preparing
32c977818204: Preparing
943132143199: Preparing
88ebb510d2fb: Preparing
f5fe472da253: Preparing
88ebb510d2fb: Waiting
f5fe472da253: Waiting
943132143199: Pushed
541cf9cf006d: Pushed
32c977818204: Pushed
58045dd06e5b: Pushed
b57b5eac2941: Pushed
f5fe472da253: Pushed
88ebb510d2fb: Pushed
v1: digest: sha256:e49b2893e997eeda7716bd7f3b2ed60aac69faa4041a4a3b88fb885609703cbb size: 1778
2025/01/26 18:19:06 Successfully pushed image: rmo279248508.azurecr.io/sample/nginx:v1
2025/01/26 18:19:06 Step ID: build marked as successful (elapsed time in seconds: 4.139364)
2025/01/26 18:19:06 Populating digests for step ID: build...
2025/01/26 18:19:07 Successfully populated digests for step ID: build
2025/01/26 18:19:07 Step ID: push marked as successful (elapsed time in seconds: 7.607337)
2025/01/26 18:19:07 The following dependencies were found:
2025/01/26 18:19:07
- image:
    registry: [REDACTED].azurecr.io
    repository: sample/nginx
    tag: v1
    digest: sha256:e49b2893e997eeda7716bd7f3b2ed60aac69faa4041a4a3b88fb885609703cbb
    runtime-dependency:
        registry: registry.hub.docker.com
        repository: library/nginx
        tag: latest
        digest: sha256:0a399eb16751829e1af26fea27b20c3ec28d7ab1fb72182879dcae1cca21206a
    git: {}

Run ID: cal was successful after 15s
richard [ ~ ]$
```

# 1.8: Azure Kubernetes Services - Implementation

```
richard [ ~ ]$ az aks create --name rmoKubernetesCluster --resource-group RichardMO --location eastus --no-ssh-key --node-vm-size Standard_DS2_v2 --nodepool-name agentpool --node-count 1 --vm-set-type AvailabilitySet --network-plugin azure --dns-name-prefix rmoKubernetesCluster-dns
docker_bridge_cidr is not a known attribute of class <class 'azure.mgmt.containerservice.v2024_09_01.models._models_py3.ContainerServiceNetworkProfile'> and will
be ignored
[- Running ..
```

```
richard [ ~ ]$ kubectl apply -f nginxexternal.yaml
deployment.apps/nginxexternal created
service/nginxexternal created
richard [ ~ ]$
```

```
richard [ ~ ]$ az aks get-credentials --resource-group RichardMO --name rmoKubernetesCluster
Merged "rmoKubernetesCluster" as current context in /home/richard/.kube/config
richard [ ~ ]$ kubectl get nodes
NAME           STATUS    ROLES   AGE     VERSION
aks-agentpool-40532185-0   Ready    <none>  5m1s   v1.30.7
richard [ ~ ]$
```

# 1.9: DevOps— Private Network Deployment (Web)

The screenshot shows the Microsoft Azure portal interface. At the top, there's a search bar, a Copilot button, and user profile information. Below the header, the 'Virtual machines' blade is open, showing three records:

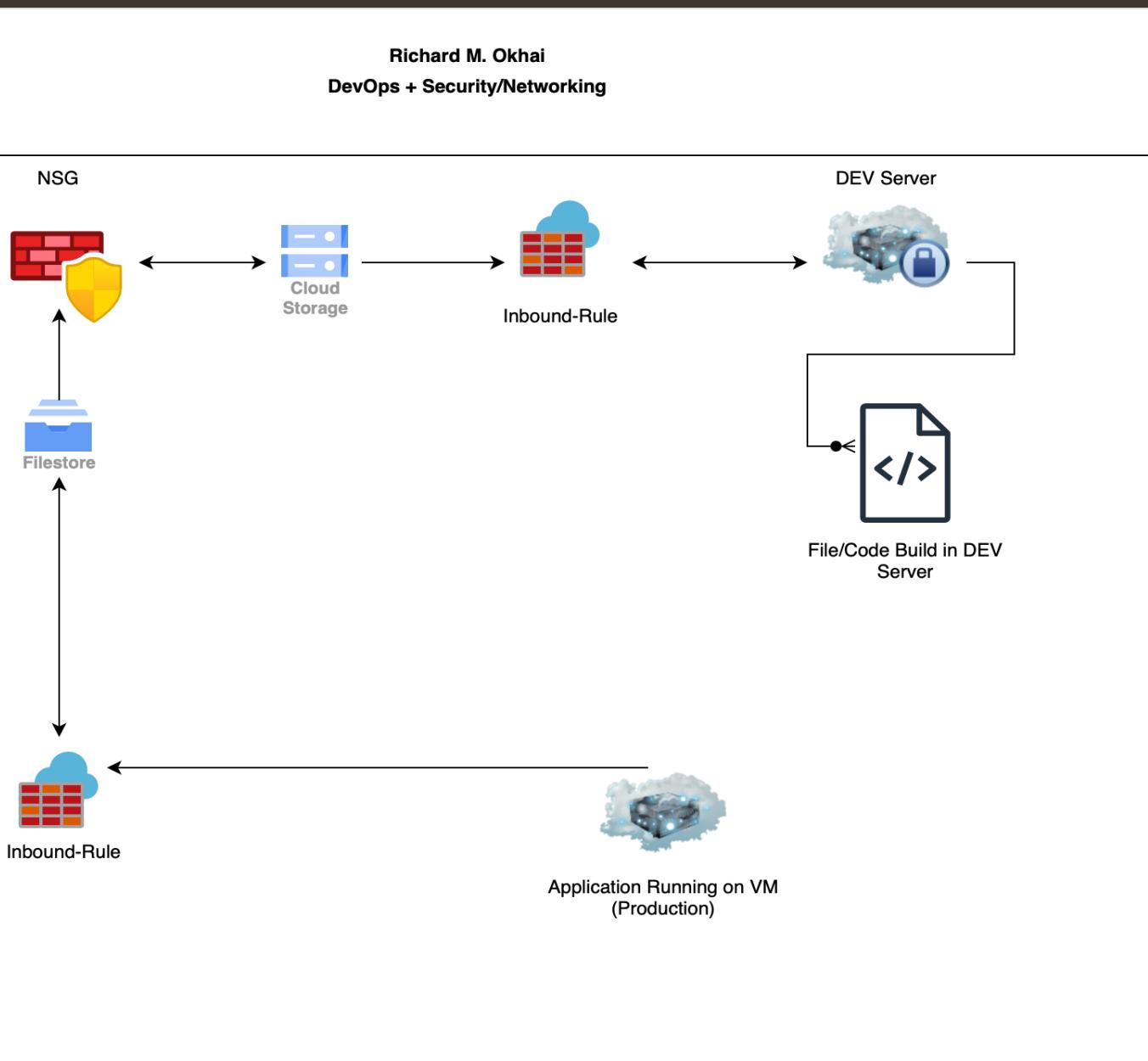
Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disk count
aks-agentpool-40532185-0	RichardMO	MC_RichardMO_rmoK...	East US	Running	Linux	Standard_DS2_v2	-	1
rmoServerMgmt	RichardMO	ADMINISTRATIVEFUN...	East US	Stopped (deallocated)	Windows	Standard_D2s_v3	[REDACTED]	1
rmoWebVM	RichardMO	AdministrativeFunction	East US	Stopped (deallocated)	Windows	Standard_D2s_v3	[REDACTED]	1

Below the table, there are navigation links for 'Page 1 of 1' and a 'Give feedback' link. At the bottom of the page, there's a footer with various icons and a help link.

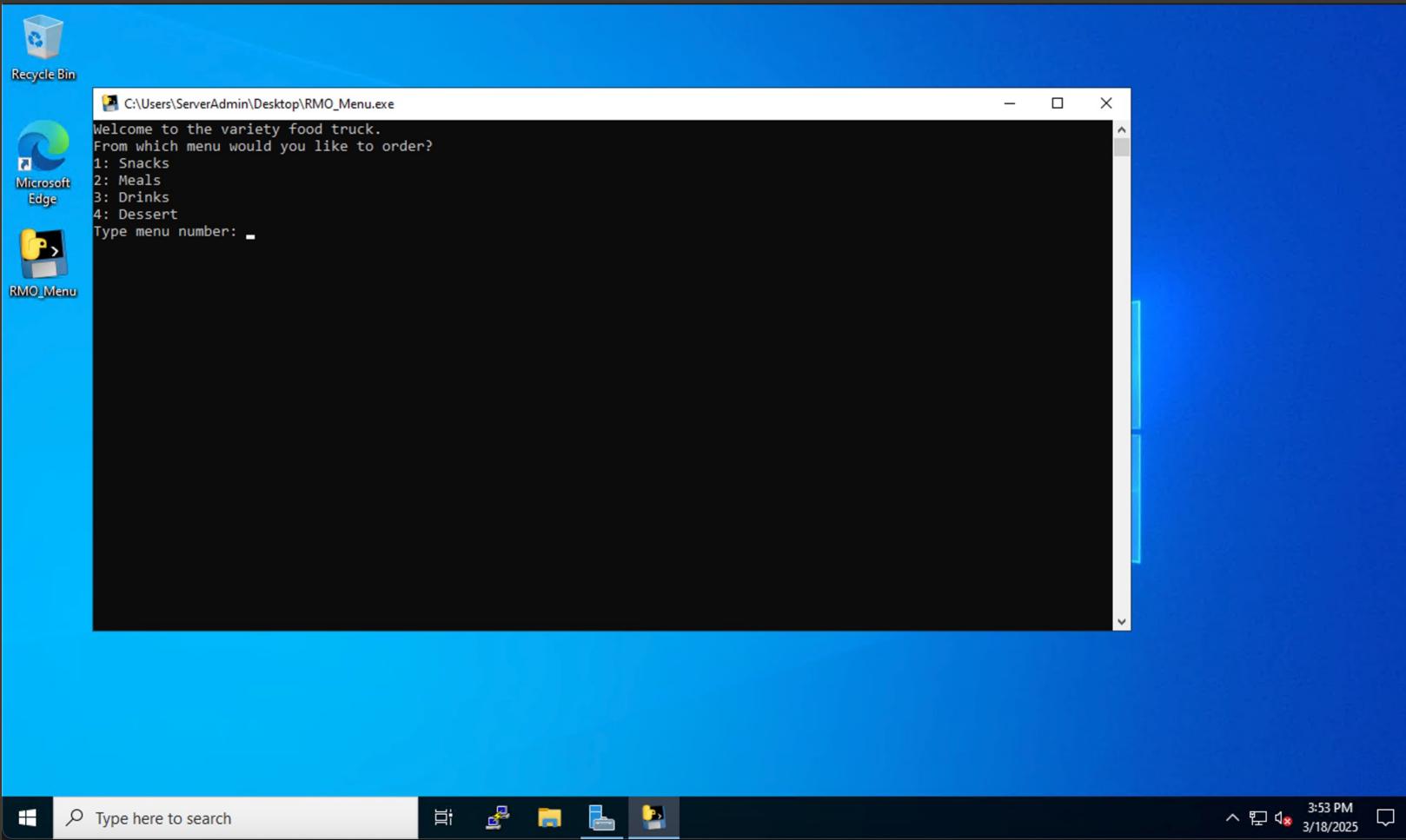
In the bottom right corner, a terminal window is open, showing a command-line session:

```
richard [ ~ ]$ kubectl exec -it nginxexternal-6f98895974-5djbk -- /bin/bash
root@nginxexternal-6f98895974-5djbk:/# curl http://[REDACTED]
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
```

## 2.0: DevOps – Deployment Architecture (Packaged Application)



## 2.1: Packaged Application – Production Endpoint



# 2.2: Endpoint Detection (Microsoft Defender XDR) – Server and AKS

The screenshot shows the Microsoft Defender XDR interface with the 'Device Inventory' page open. The left sidebar includes sections for Home, Exposure management, Investigation & response (Incidents & alerts, Incidents, Alerts), Hunting, Actions & submissions, Partner catalog, Threat intelligence, Assets, Devices, Microsoft Sentinel, Search, Threat management, Content management, and Configuration. The main content area is titled 'Device Inventory' and features a callout for 'Classify critical assets'. It displays a summary of device counts: Total 3, Critical assets 1, High risk 0, High exposure 0, Not onboarded 0, Newly discovered 0. Below this is a table with columns: Name, IP, Criticality level, Device category, Device type, Domain, and Device AAD id. The table lists three devices:

Name	IP	Criticality level	Device category	Device type	Domain	Device AAD id
rmowebvm	10.0.0.4	Medium	Computers and Mo...	Server	Workgroup	
aks-agentpool-40532185-0.ptk...	10.224.0.4	Medium	Computers and Mo...	Server		ptkvovp23bbe3msecv1sjijeh...
rmoservermgmt	10.0.0.5	Medium	Computers and Mo...	Server	Workgroup	

## 2.3: Endpoint Detection – Connection with M.S Sentinel (SIEM)

The screenshot shows the Microsoft Defender XDR interface. On the left, a navigation sidebar lists various modules: Home, Exposure management, Investigation & response, Threat intelligence, Assets, Microsoft Sentinel (which is expanded), Threat management, Content management, Configuration, Endpoints, Email & collaboration, Cases, SOC optimization, Reports, and Learning hub. The main content area is titled "Settings > Microsoft Sentinel" and displays the "Workspaces" section. It prompts the user to "Select the Microsoft Sentinel workspace you'd like to connect to Microsoft Defender XDR." Below this, there are two buttons: "Connect workspace" and "Disconnect workspace". A search bar and a "Filter" button are also present. A table lists the connected workspaces, with one entry shown:

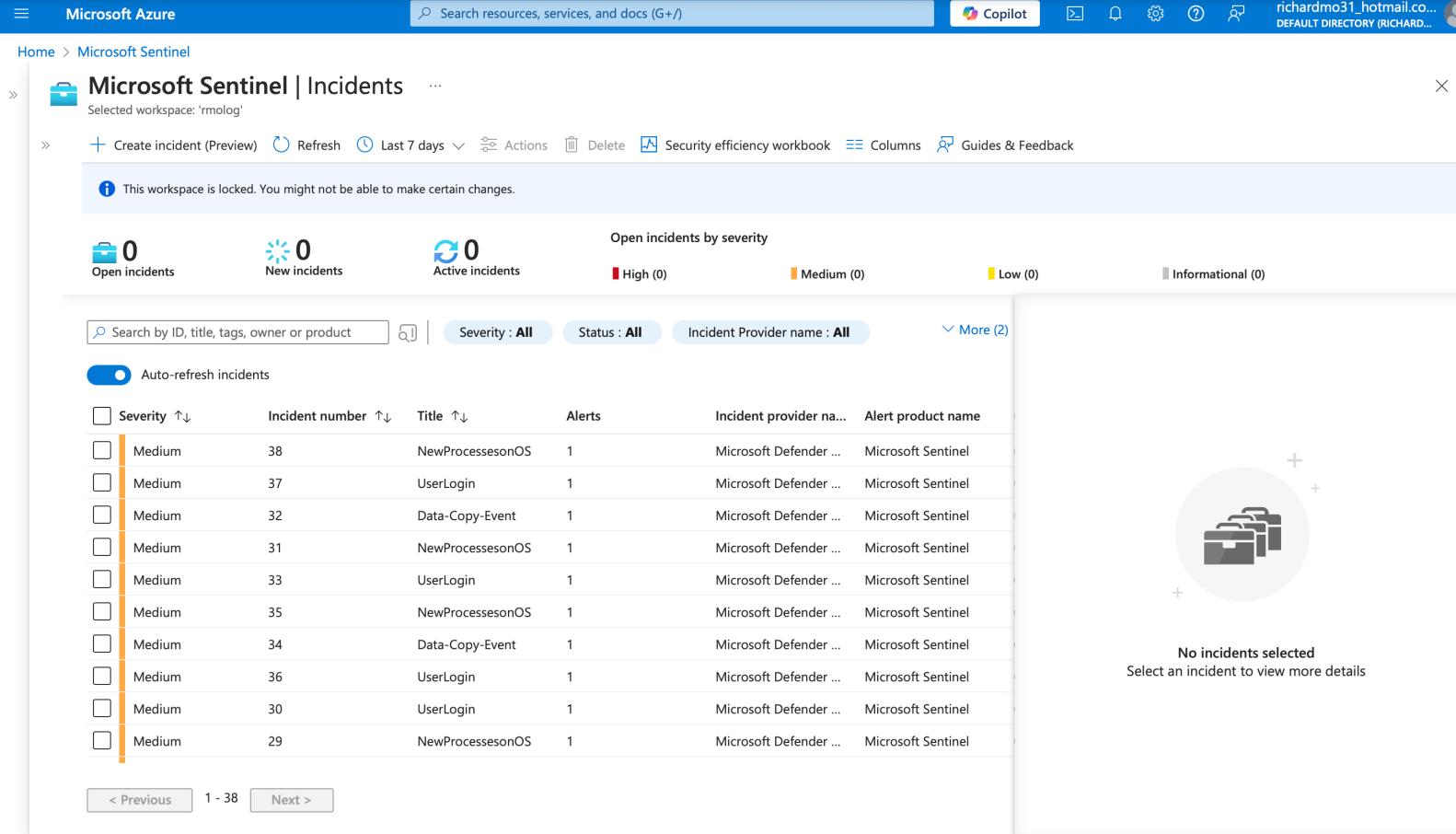
Name	Status	Resource Group	Location	Subscription
rmolog Primary	Connected	administrativefunction	eastus	RichardMO

# 2.4: Endpoint Detection – Escalated Incident (Active Rule)

The screenshot shows the Microsoft Defender XDR interface with the 'Incidents' page selected. The left sidebar includes sections like Home, Exposure management, Investigation & response (Incidents, Alerts), Hunting, Actions & submissions, Partner catalog, Threat intelligence, Assets, Microsoft Sentinel, Search, Threat management, Content management, Configuration, and Endpoints. The main area displays a list of incidents with columns for Incident name, Incident Id, Tags, Severity (Medium), Investigation state (Persistence or Suspicious activity), and Categories. A search bar at the top right allows filtering by name or ID.

Incident name	Incident Id	Tags	Severity	Investigation state	Categories
NewProcessesonOS	121		Medium	Persistence	
UserLogin	120		Medium	Suspicious activity	
Data-Copy-Event	118		Medium	Suspicious activity	
NewProcessesonOS	119		Medium	Persistence	
UserLogin	117		Medium	Suspicious activity	
NewProcessesonOS	115		Medium	Persistence	
UserLogin	114		Medium	Suspicious activity	
Data-Copy-Event	116		Medium	Suspicious activity	

## 2.5: Continuous Monitoring (Endpoints)



The screenshot shows the Microsoft Sentinel Incidents page within the Microsoft Azure portal. The top navigation bar includes 'Microsoft Azure', a search bar, 'Copilot' integration, and user information for 'richardmo31\_hotmail.co... DEFAULT DIRECTORY (RICHARD...)'. The main title is 'Microsoft Sentinel | Incidents' under the 'Home > Microsoft Sentinel' breadcrumb.

Key UI elements include:

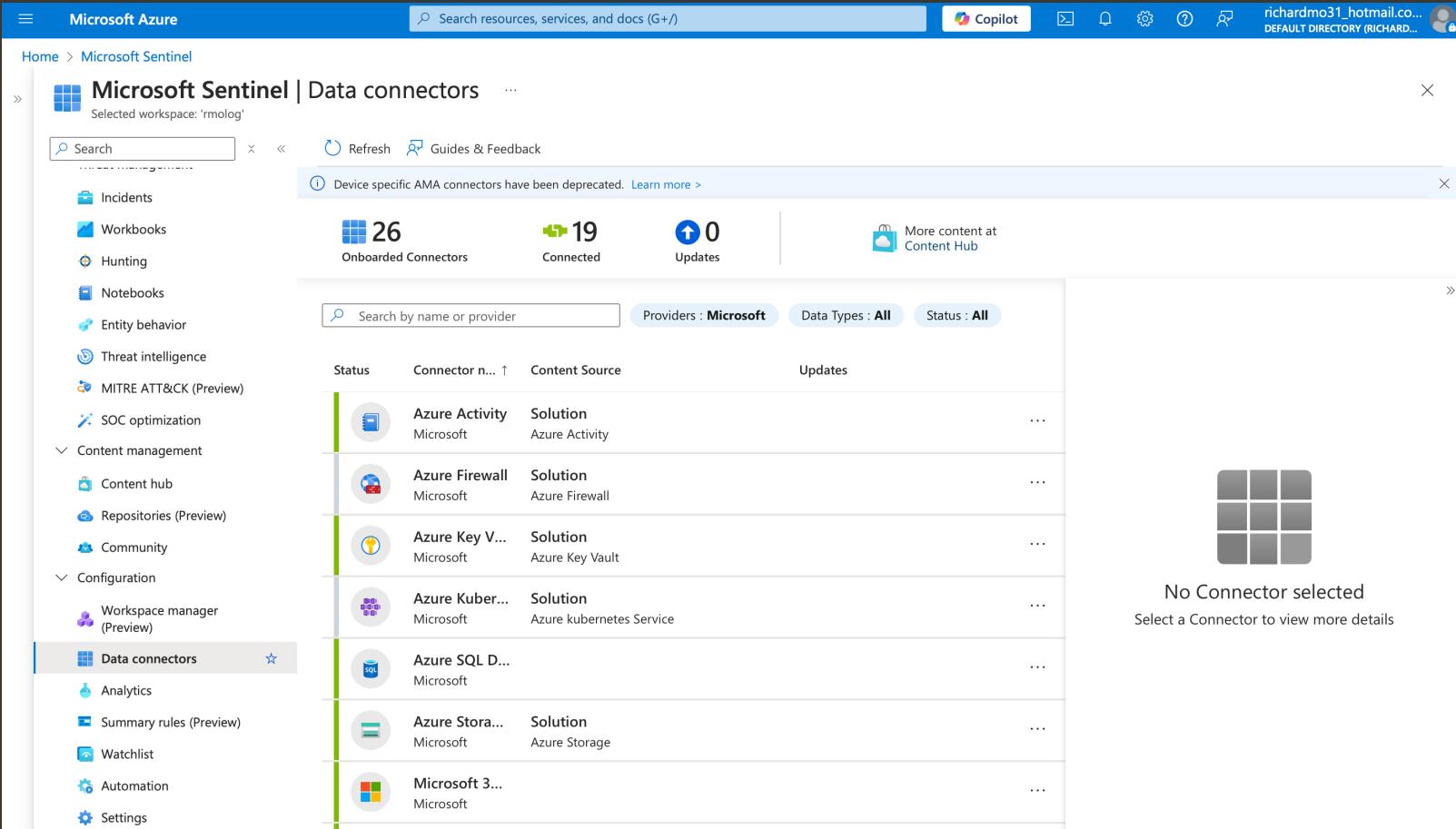
- Incident Count Indicators:** Open incidents (0), New incidents (0), Active incidents (0).
- Open incidents by severity:** High (0), Medium (0), Low (0), Informational (0).
- Search and Filter:** 'Search by ID, title, tags, owner or product' input, and filters for Severity (All), Status (All), Incident Provider name (All), and a 'More (2)' dropdown.
- Auto-refresh incidents:** A toggle switch is turned on.
- Table View:** A grid of incident details. Headers include: Severity ↑↓, Incident number ↑↓, Title ↑↓, Alerts, Incident provider na..., and Alert product name. Data rows show 10 incidents, all of which are Medium severity. The first incident is 'NewProcessesonOS' with ID 38.
- Right Panel:** A large circular icon with three stacked boxes and a plus sign, labeled 'No incidents selected. Select an incident to view more details'.
- Pagination:** Navigation buttons for '< Previous', '1 - 38', and 'Next >'.

# 2.6: Continuous Monitoring – Analytics (Implemented Rules)

The screenshot shows the Microsoft Azure Sentinel Analytics interface. The left sidebar navigation bar includes Home, Microsoft Sentinel, and several other options like Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization, Content management, Configuration, Analytics (which is selected and highlighted in blue), Summary rules (Preview), Watchlist, Automation, and Settings. The main content area displays the 'Microsoft Sentinel | Analytics' page for the workspace 'rmolog'. It features a search bar, a toolbar with Create, Refresh, Analytics workbooks, Rule runs (Preview), Enable, Disable, Delete, Import, Export, Columns, and more. A summary section shows 11 Active rules, a 'More content at Content hub' button, and a 'Rules by severity' chart with 2 High, 8 Medium, 1 Low, and 0 Informational rules. Below this is a table titled 'Active rules' with columns for Severity, Name, Rule type, Status, and Tactics. The table lists 11 rules, each with a checkbox, severity color, name, rule type (Scheduled, ML Behavior Analytics, NRT), status (Enabled), and tactic (Exfiltration, Initial Access, Impact, Defense Evasion, Persistence, Credential Access). The last rule is a Low-severity rule named 'Suspicious application consent for offline access...'.

Severity	Name	Rule type	Status	Tactics
Medium	Data-Copy-Event	Scheduled	Enabled	
High	Data-Exfiltration	Scheduled	Enabled	Exfiltration
Medium	(Preview) Anomalous SSH Login Detection	ML Behavior Analytics	Enabled	Initial Access
Medium	Suspicious number of resource creation or de...	Scheduled	Enabled	Impact
Medium	NRT Creation of expensive computes in Azure	NRT	Enabled	Defense Evasion
Medium	(Preview) Anomalous RDP Login Detections	ML Behavior Analytics	Enabled	Initial Access
Medium	FailedLogon	Scheduled	Enabled	
Medium	UserLogin	Scheduled	Enabled	
Medium	NewProcessesonOS	Scheduled	Enabled	Persistence
High	New user Added to Entra	Scheduled	Enabled	
Low	Suspicious application consent for offline acce...	Scheduled	Enabled	Credential Access

# 2.7: Continuous Monitoring – Connected Data Source



The screenshot shows the Microsoft Azure Sentinel Data connectors page. The left sidebar includes links for Home, Microsoft Sentinel, Incidents, Workbooks, Hunting, Notebooks, Entity behavior, Threat intelligence, MITRE ATT&CK (Preview), SOC optimization, Content management (Content hub, Repositories (Preview), Community), Configuration (Workspace manager (Preview), Data connectors, Analytics, Summary rules (Preview), Watchlist, Automation, Settings), and Copilot. The main content area displays 26 Onboarded Connectors and 19 Connected connectors. A message indicates that device specific AMA connectors have been deprecated. The table lists connectors like Azure Activity, Azure Firewall, Azure Key Vault, Azure Kubernetes Service, Azure SQL Database, Azure Storage, and Microsoft 365.

Status	Connector n...	Content Source	Updates
Green	Azure Activity	Solution Azure Activity	...
Green	Azure Firewall	Solution Azure Firewall	...
Green	Azure Key V...	Solution Azure Key Vault	...
Green	Azure Kuber...	Solution Azure kubernetes Service	...
Green	Azure SQL D...	Solution Microsoft	...
Green	Azure Stora...	Solution Azure Storage	...
Green	Microsoft 3...	Solution Microsoft	...

No Connector selected  
Select a Connector to view more details

# 2.8: Continuous Monitoring – Additional External Threat Intelligence

Microsoft Azure Search resources, services, and docs (G+/) Copilot richardmo31@hotmail.co... DEFAULT DIRECTORY (RICHARD...)

Home > Microsoft Sentinel | Data connectors > Threat intelligence - TAXII ...

Delete Threat intelligence - TAXII

Connected Status Microsoft Provider 3 Minutes Ago Last Log Received

Author Microsoft Supported by Microsoft Corporation | Email

Related content: Workbooks (0), Queries (2), Analytics rules templates (48)

Data received: Go to log analytics

Date	Data Received (K)
March 30	0
March 31	0
April 1	0
April 2	120K
April 3	30K
April 4	25K
April 5	30K

ThreatIntelligen... 213K

Data types: ThreatIntelligenceIndicator 4/6/2025, 10:09:56 PM

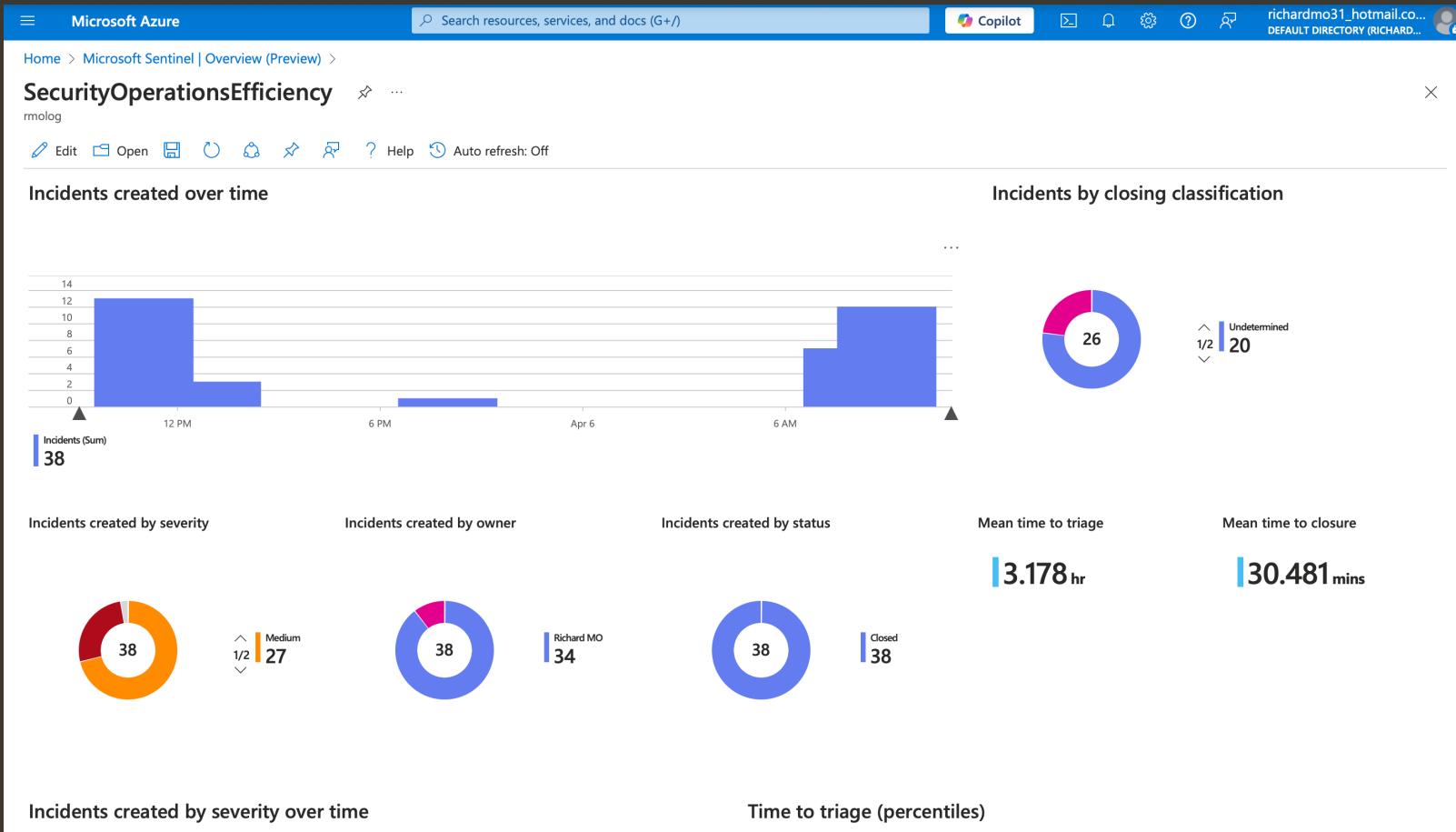
Import indicators: All available  
Poling frequency: Once an hour

Add

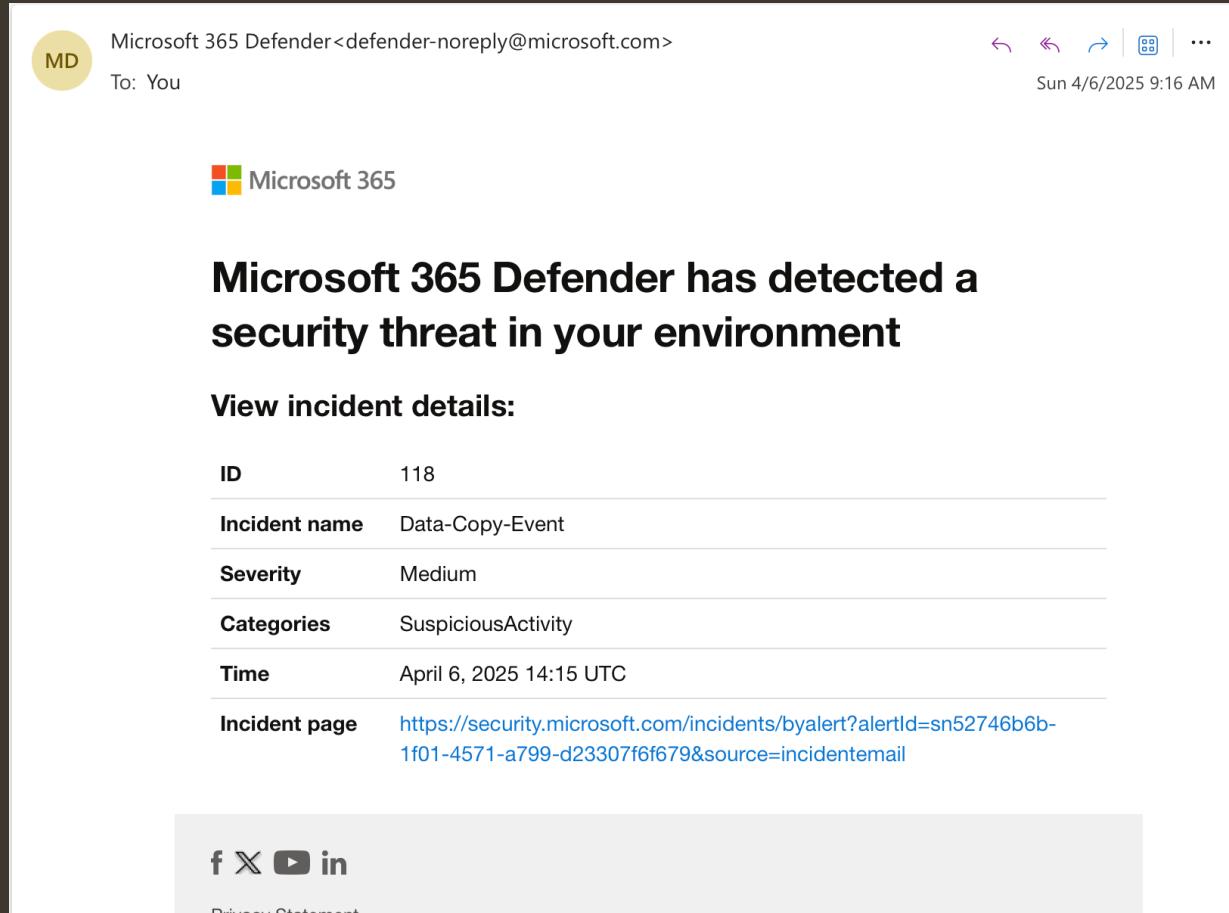
List of configured TAXII servers

Friendly name	TAXII server	Collection ID	Last indicator
Pulsedive	https://pulsediv...	981c4916-ebb2...	04/06/25, 09:

# 2.9: Continuous Monitoring – Security Operations Efficiency



# 3.0: Continuous Monitoring – Incident Escalated



# 3.1: Continuous Monitoring – Azure Monitor (VM Status)

**Fired:Sev4 Azure Monitor Alert VMShutDown  
on rmoservermgmt (microsoft.compute/virtualmachines ) at  
4/6/2025 2:17:36 PM**

[View the alert in Azure Monitor >](#) [Investigate >](#)

**Summary**

---

<b>Alert name</b>	VMShutDown
<b>Severity</b>	Sev4
<b>Monitor condition</b>	Fired
<b>Affected resource</b>	rmoservermgmt
<b>Resource type</b>	microsoft.compute/virtualmachines
<b>Resource group</b>	administrativefunction
<b>Description</b>	Your VM has been powered off
<b>Monitoring service</b>	Activity Log - Administrative
<b>Signal type</b>	Activity Log

## 3.2: Security - Defense-in-depth Design

