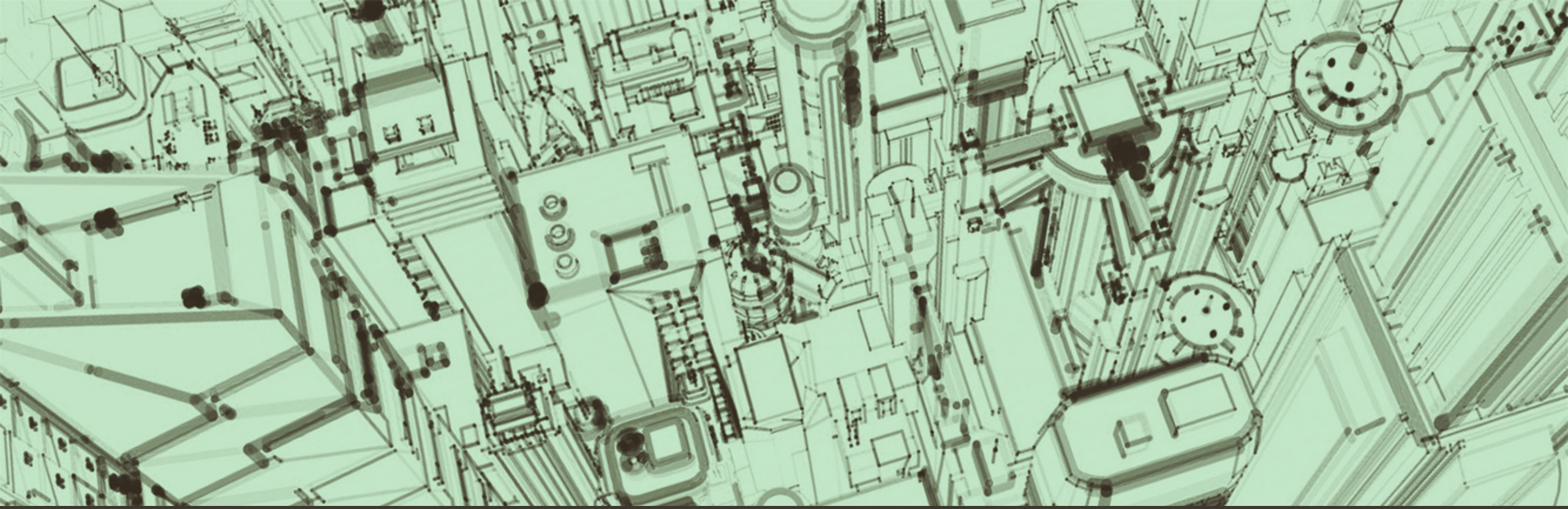


Richard M. Okhai

Technical Portfolio

Cybersecurity | Data Science | Technology & Engineering

Table of Content

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.

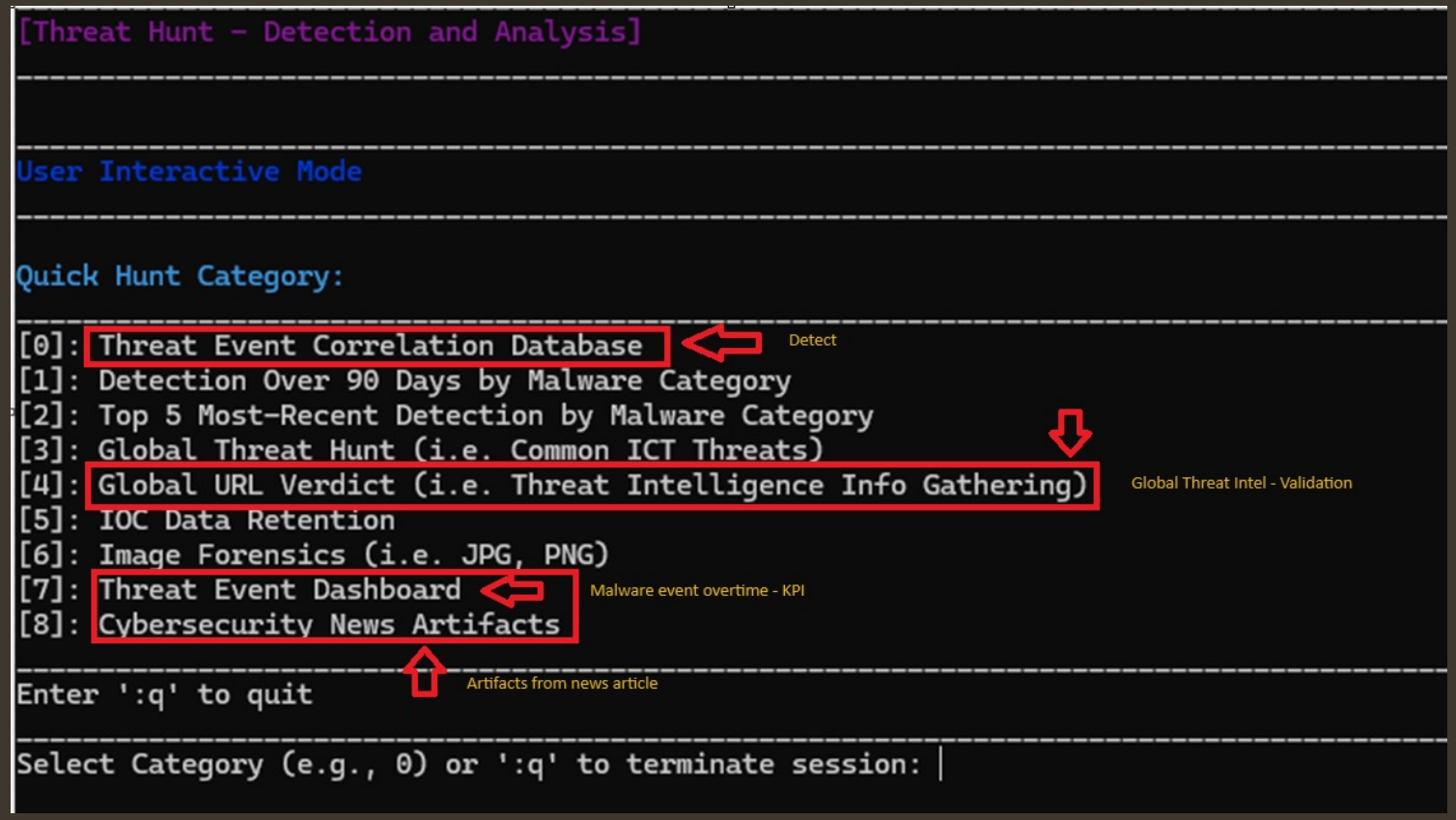
Competitive Intelligence – Supply Chain & Program Modernization

- 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.

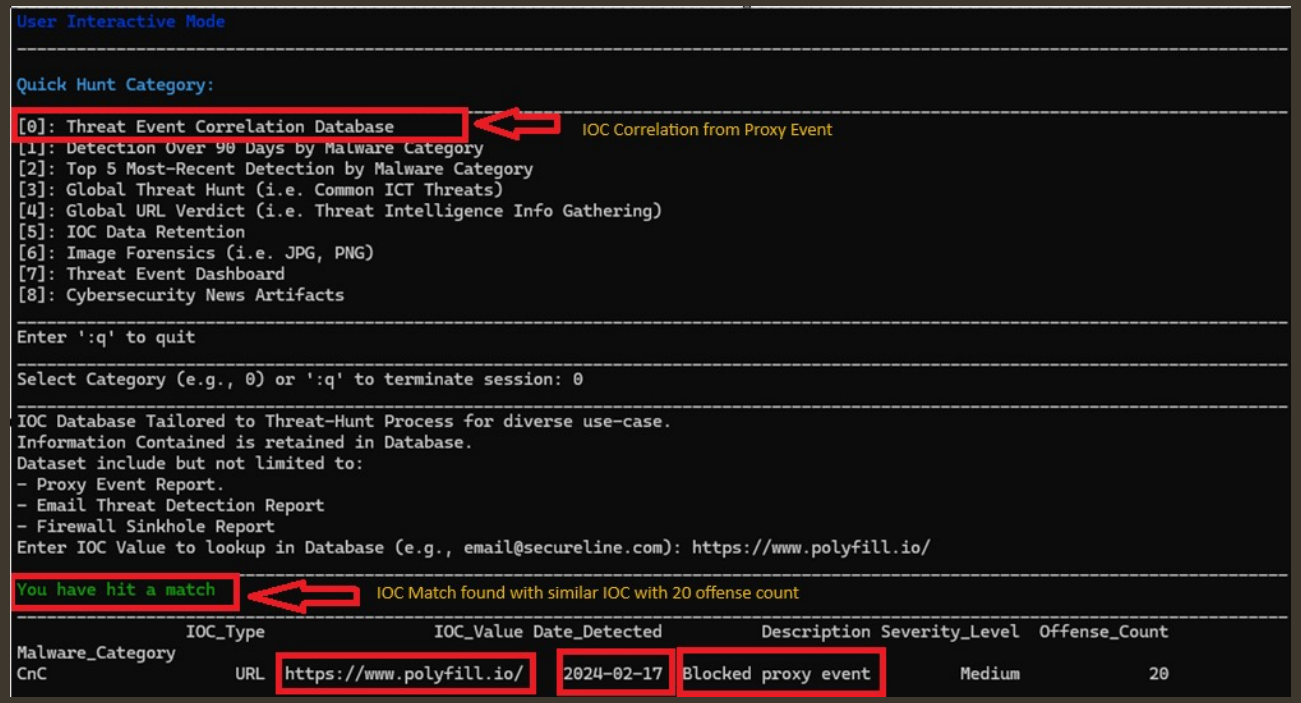
1.0: Incident Response & Malware Forensics



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

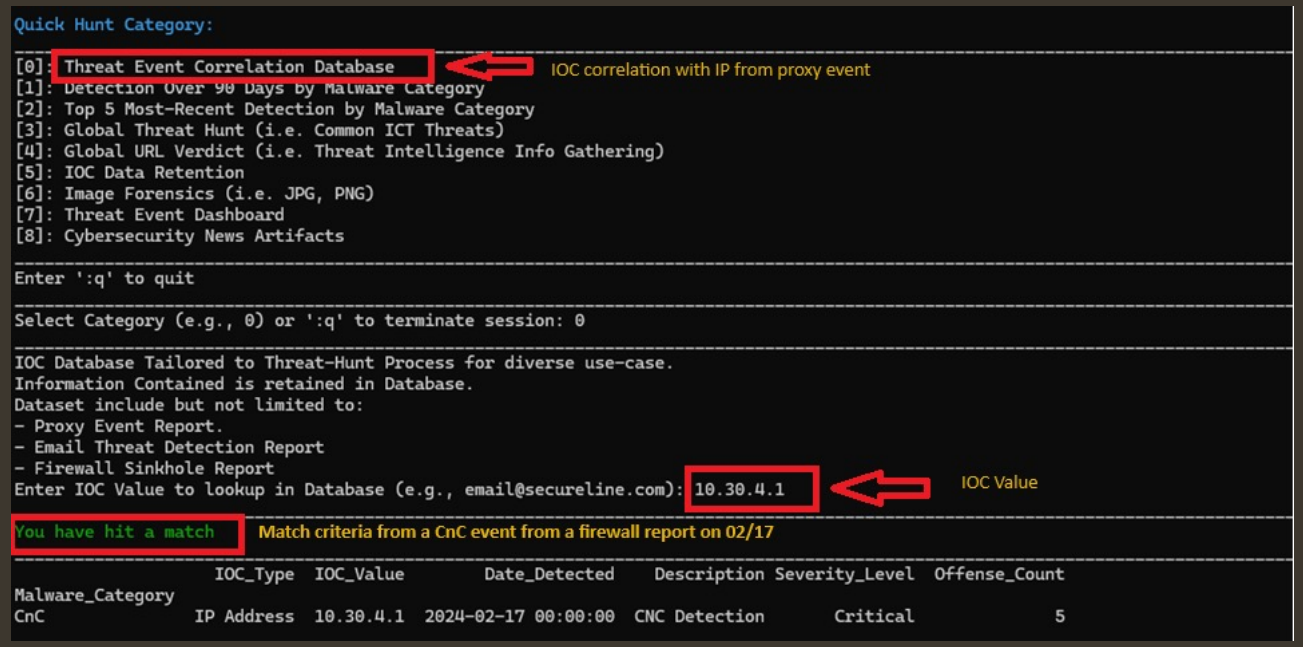
IOC Retained: IP Address & URL.

1.1: Incident Response & Malware Forensics



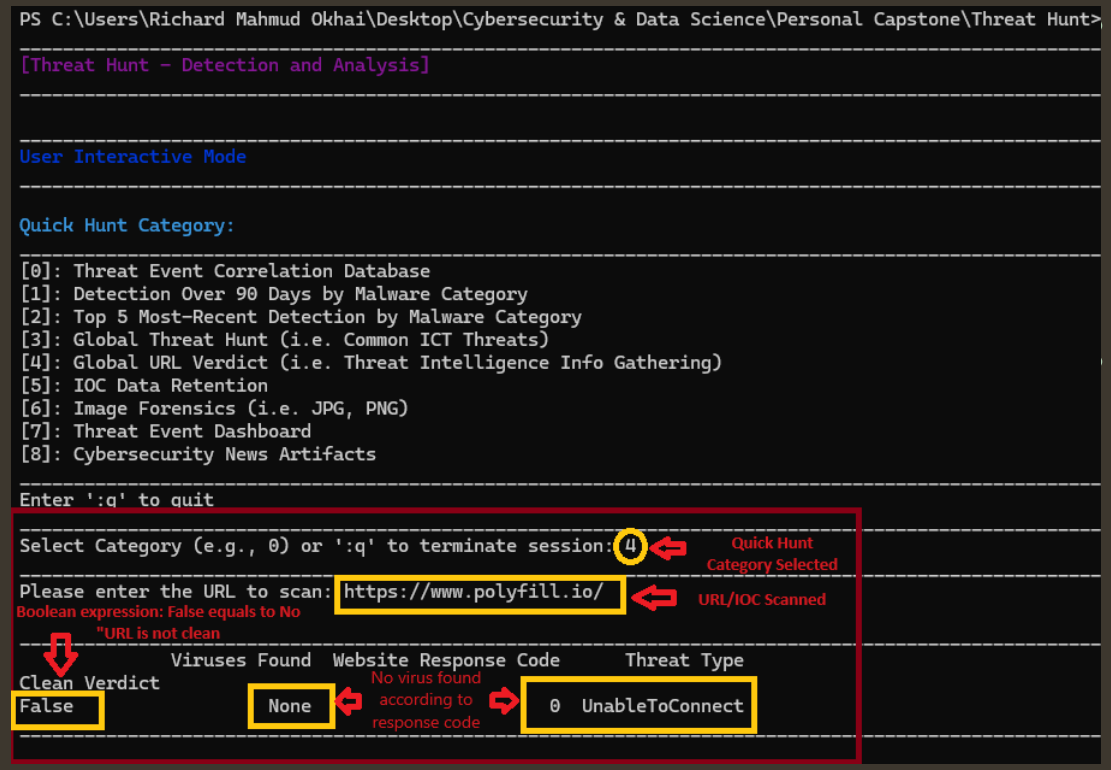
- **Action Plan** – Correlate IOC from proxy with IOC Database for previous event detected.
  - **Provided IOC:** URL.
  - **Provided Source:** Proxy Daily Report.

1.2: Incident Response & Malware Forensics



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

1.3: Incident Response & Malware Forensics



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).

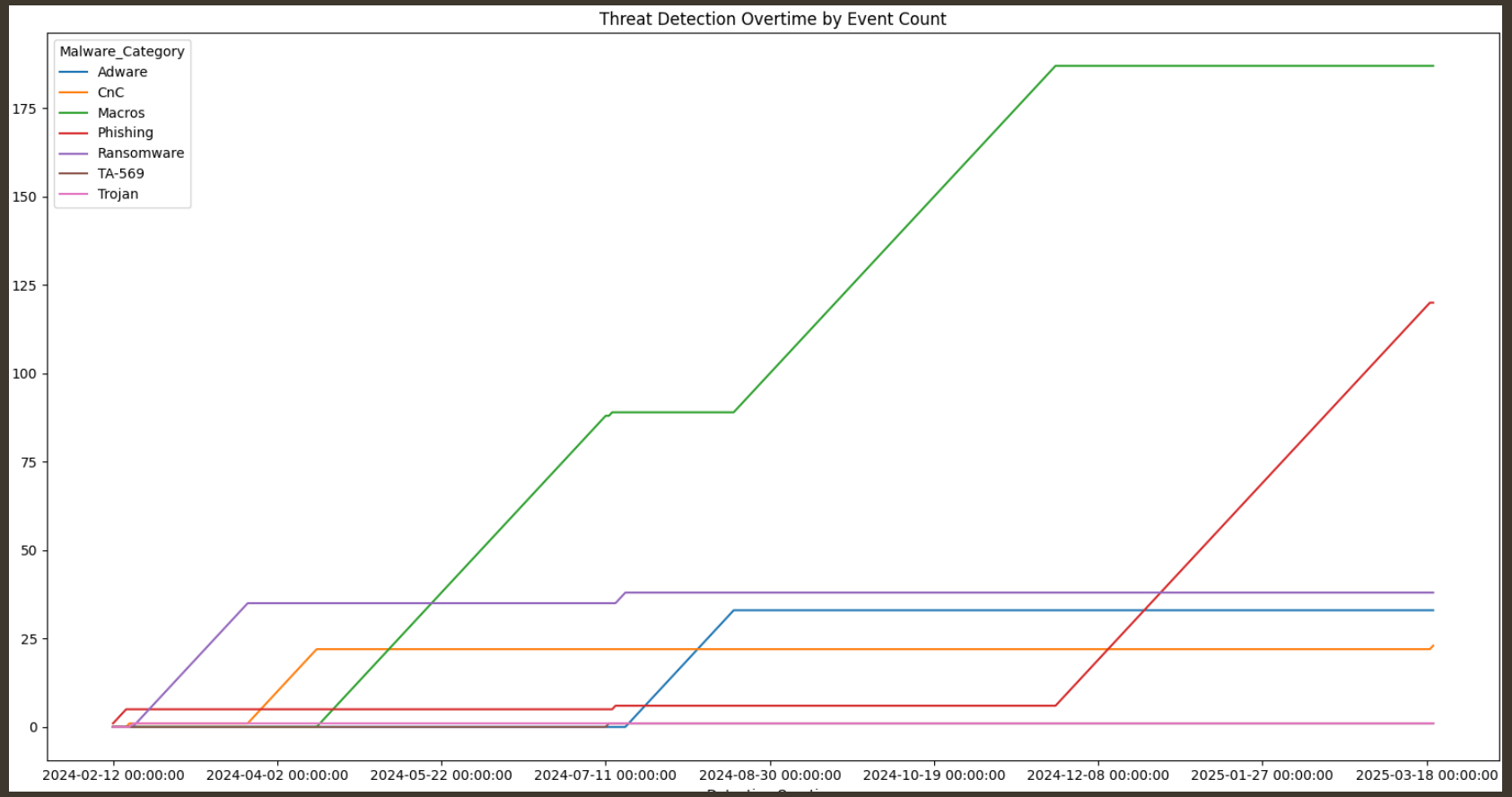
Correlation with Global Threat Intelligence: Shows result as False (Clean? "**No**").

1.4: Incident Response & Malware Forensics

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

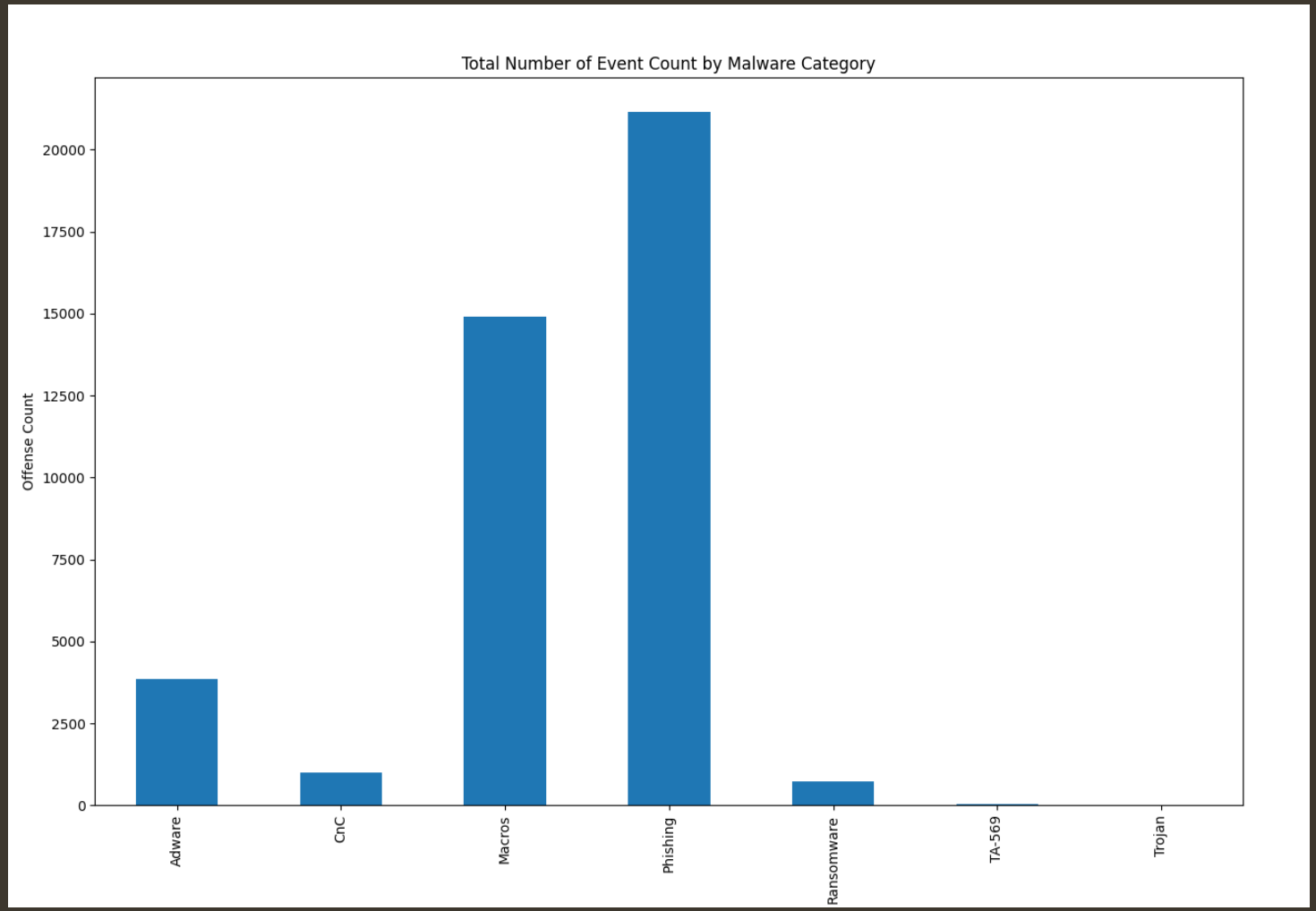
```
Select Category (e.g., 0) or ':q' to terminate session: 7
--------------------------------------------------------------------------------------------------------------------------------
[Local Threat Hunt Report]
--------------------------------------------------------------------------------------------------------------------------------
Timestamp:  2024-06-28 16:10:47.103834


--------------------------------------------------------------------------------------------------------------------------------
Threat Overview - Top 10 Detection by Event Count
--------------------------------------------------------------------------------------------------------------------------------
                IOC_Type                                    IOC_Value        Date_Detected           Description Severity_Level  Offense_Count
Malware_Category
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



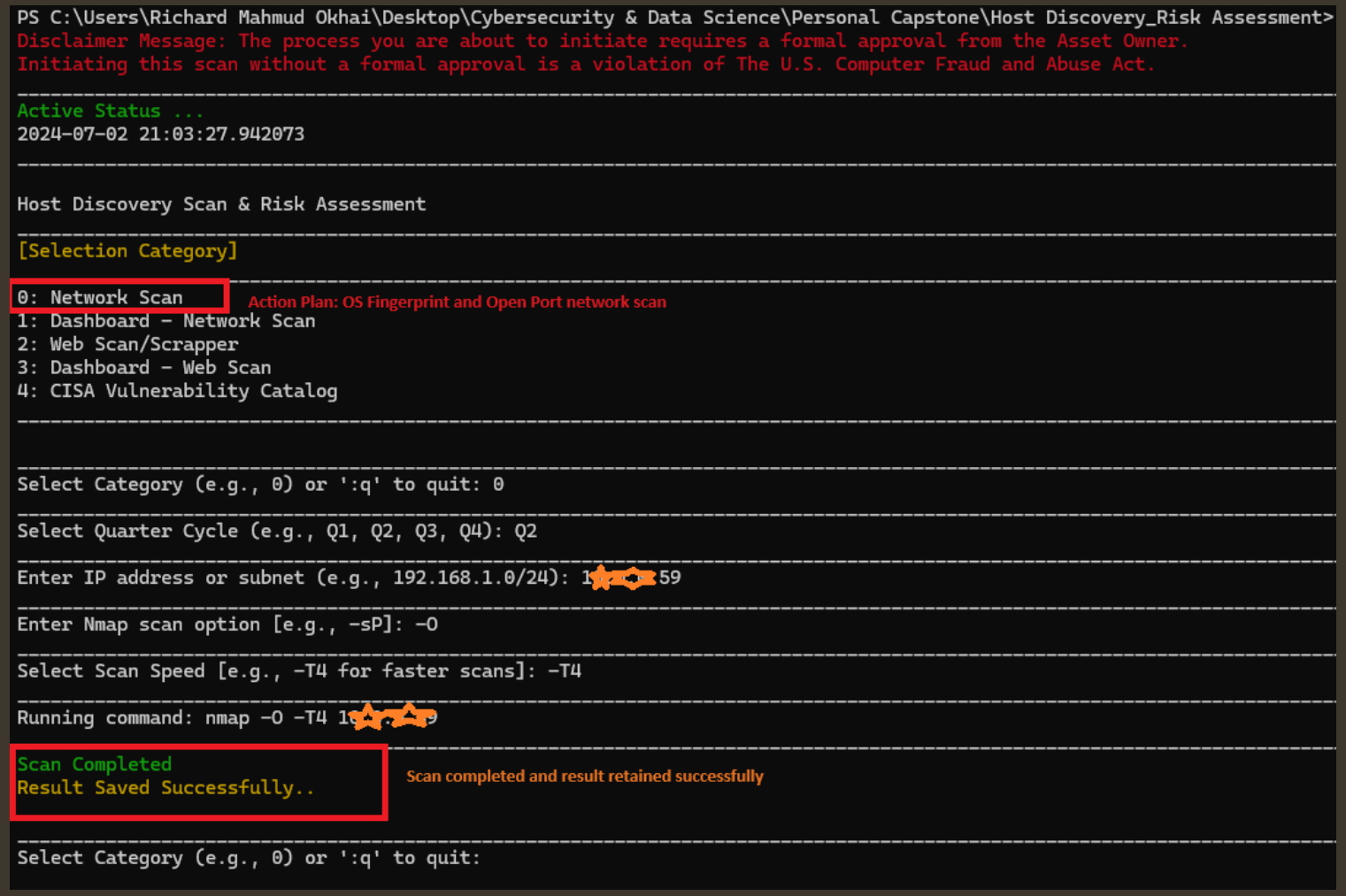
- **Dashboard Report Analysis**: Total Number of Event Count by Malware Category.

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
----------------------------------------------------------------------------------------------------------------------------------
Newsfeed based on Phishing email
----------------------------------------------------------------------------------------------------------------------------------
                                                          Description                                                    Artifacts                                                    Web URL Published Date
Source
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

----------------------------------------------------------------------------------------------------------------------------------
References
----------------------------------------------------------------------------------------------------------------------------------
Reference Article: https://www.nytimes.com/2017/09/14/technology/personaltech/spotting-the-phish-in-a-sea-of-email.html
Reference Article: https://www.nytimes.com/2021/05/13/world/europe/phishing-test-covid-bonus.html
Reference Article: https://www.nytimes.com/2016/11/29/technology/personaltech/skip-the-phish-on-the-menu.html
Reference Article: https://www.nytimes.com/2017/05/03/technology/personaltech/email-attack-hits-google-what-to-do-if-you-clicked.html
Reference Article: https://www.nytimes.com/2018/12/06/opinion/maggie-shen-king-the-big-phish.html
Reference Article: https://www.nytimes.com/2017/08/11/arts/music/popcast-phish-bakers-dozen.html
Reference Article: https://www.nytimes.com/2023/05/31/books/review/fancy-bear-goes-phishing-scott-shapiro.html
Reference Article: https://www.nytimes.com/2022/06/23/magazine/judge-john-hodgman-on-phish-shows.html
Reference Article: https://www.nytimes.com/2023/03/17/arts/artist-email-scam.html
Reference Article: https://www.nytimes.com/2020/06/04/us/politics/china-joe-biden-hackers.html
```

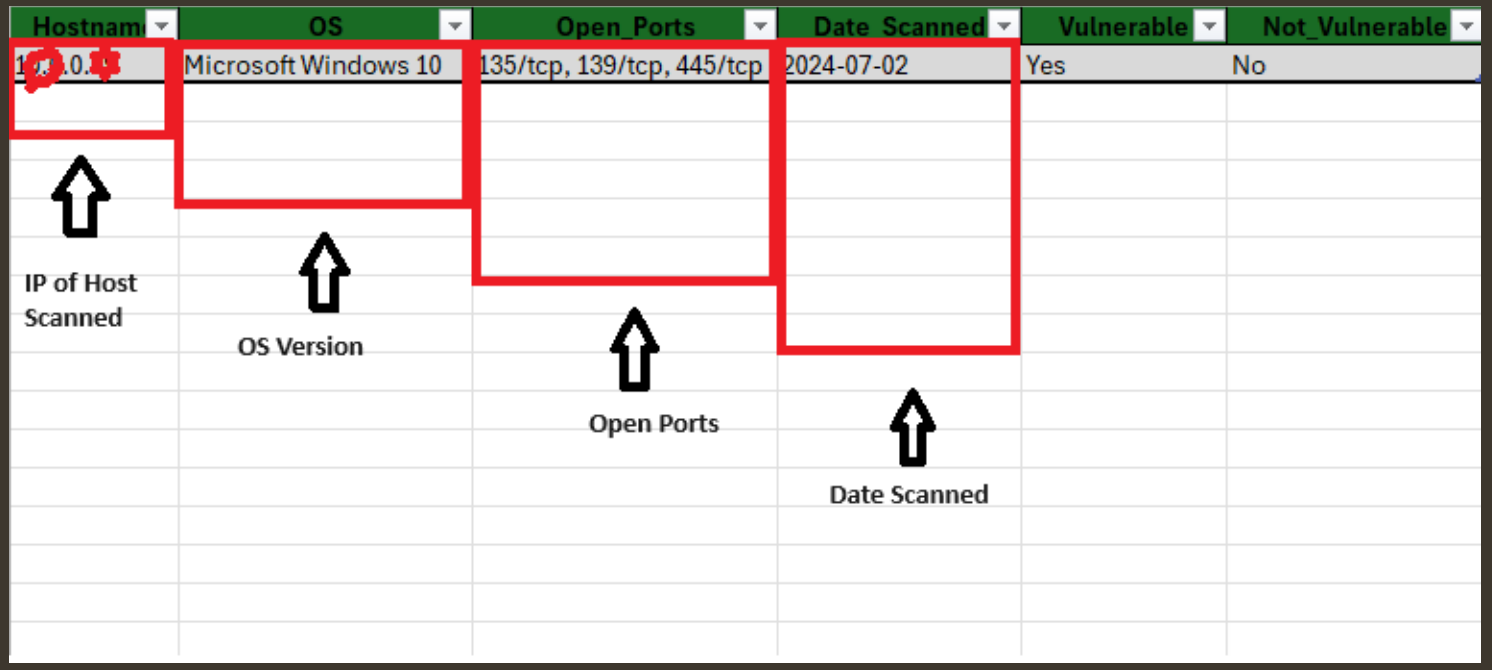
1.7: Process Automation – Cybersecurity



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

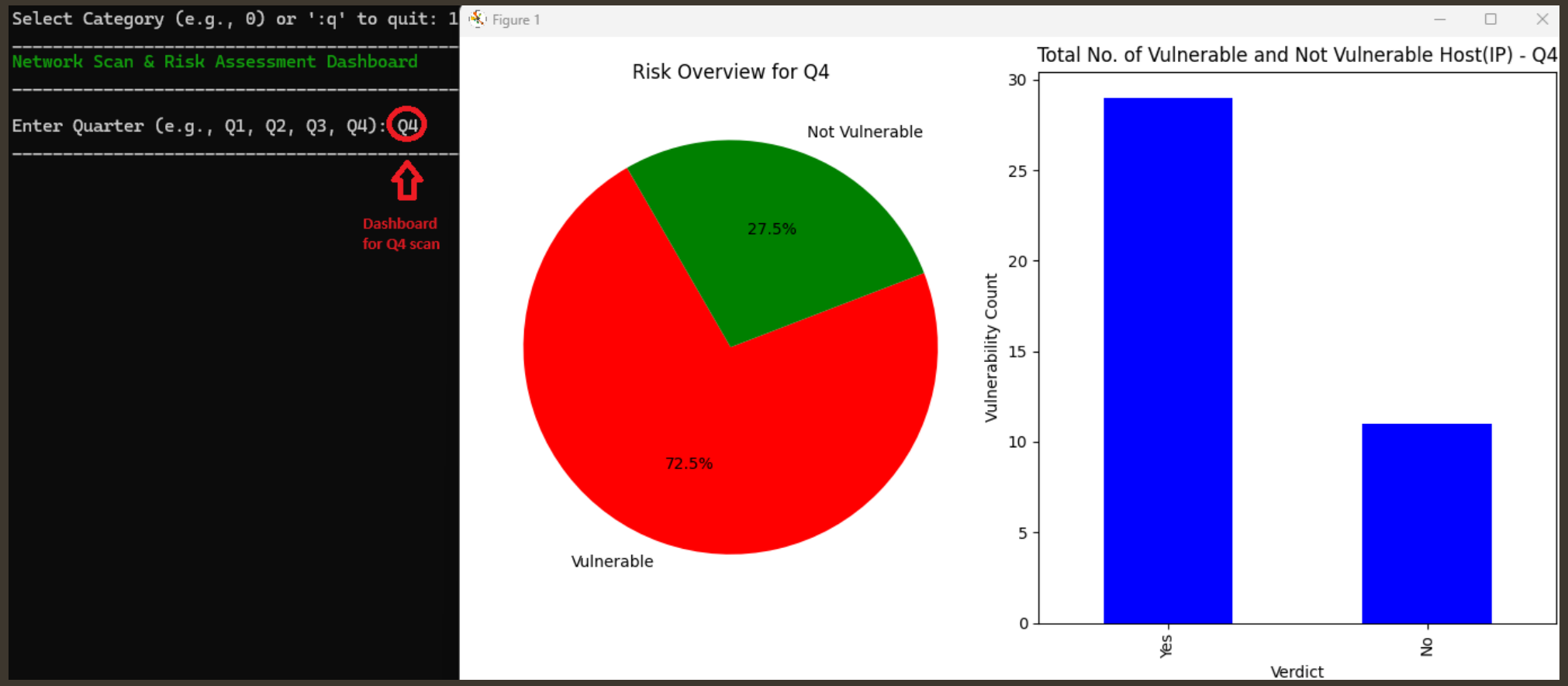
1.8: Process Automation – Cybersecurity

- **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.



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 utilzed 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

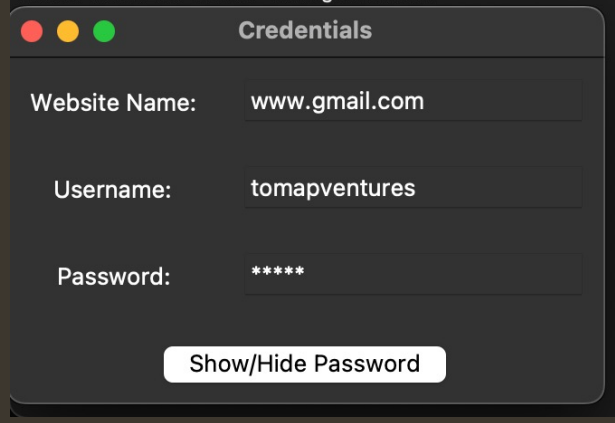
- Credentials Saved in a database table.

```
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

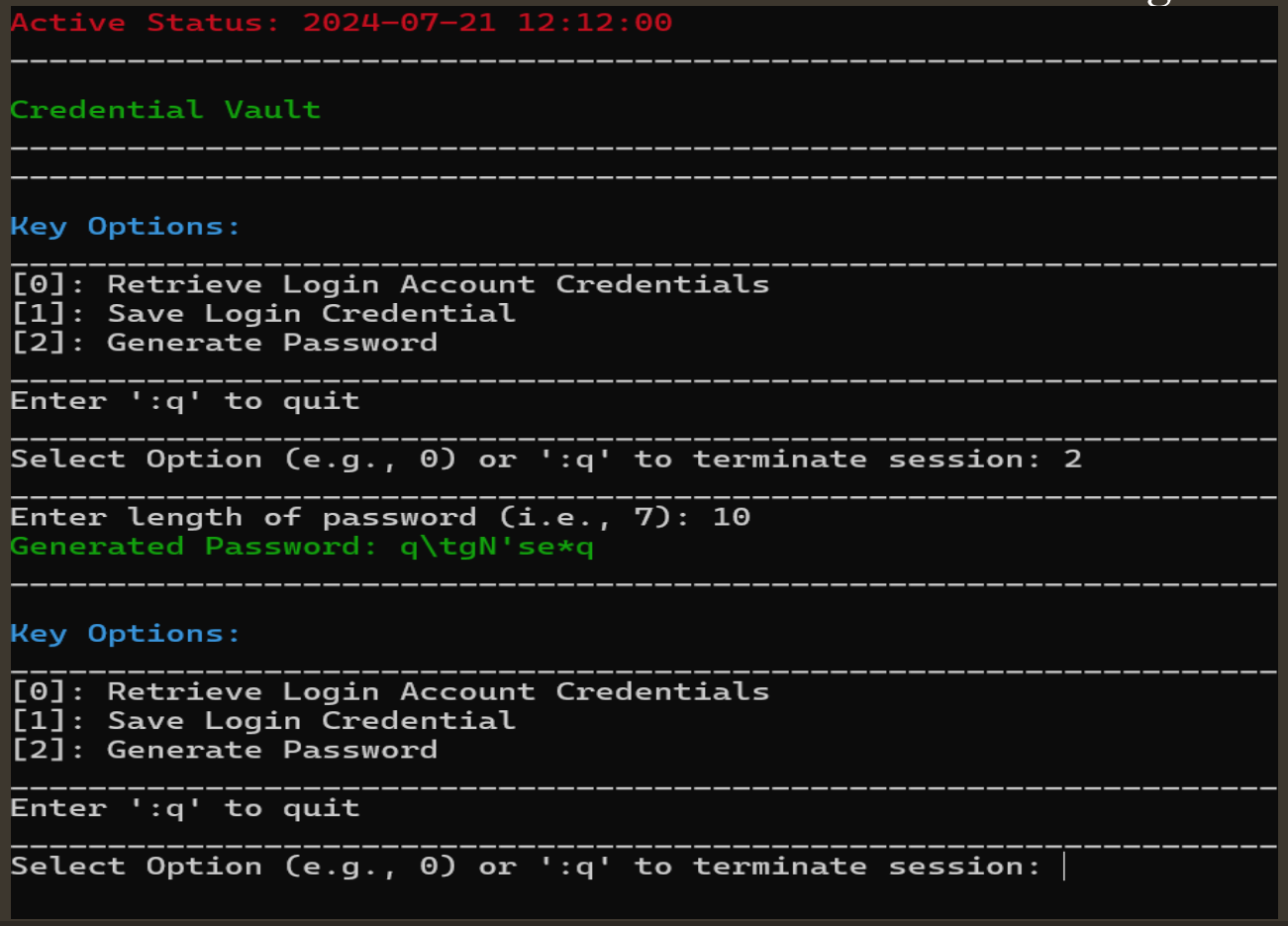
- Credential Utilized in next login.

```
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
```



2.9: Generate Credentials

- Generate Credentials on a website for future login.

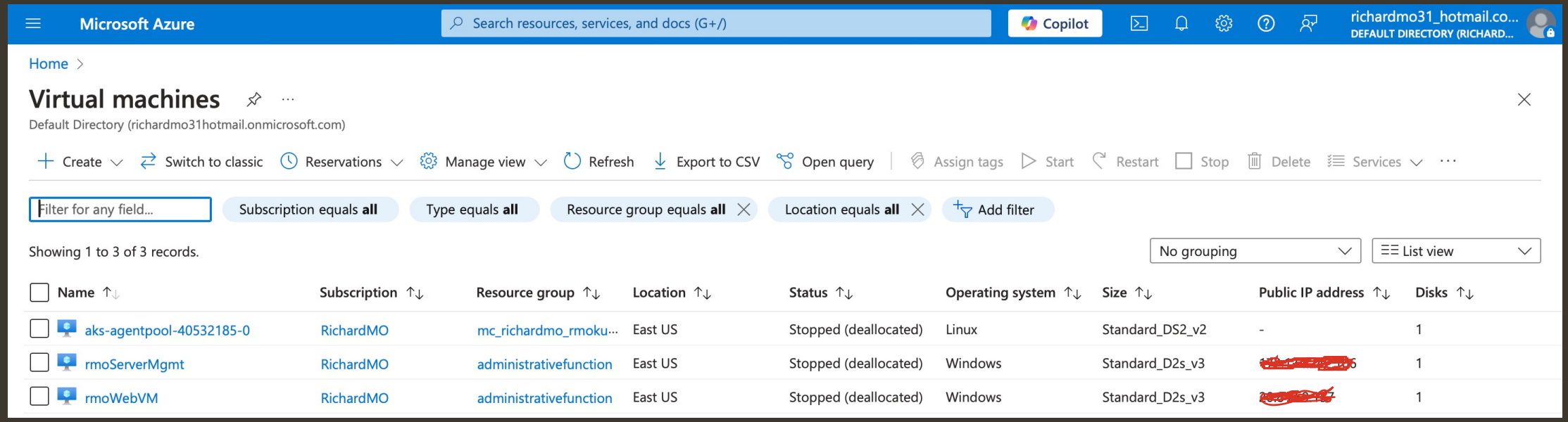


Domain 4: Cloud Integration

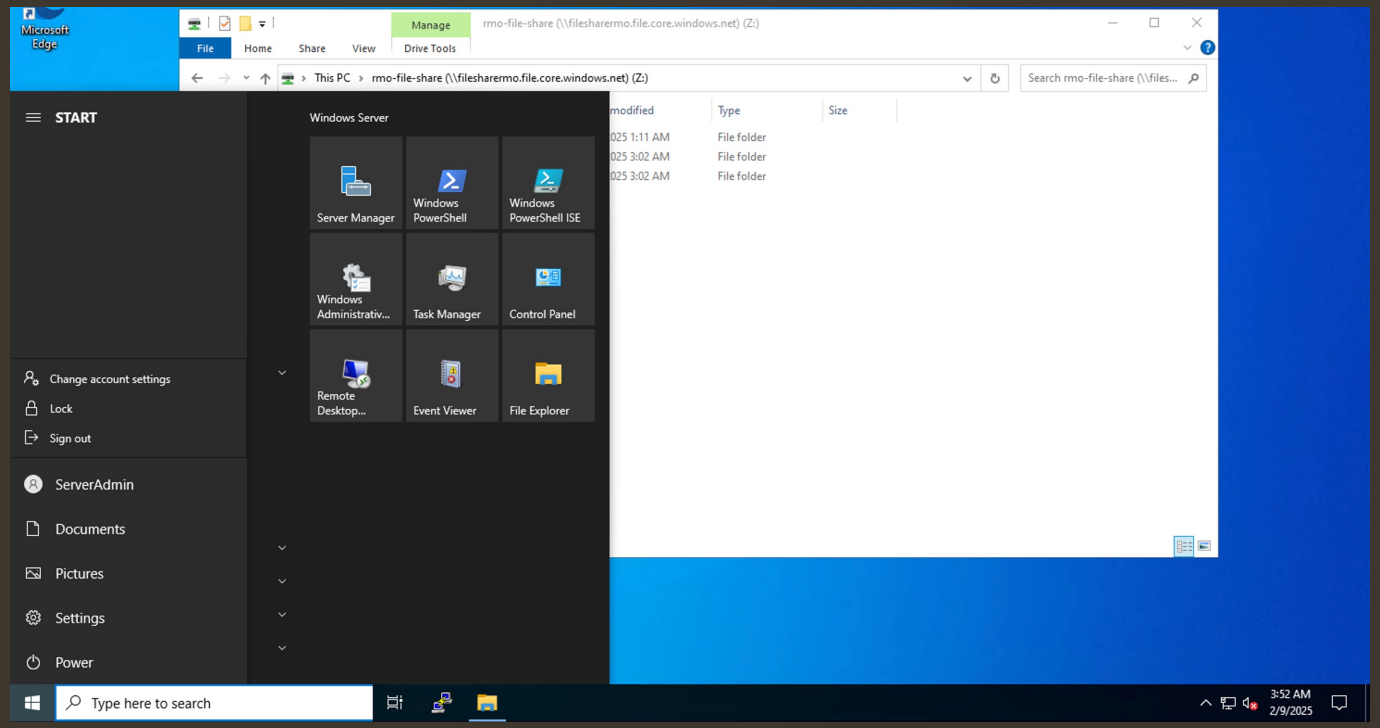
- Azure - Infrastructure as a Service | Platform as a Service
- Objective: Web App Implementation
  - **Business|Use Case**: Web accessibility for KeyVault App.
    - **Automation Task**: PowerShell Script – Azure Virtual Machine | Kubernetes Services | Container Registry
      - **Resolution:** Develop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

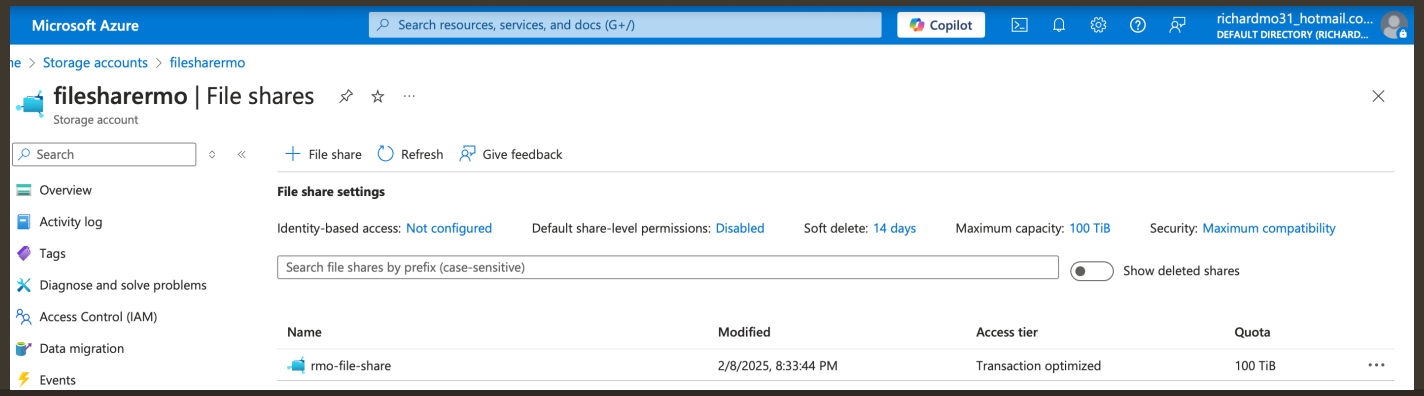
3.0: Remote Accessibility – Server Management

- 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~~)



3.1: File-Share Capability

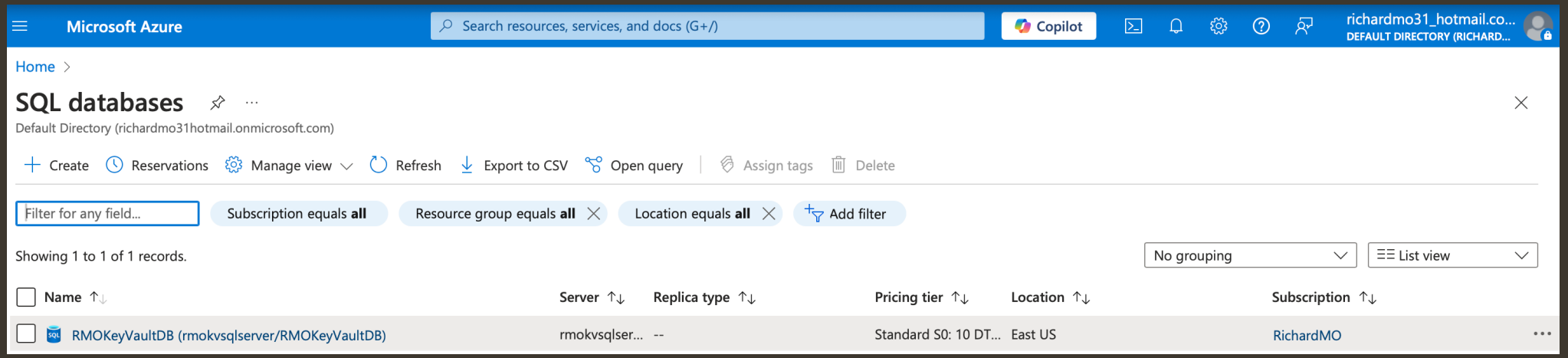




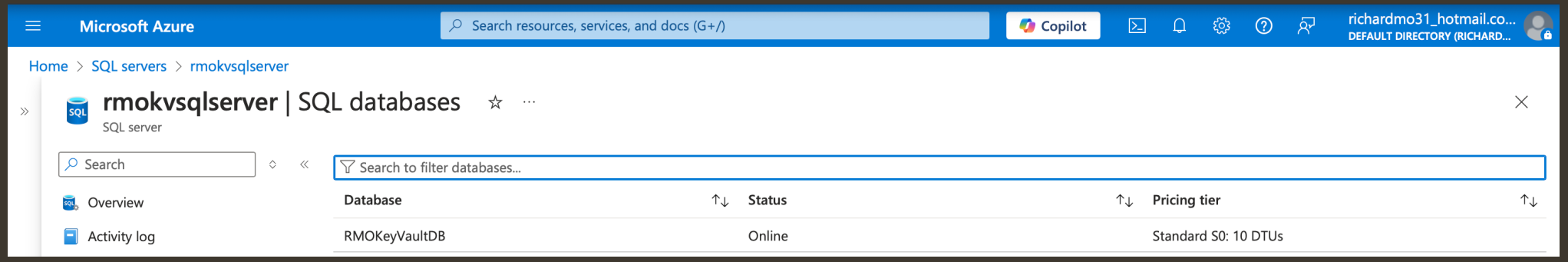
- **File shared**:
  - Development file and codes
  - Shared from the local endpoint to AZ VM
- **Connected Endpoint**:
  - WebVM
  - Jump-post

3.2: SQL Database & Database Server

SQL Database - KeyVault

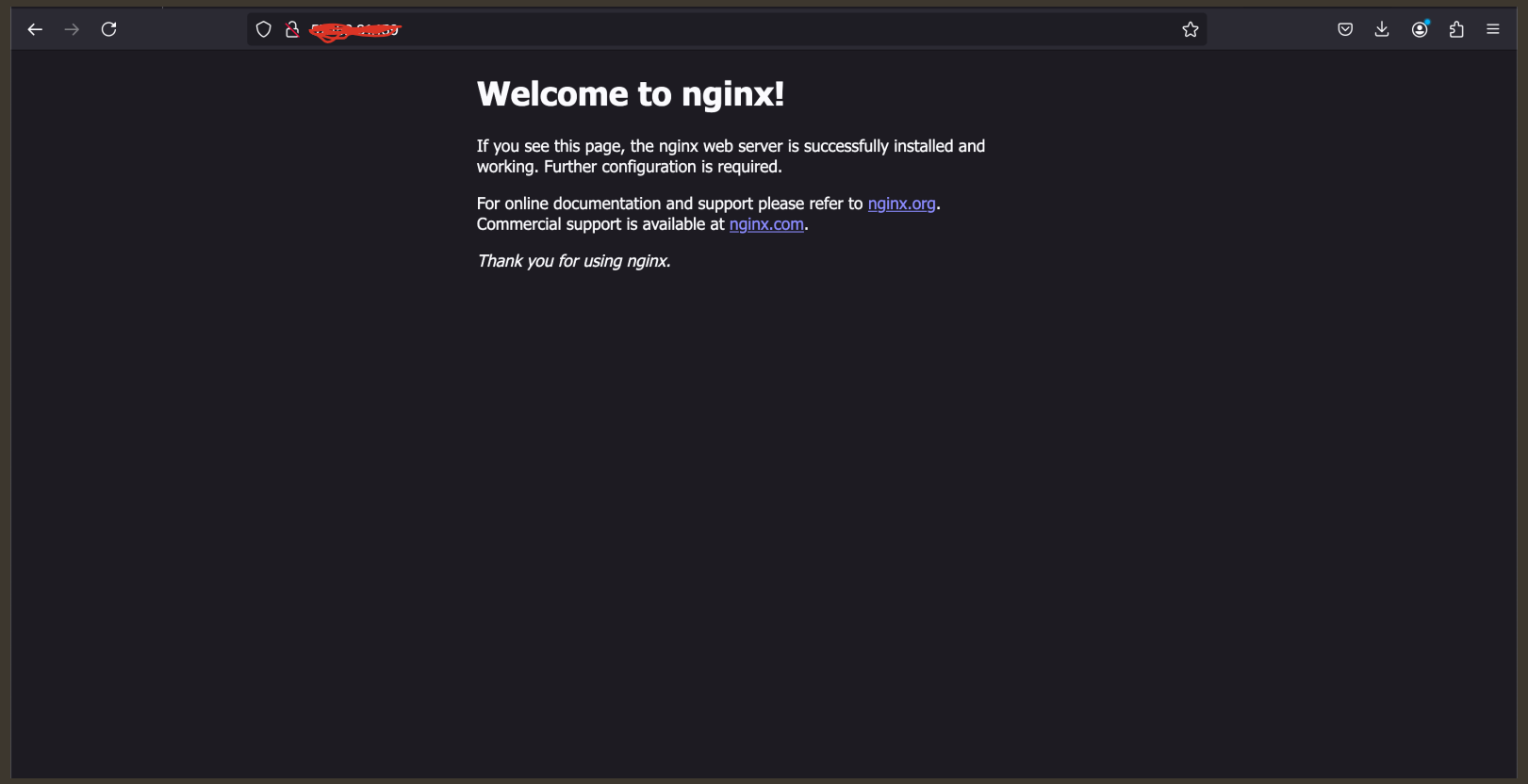


Database Server - KeyVault



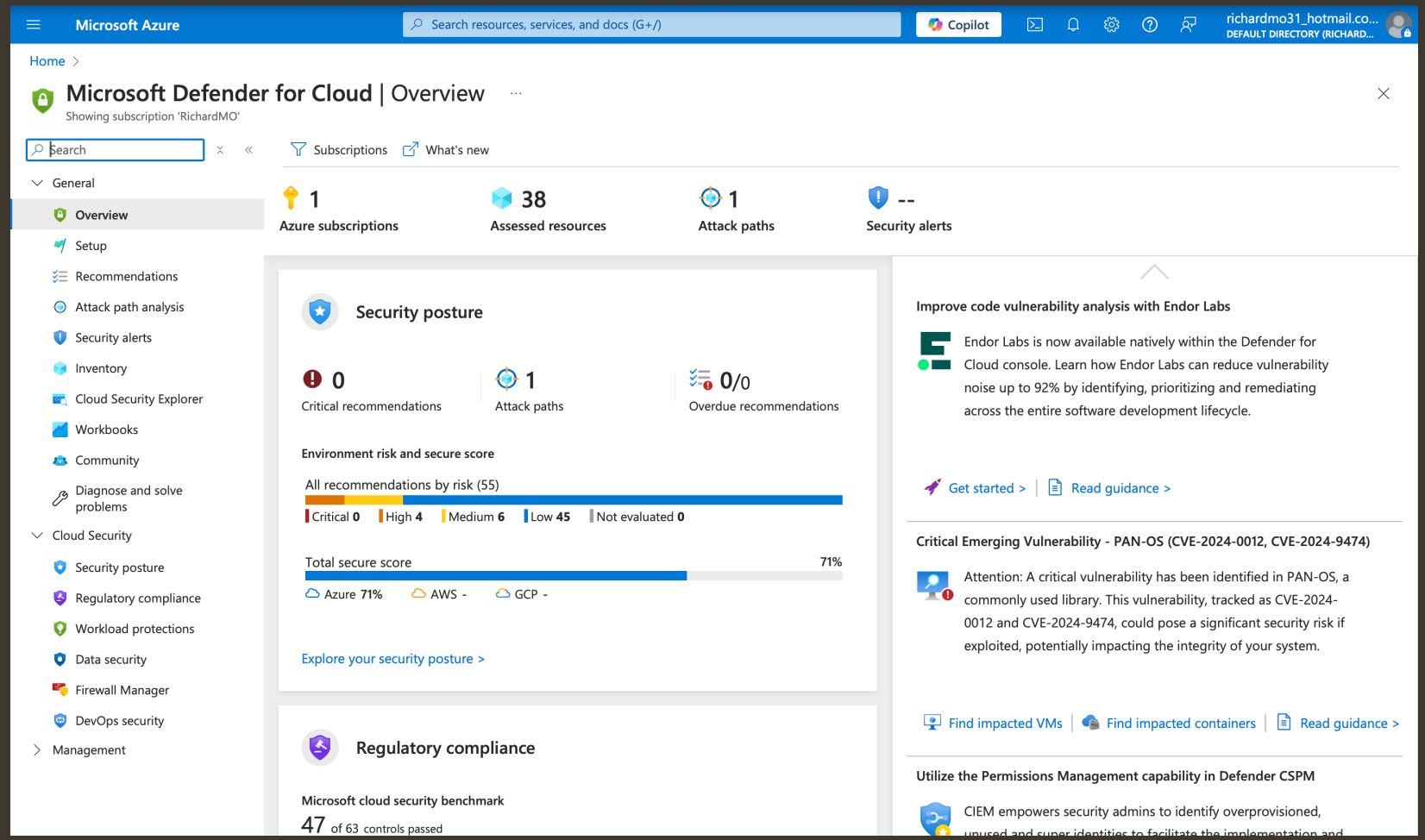
3.3: Web/Database Server – ACR | AKS

```
richard [ ~ ]$ kubectl get service nginxexternal
NAME            TYPE           CLUSTER-IP     EXTERNAL-IP     PORT(S)        AGE
nginxexternal   LoadBalancer   [redacted]     [redacted]      80:31806/TCP   55s
richard [ ~ ]$
```



- 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

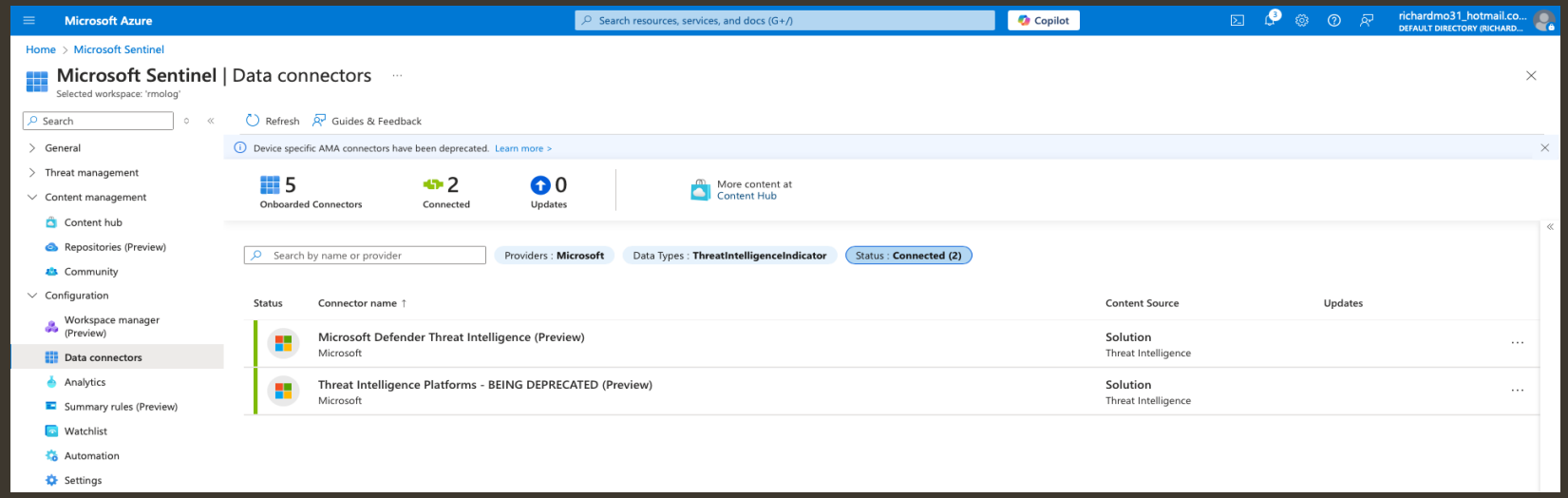
3.4: Security Control: Microsoft Defender for Cloud

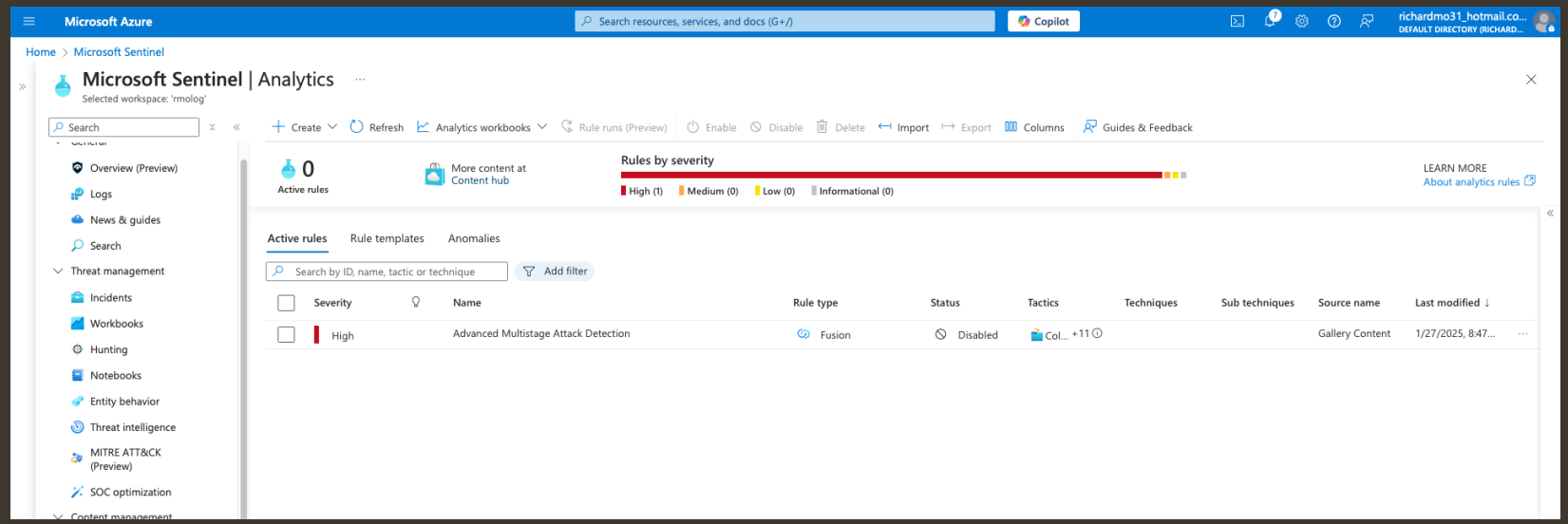


Microsoft Defender for Cloud -

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

3.5: Continuous Monitoring – Microsoft Sentinel





Microsoft Sentinel

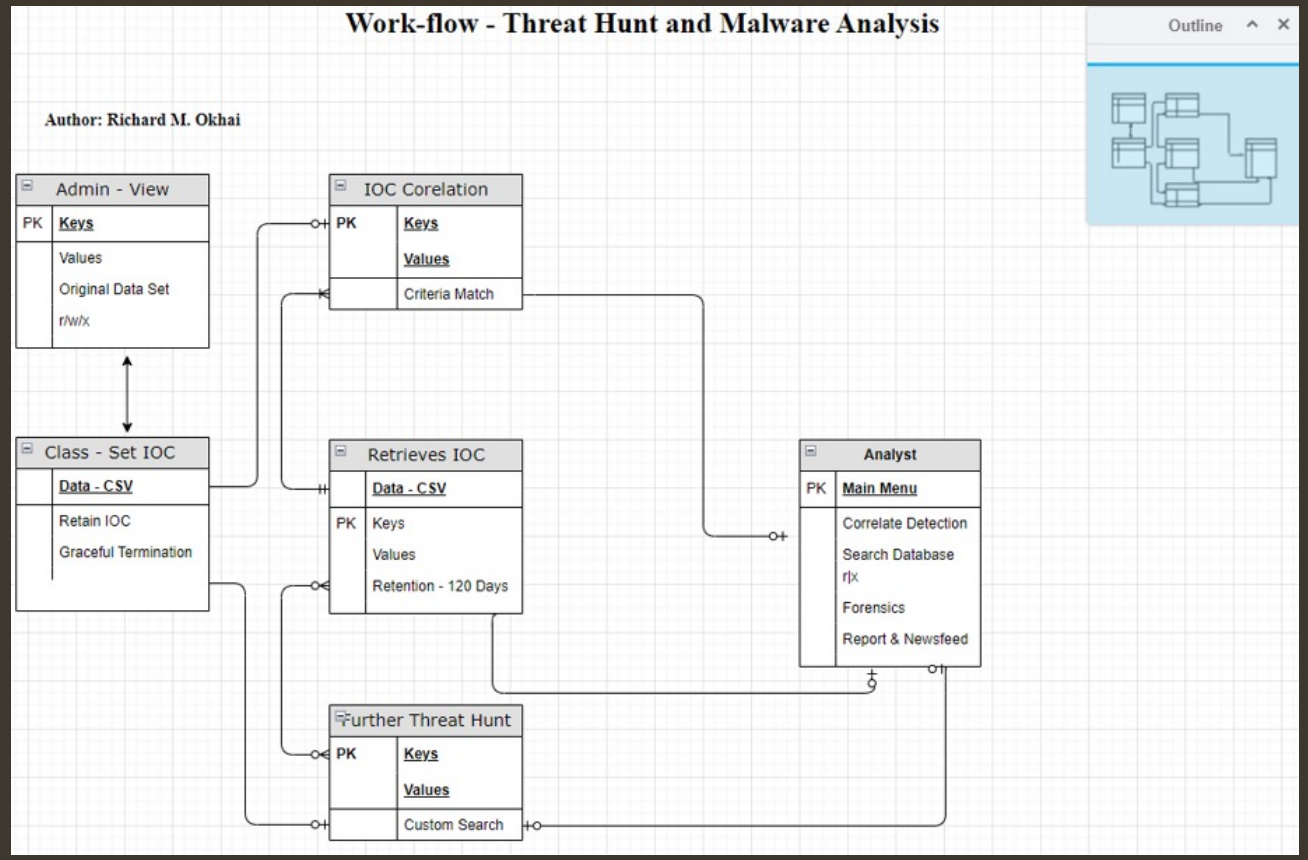
Log Source: Data Analytics Workspace

Connected Log Sources:

- Microsoft Defender Threat Intelligence
- Threat Intelligence Platforms

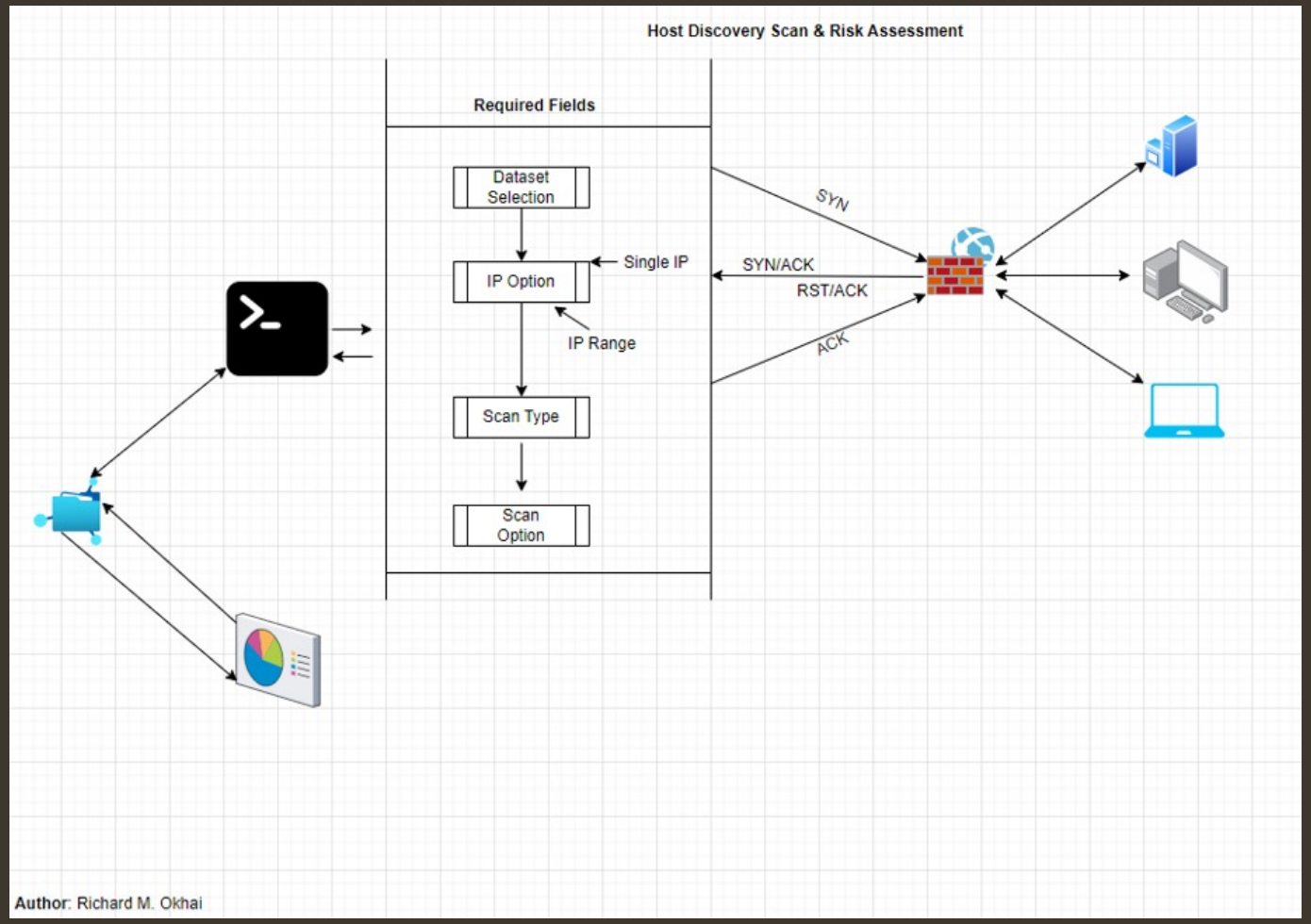
Appendix

1.0: Workflow: Threat-Hunt Tool



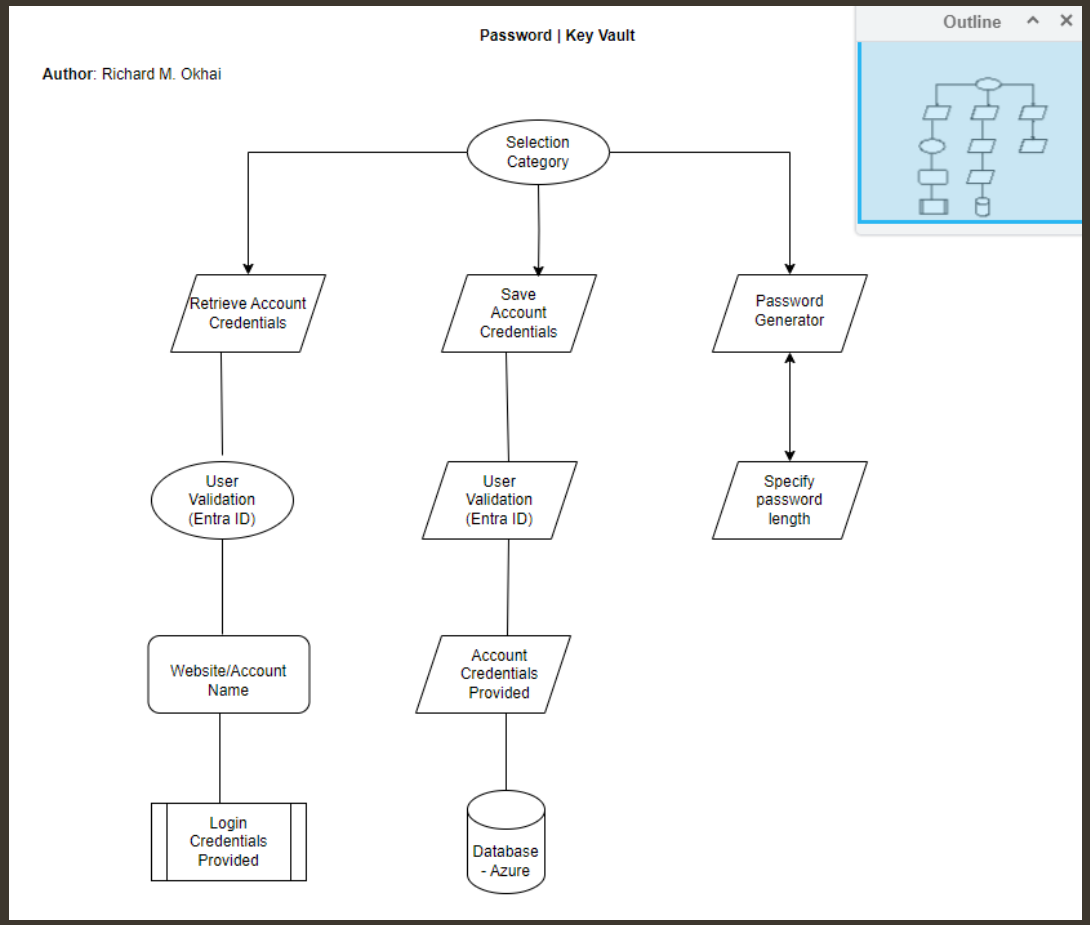
- **Language:** Python
- **Product Type:** Threat-Hunt Tool (Prototype)

1.1: Workflow: Host Discovery & Risk Assessment



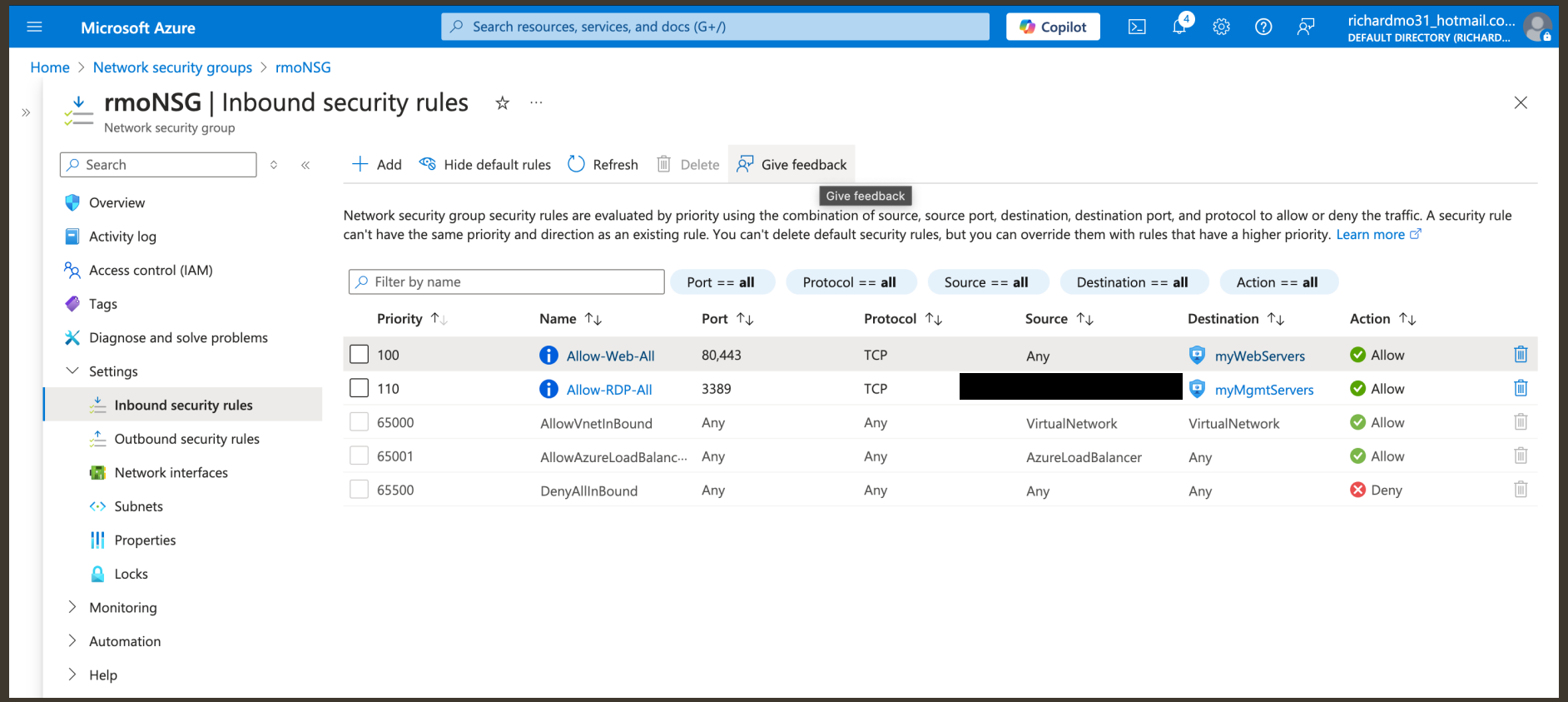
- **Language:** Python
- **Product Type:** Security Assessment Tool (Prototype)

1.2: Workflow: KeyVault

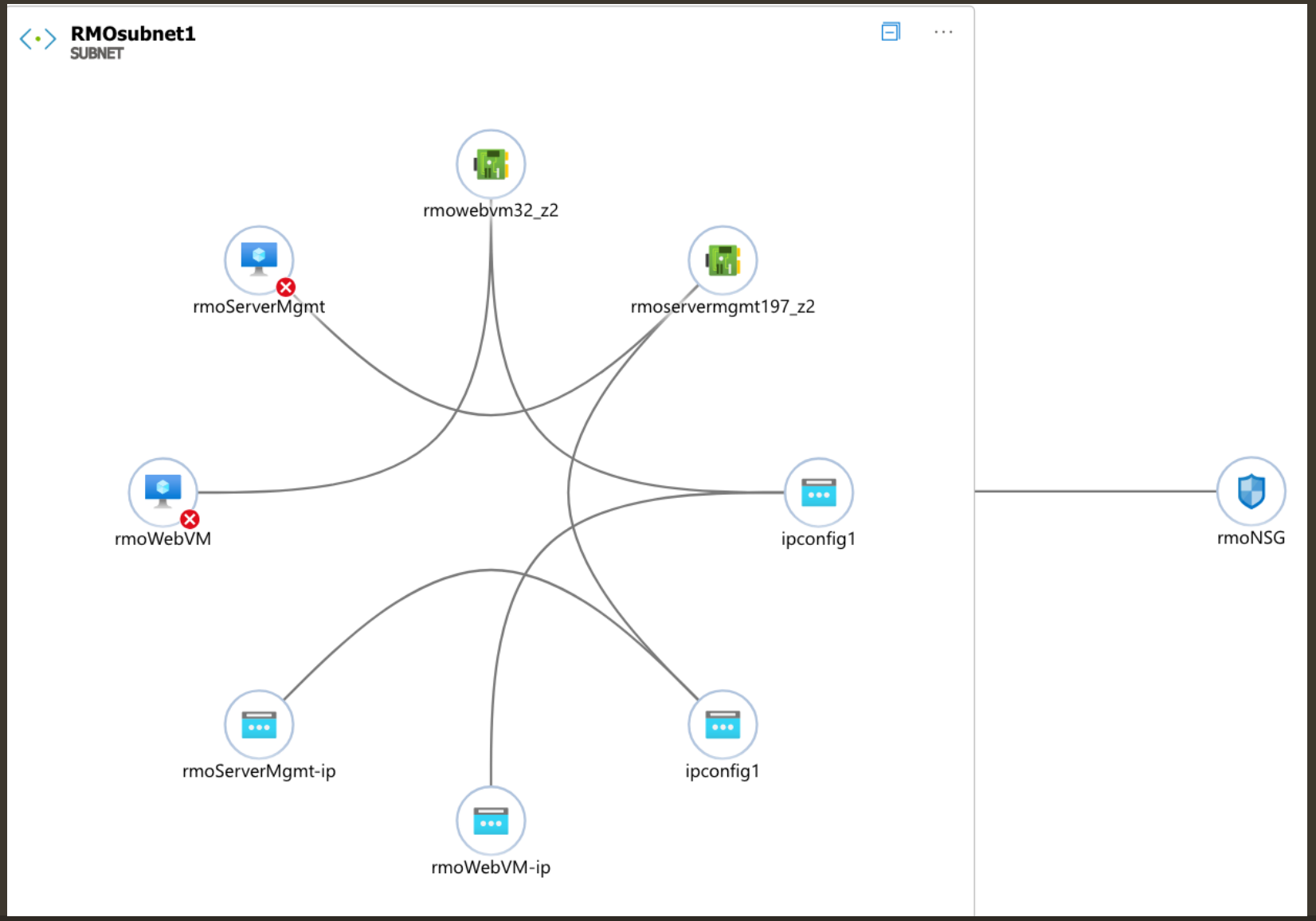


Language: Python
Product: Credential Management App (In Development)

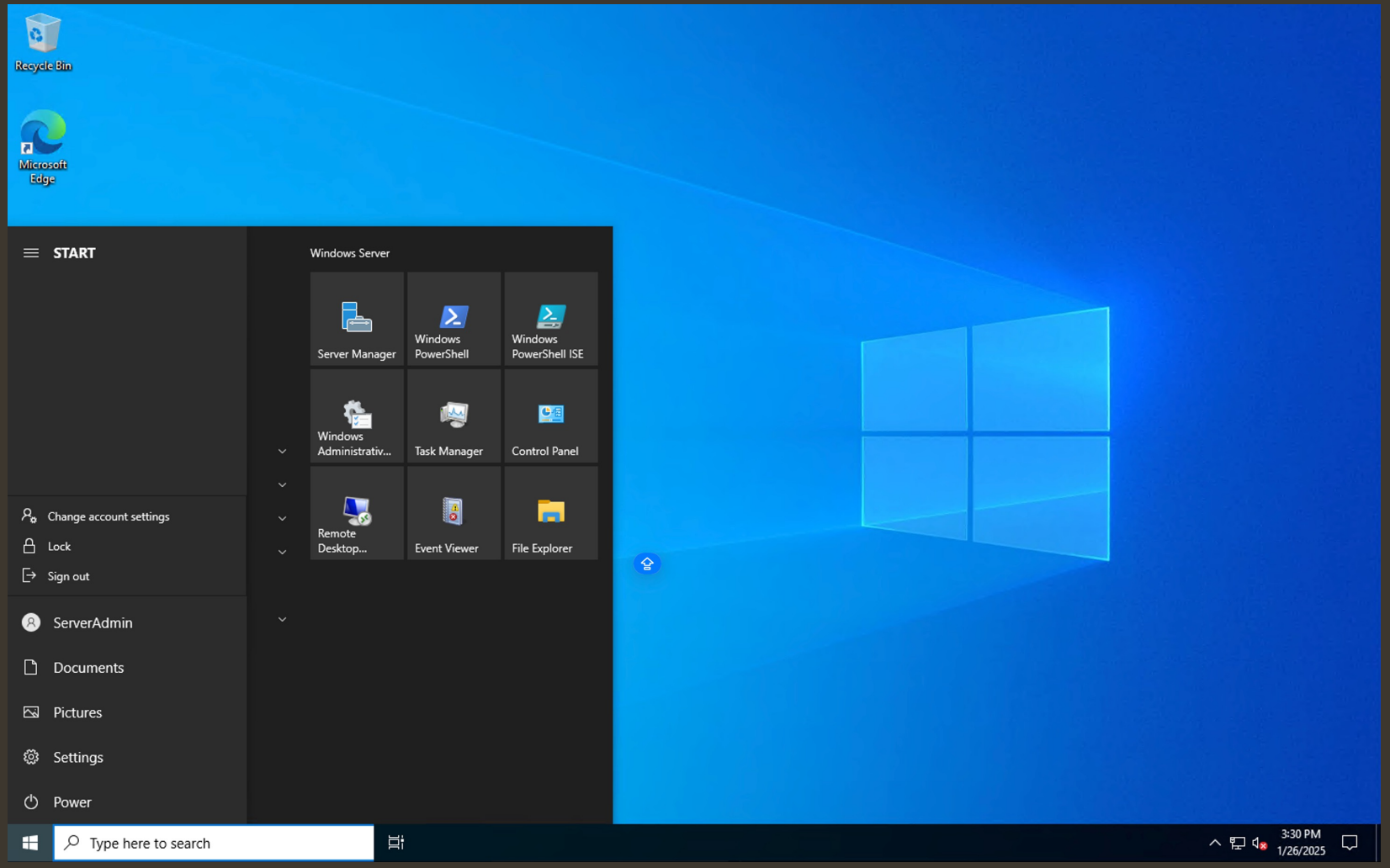
1.3: Network Security Groups for Azure Resources



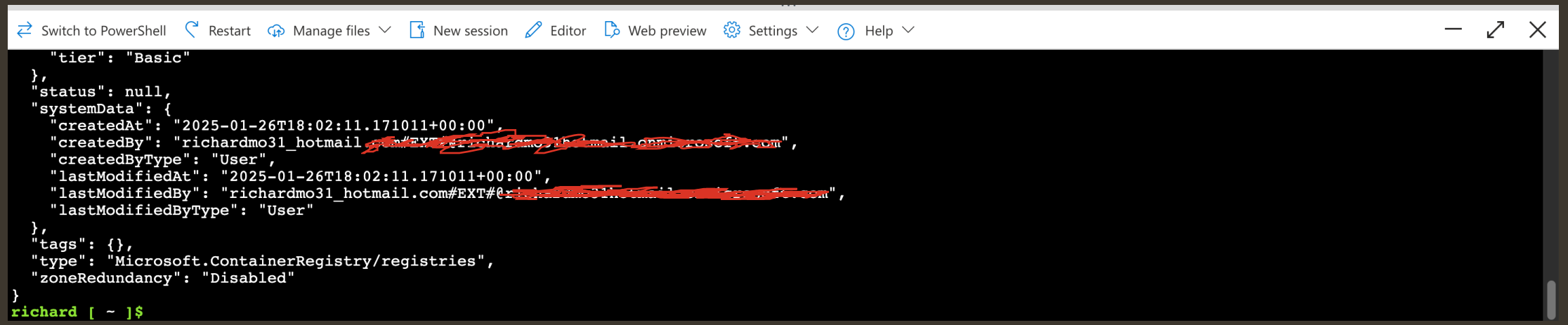
1.4: Network Architecture – RMO Cloud Instance



1.5: Jump-box to Azure Resources



1.6: Azure Container Registry



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: ca1 was successful after 15s
richard [ ~ ]$
```

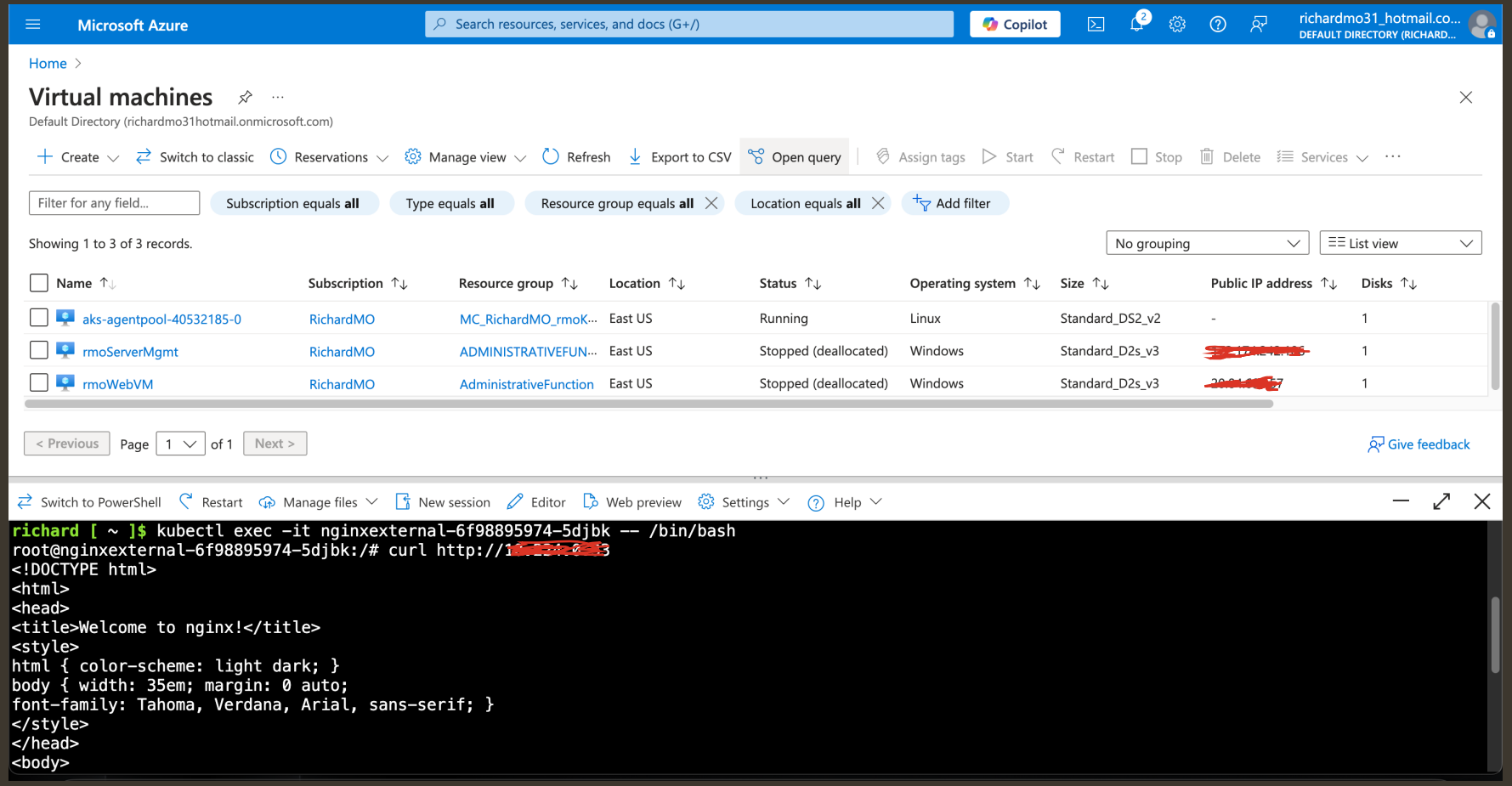
1.8: Azure Kubernetes Services - Implementation

```
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 ..
```

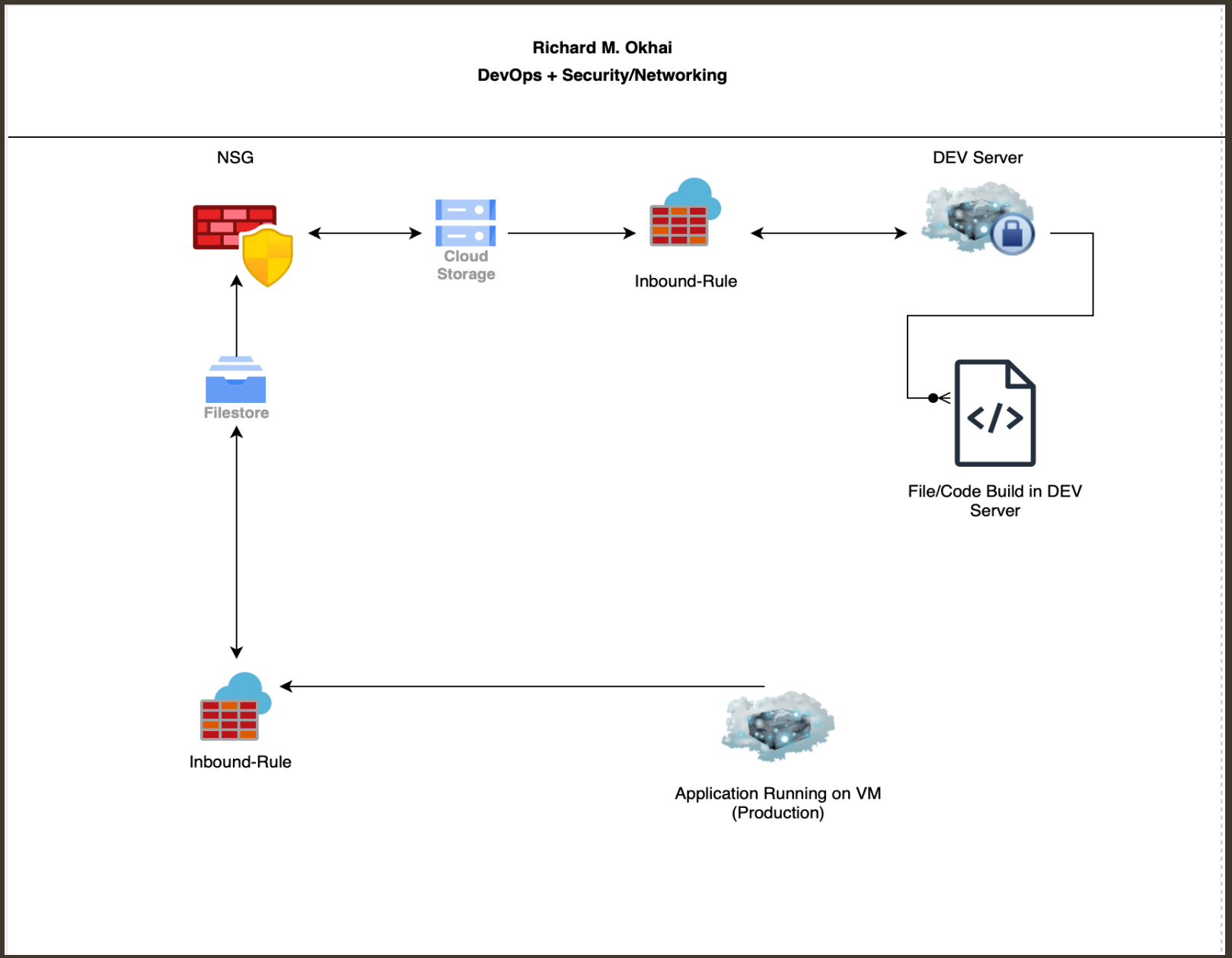
```
richard [ ~ ]$ kubectl apply -f nginxexternal.yaml
deployment.apps/nginxexternal created
service/nginxexternal created
richard [ ~ ]$
```

```
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 [ ~ ]$
```

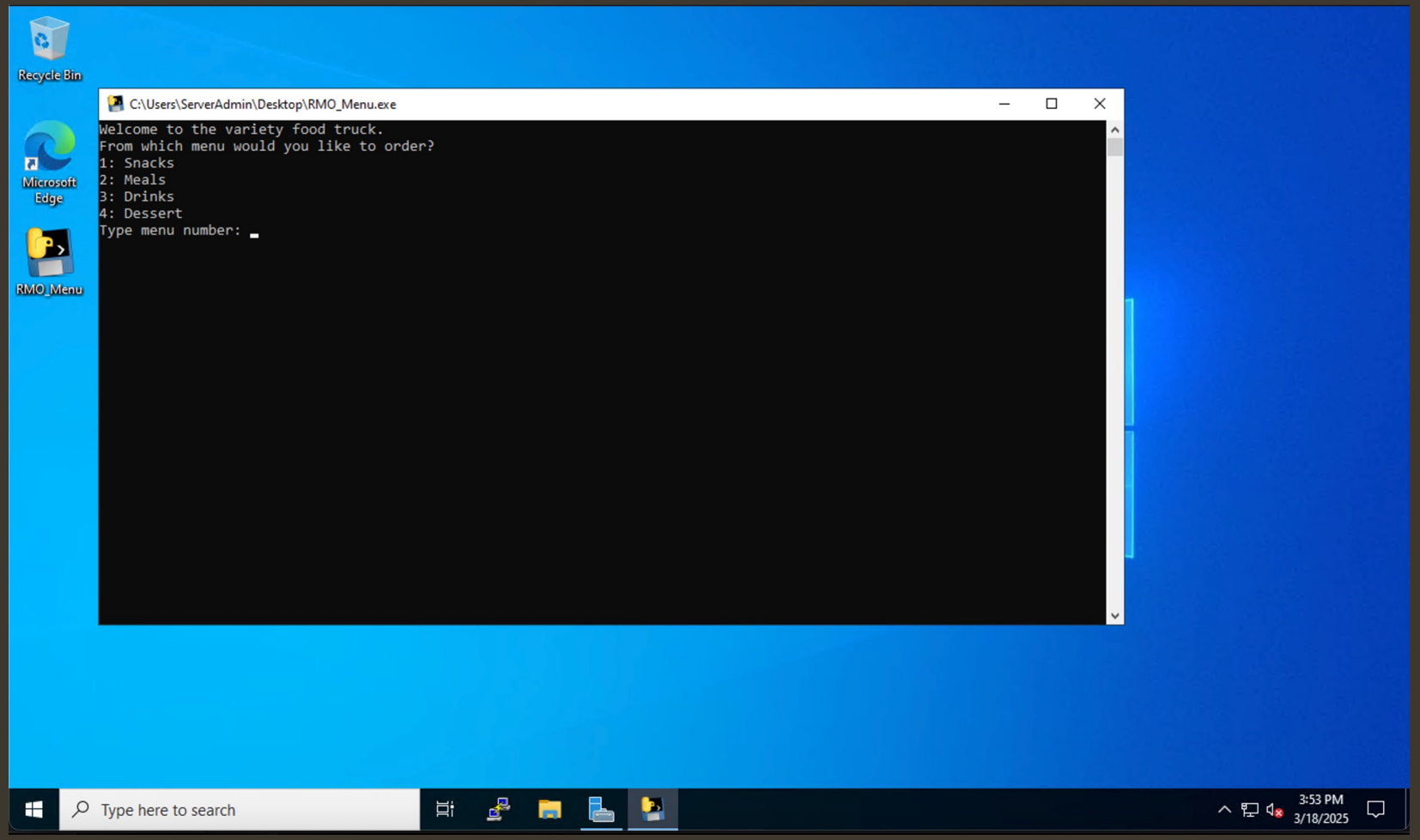
1.9: DevOps– Private Network Deployment (Web)



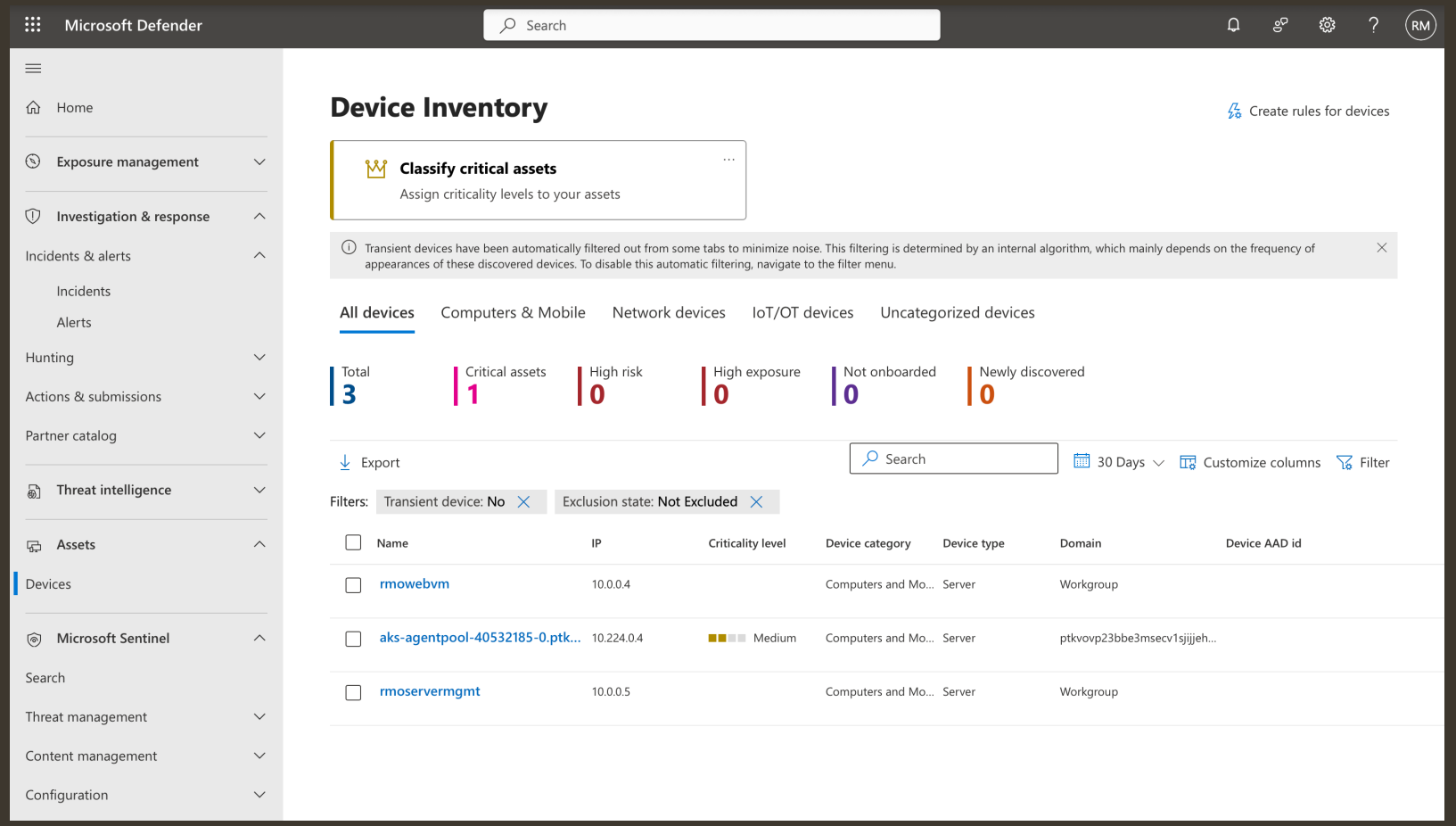
2.0: DevOps – Deployment Architecture (Packaged Application)



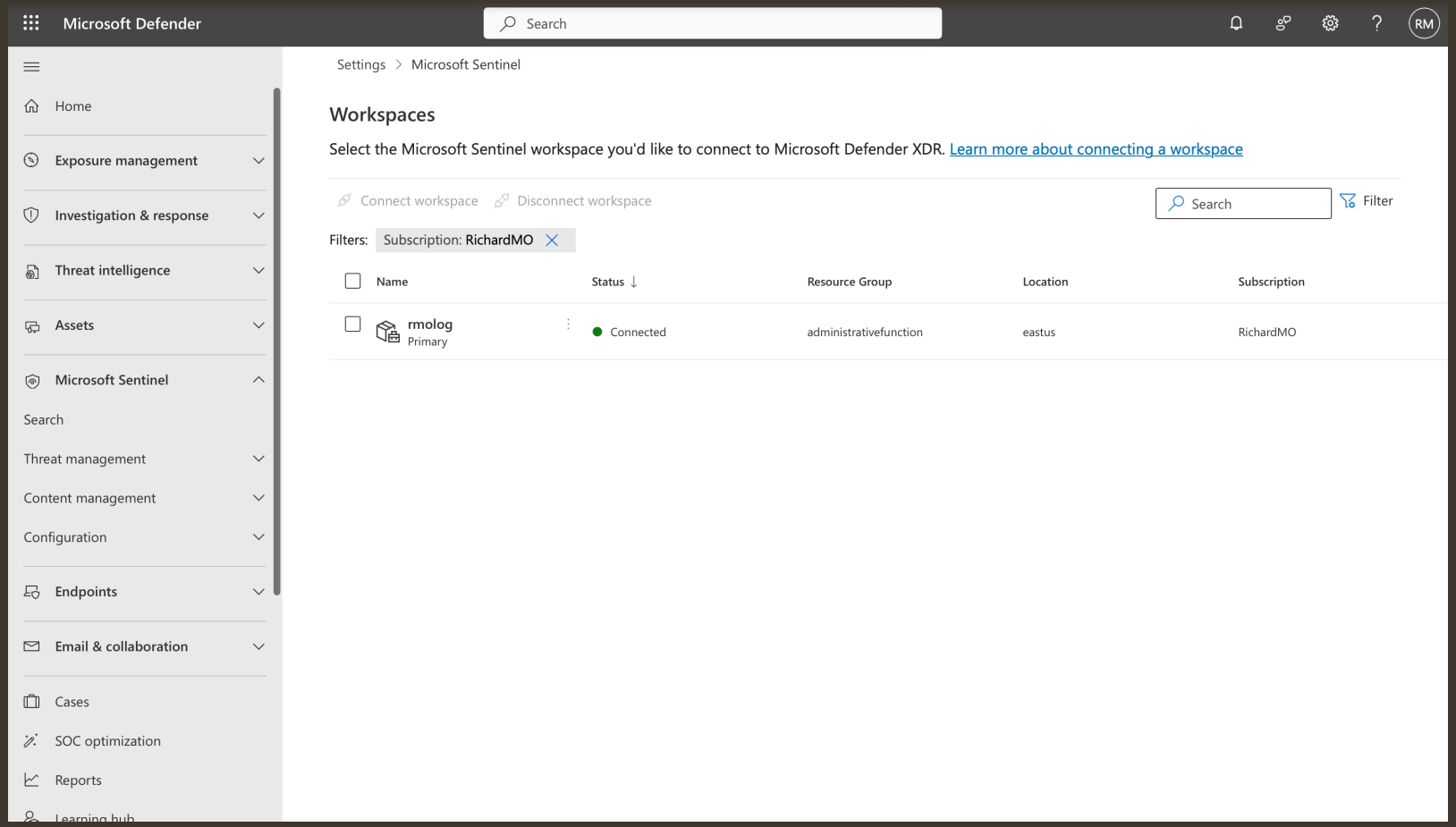
2.1: Packaged Application – Production Endpoint



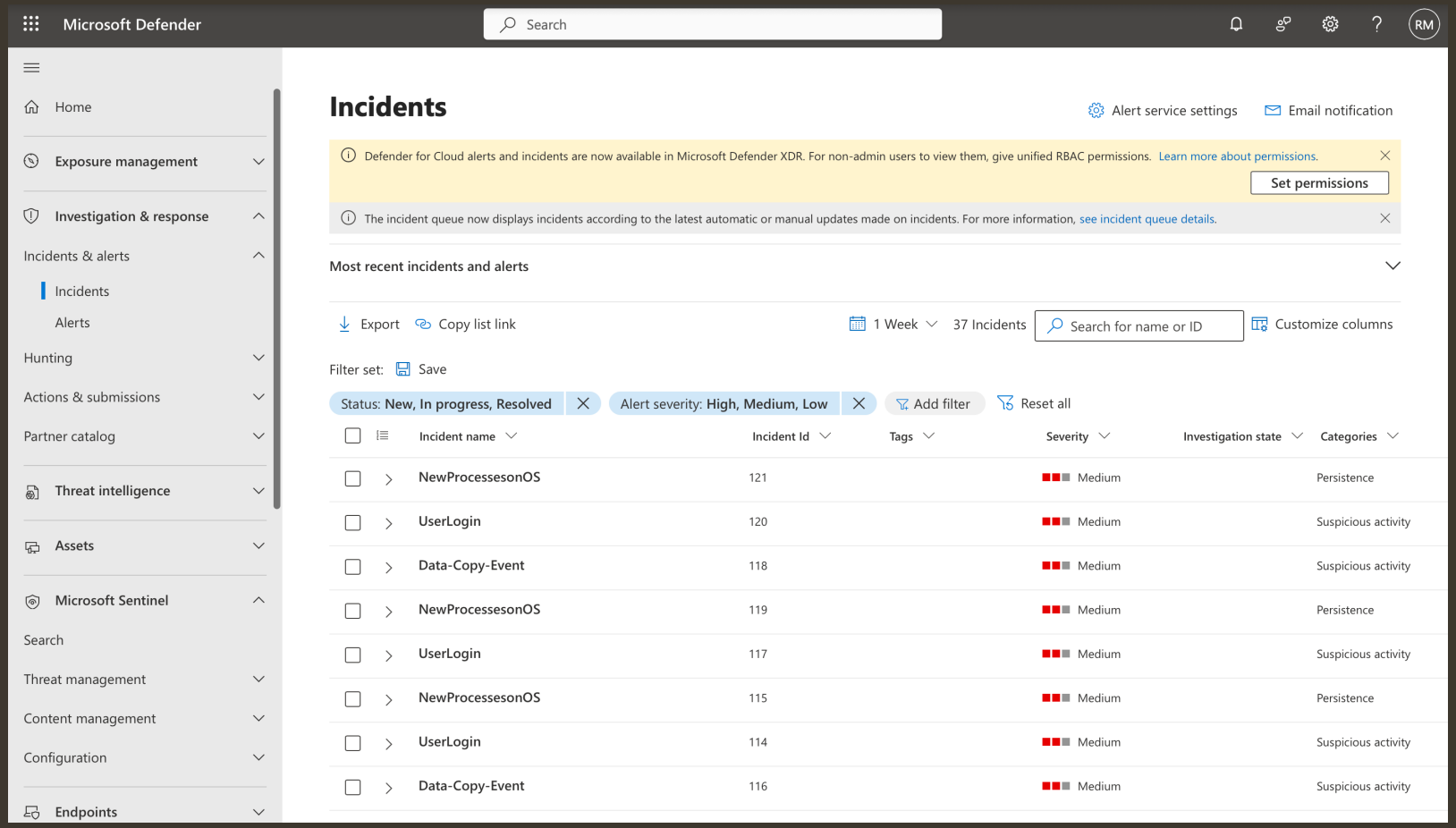
2.2: Endpoint Detection (Microsoft Defender XDR) – Server and AKS



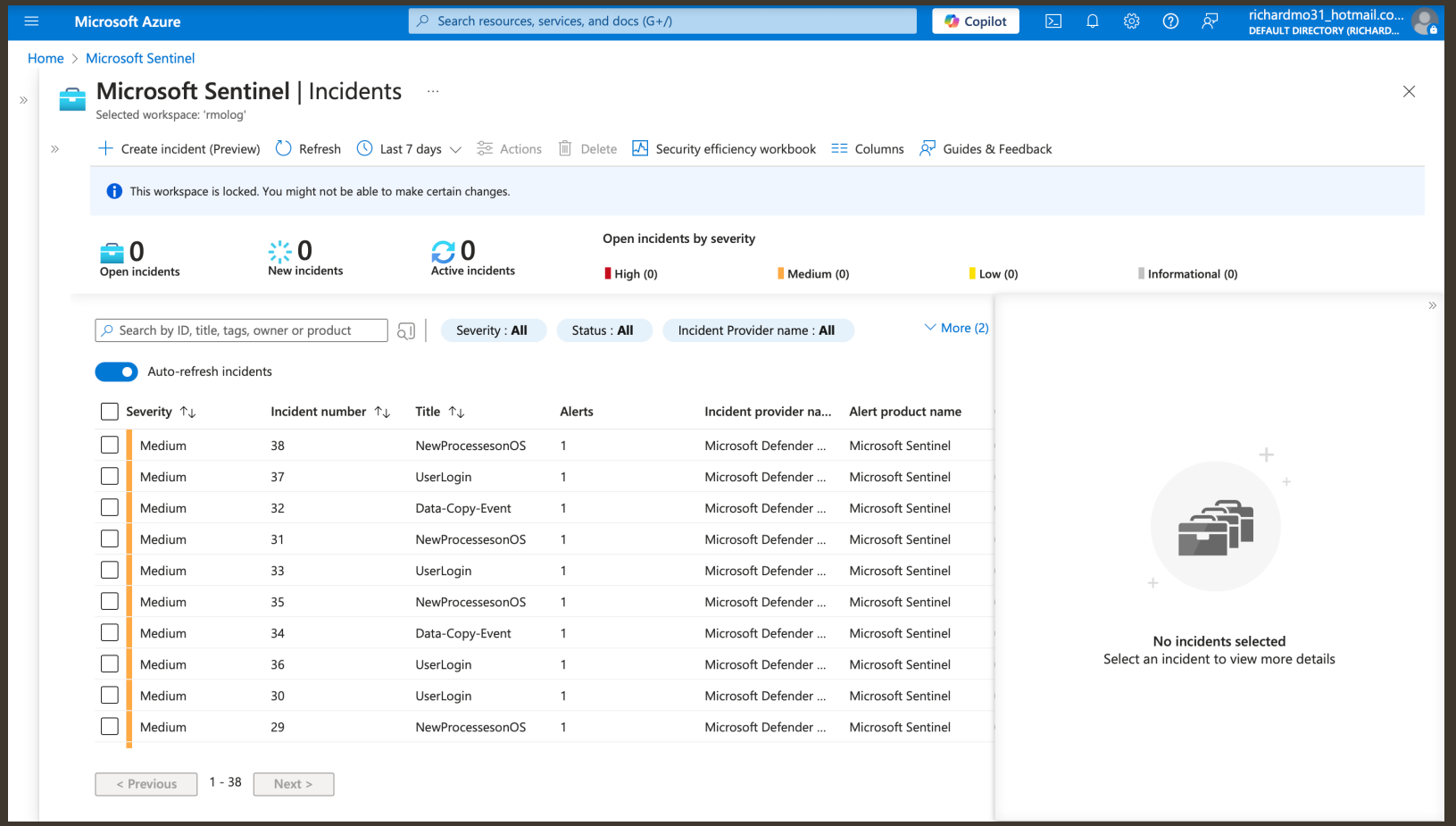
2.3: Endpoint Detection – Connection with M.S Sentinel (SIEM)



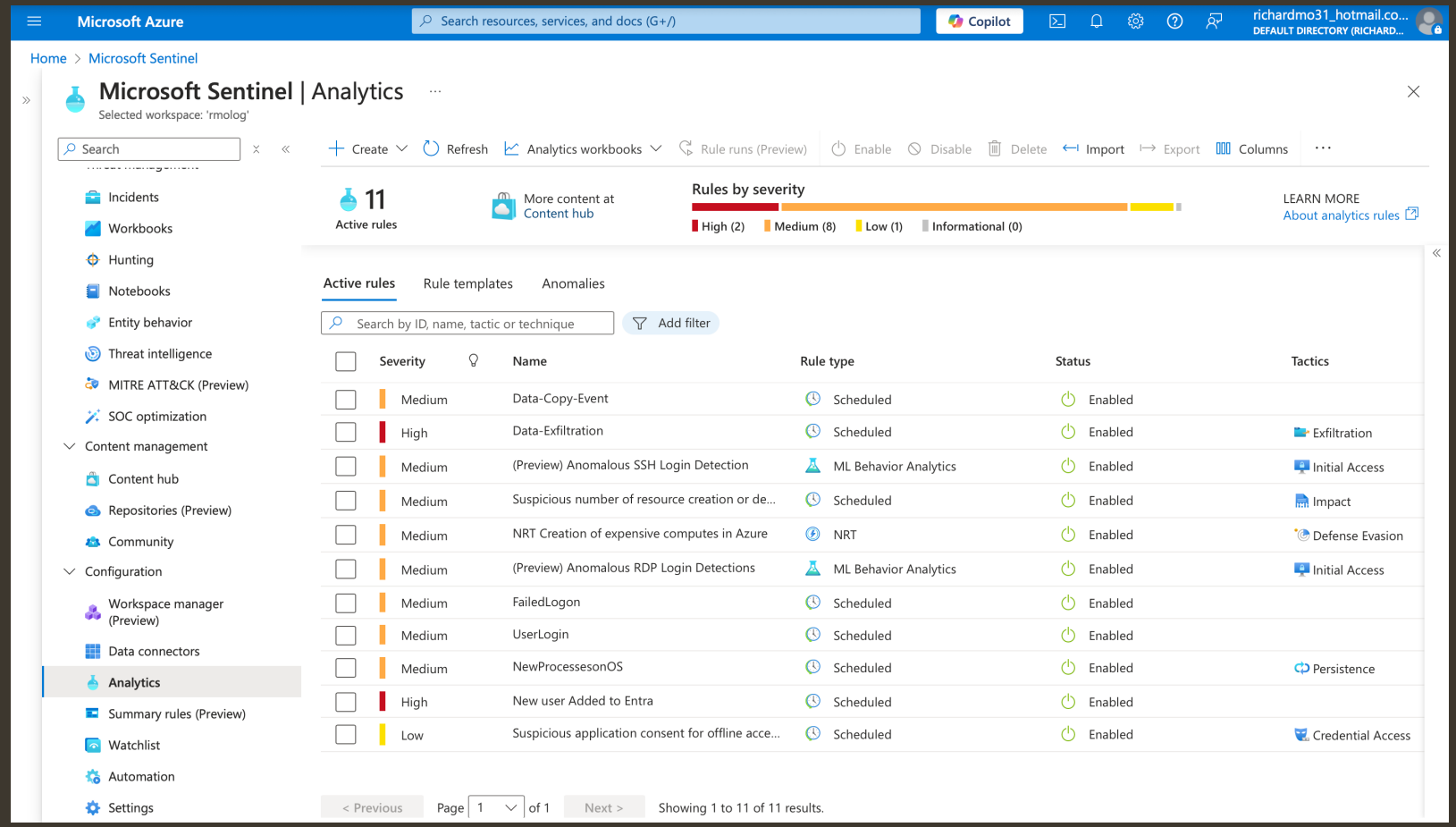
2.4: Endpoint Detection – Escalated Incident (Active Rule)



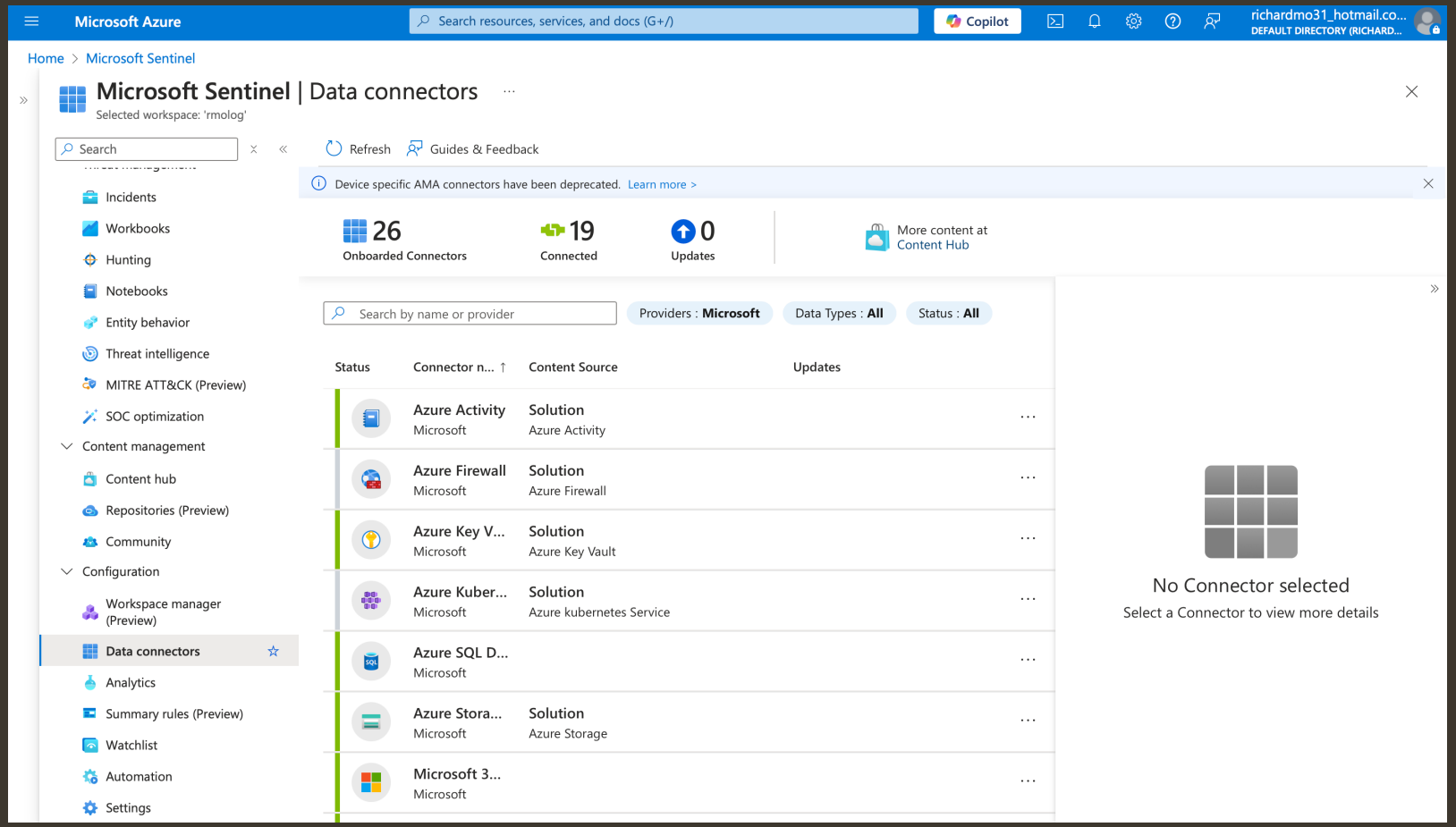
2.5: Continuous Monitoring (Endpoints)



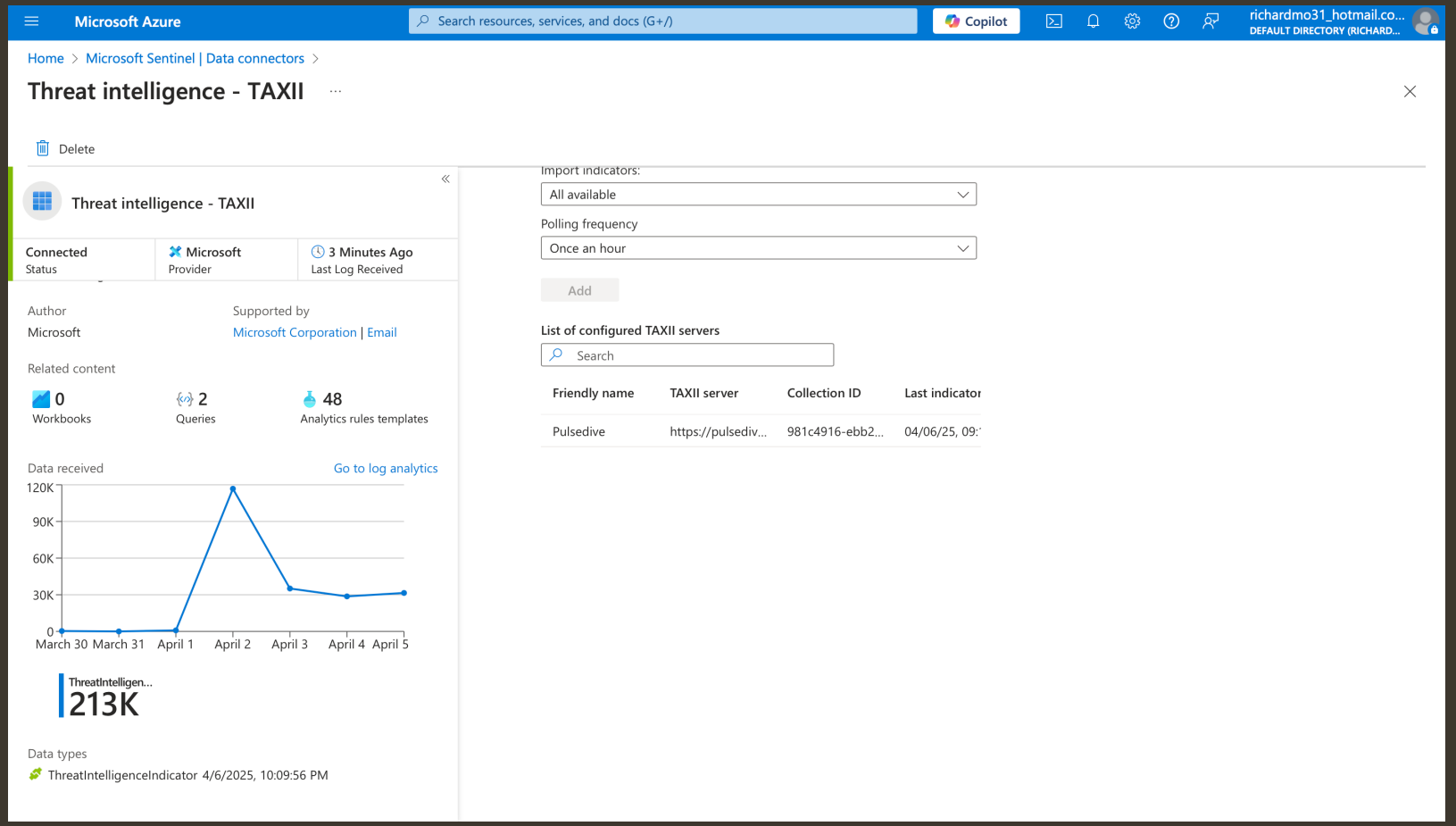
2.6: Continuous Monitoring – Analytics (Implemented Rules)



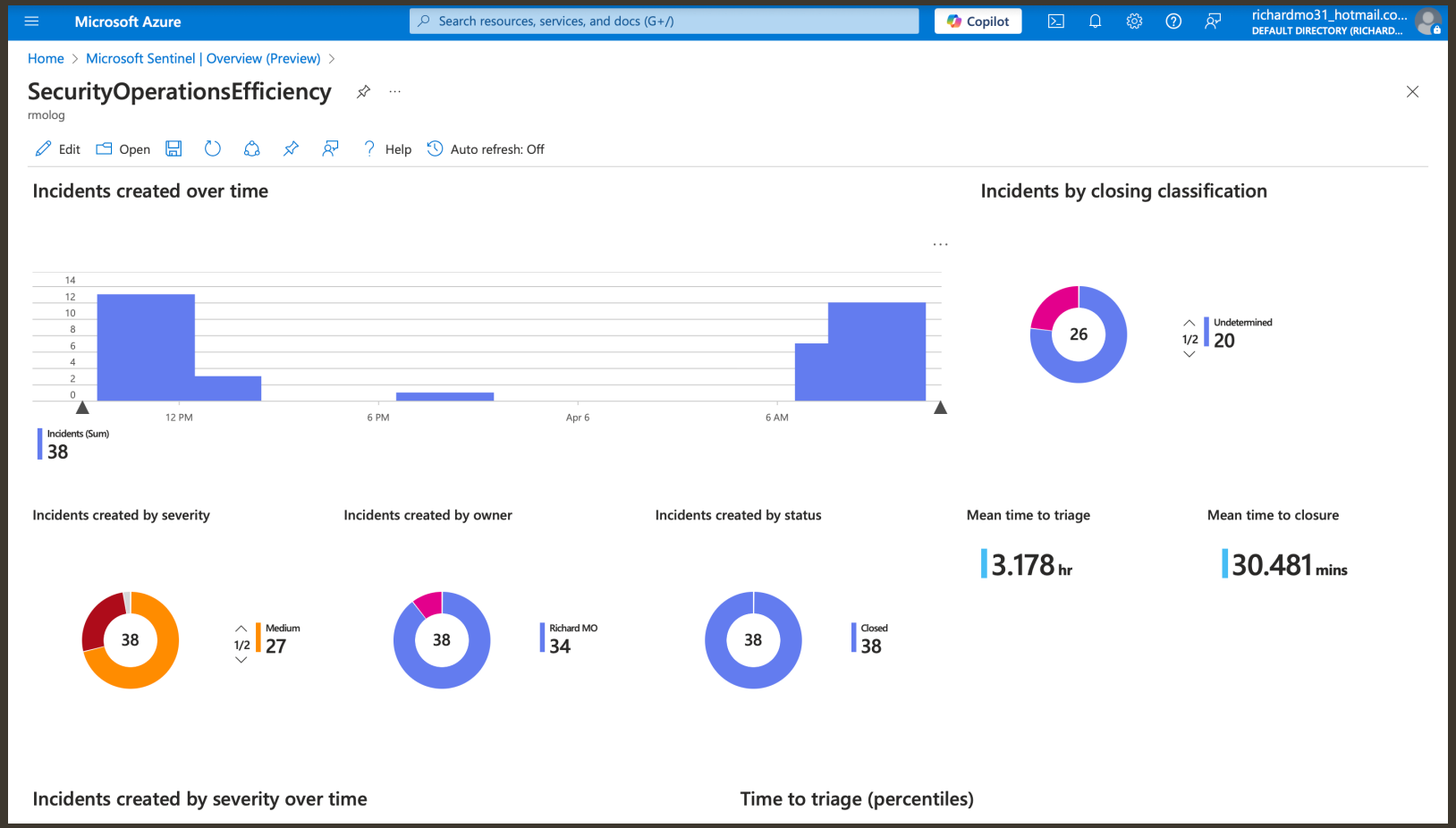
2.7: Continuous Monitoring – Connected Data Source



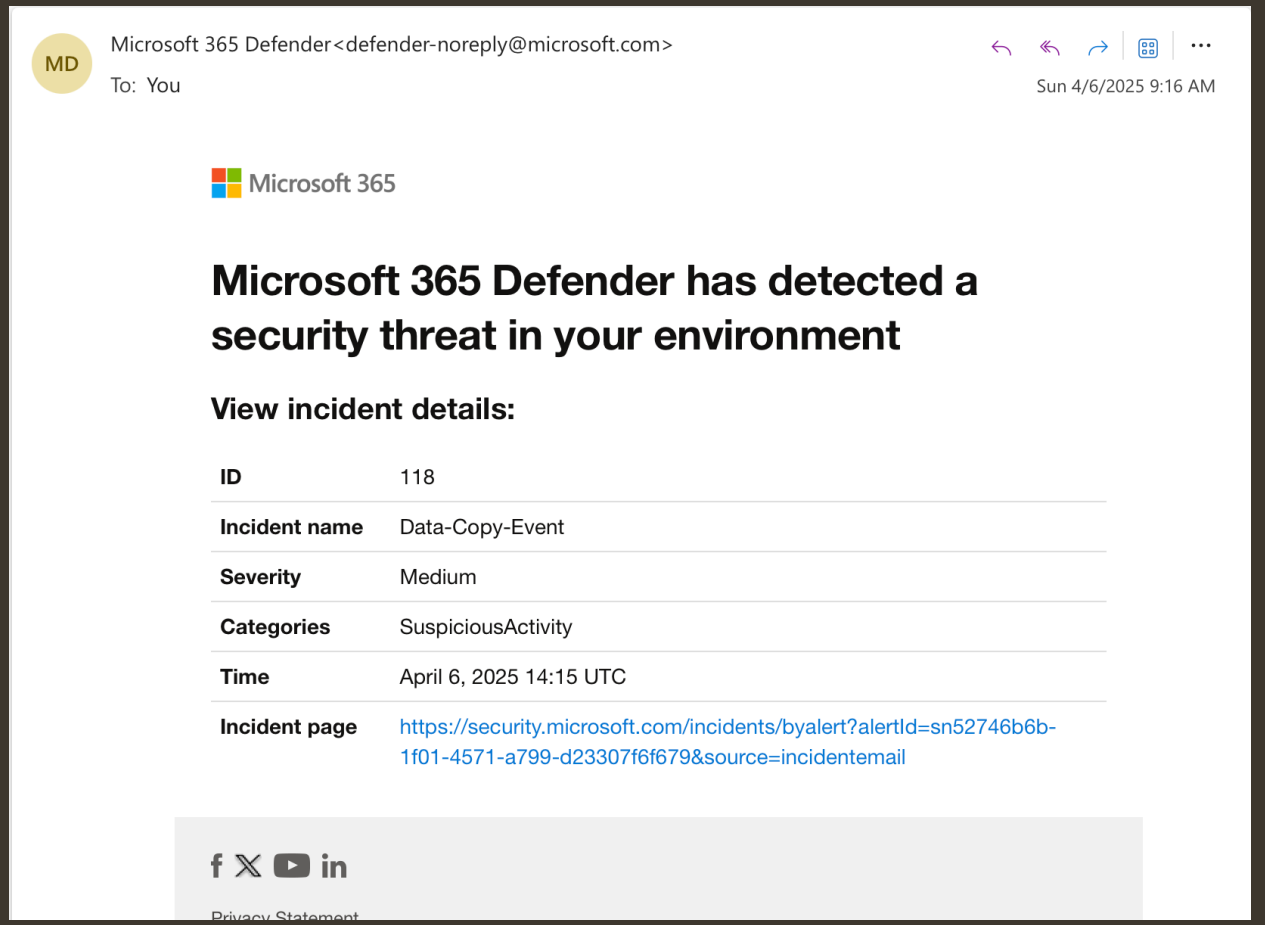
2.8: Continuous Monitoring – Additional External Threat Intelligence



2.9: Continuous Monitoring – Security Operations Efficiency



3.0: Continuous Monitoring – Incident Escalated



MD

Microsoft 365 Defender<defender-noreply@microsoft.com>

To: You

Sun 4/6/2025 9:16 AM

Microsoft 365

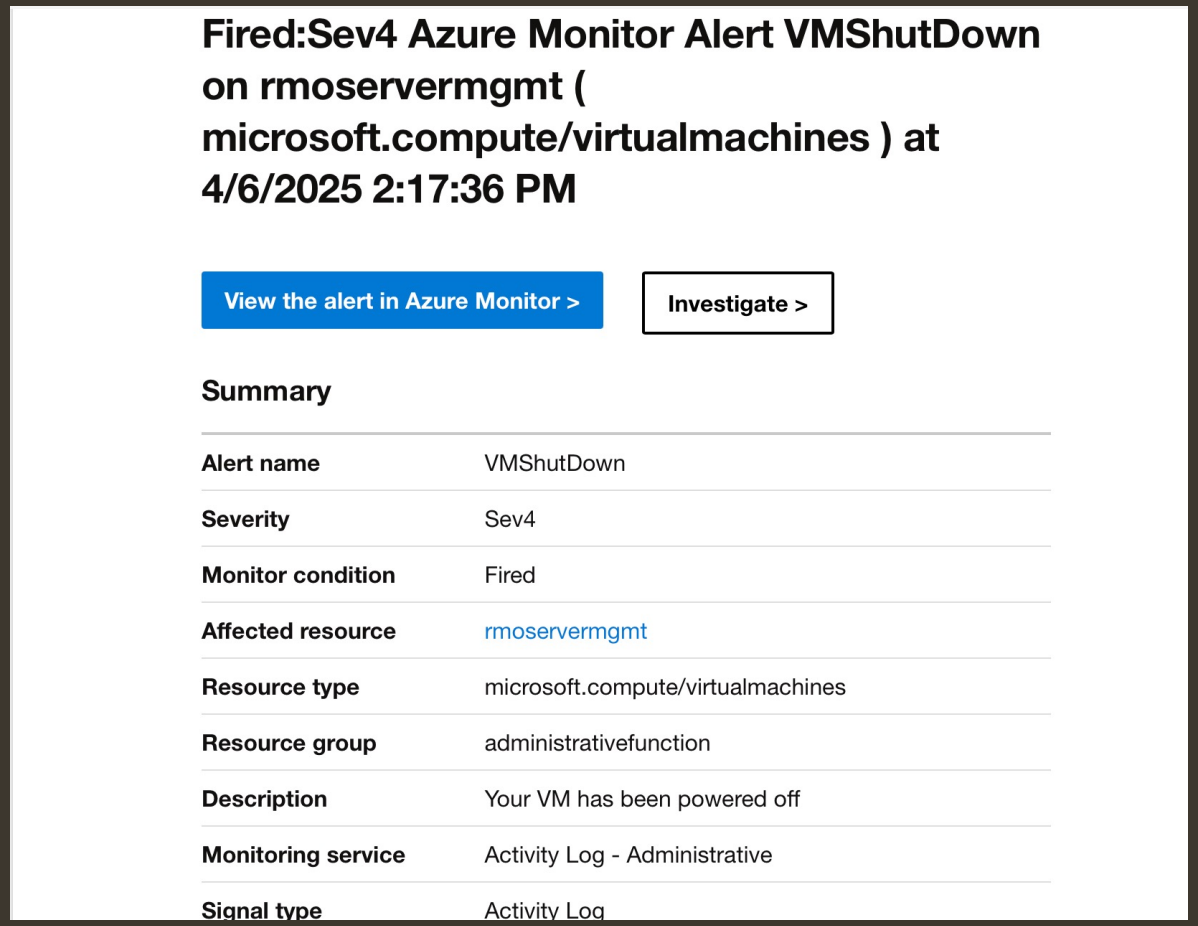
Microsoft 365 Defender has detected a security threat in your environment

View incident details:

ID	118
Incident name	Data-Copy-Event
Severity	Medium
Categories	SuspiciousActivity
Time	April 6, 2025 14:15 UTC
Incident page	https://security.microsoft.com/incidents/byalert?alertId=sn52746b6b-1f01-4571-a799-d23307f6f679&source=incidentemail

Privacy Statement

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

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

3.2: Security - Defense-in-depth Design