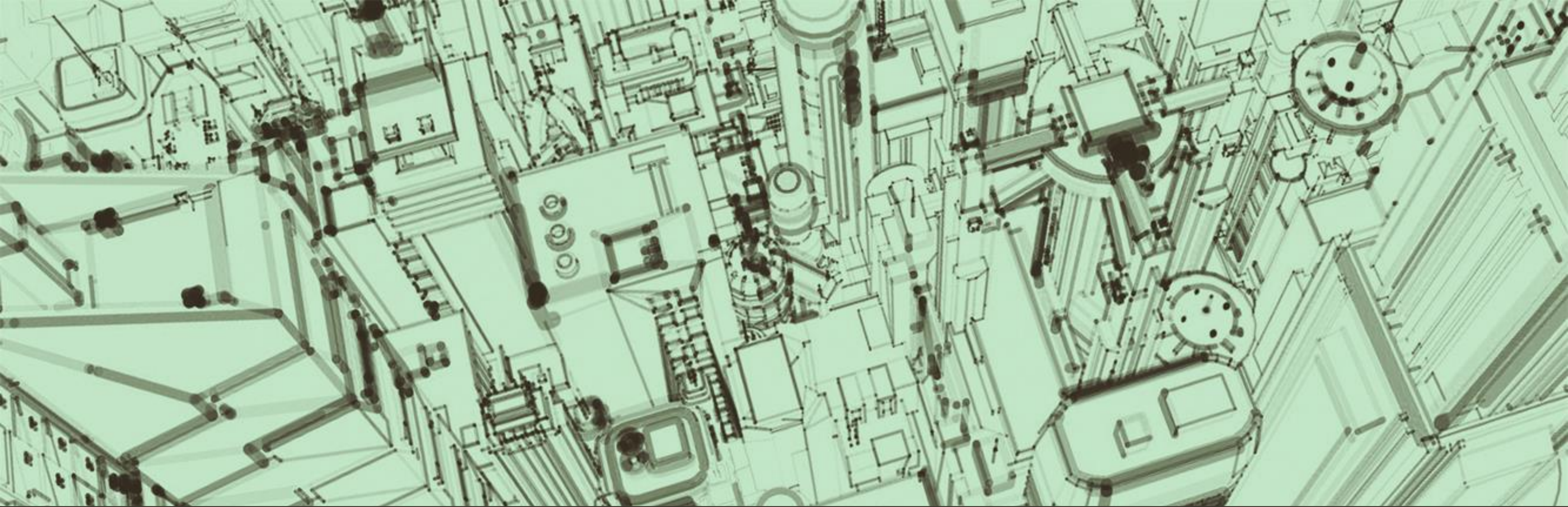


Richard M. Okhai

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.

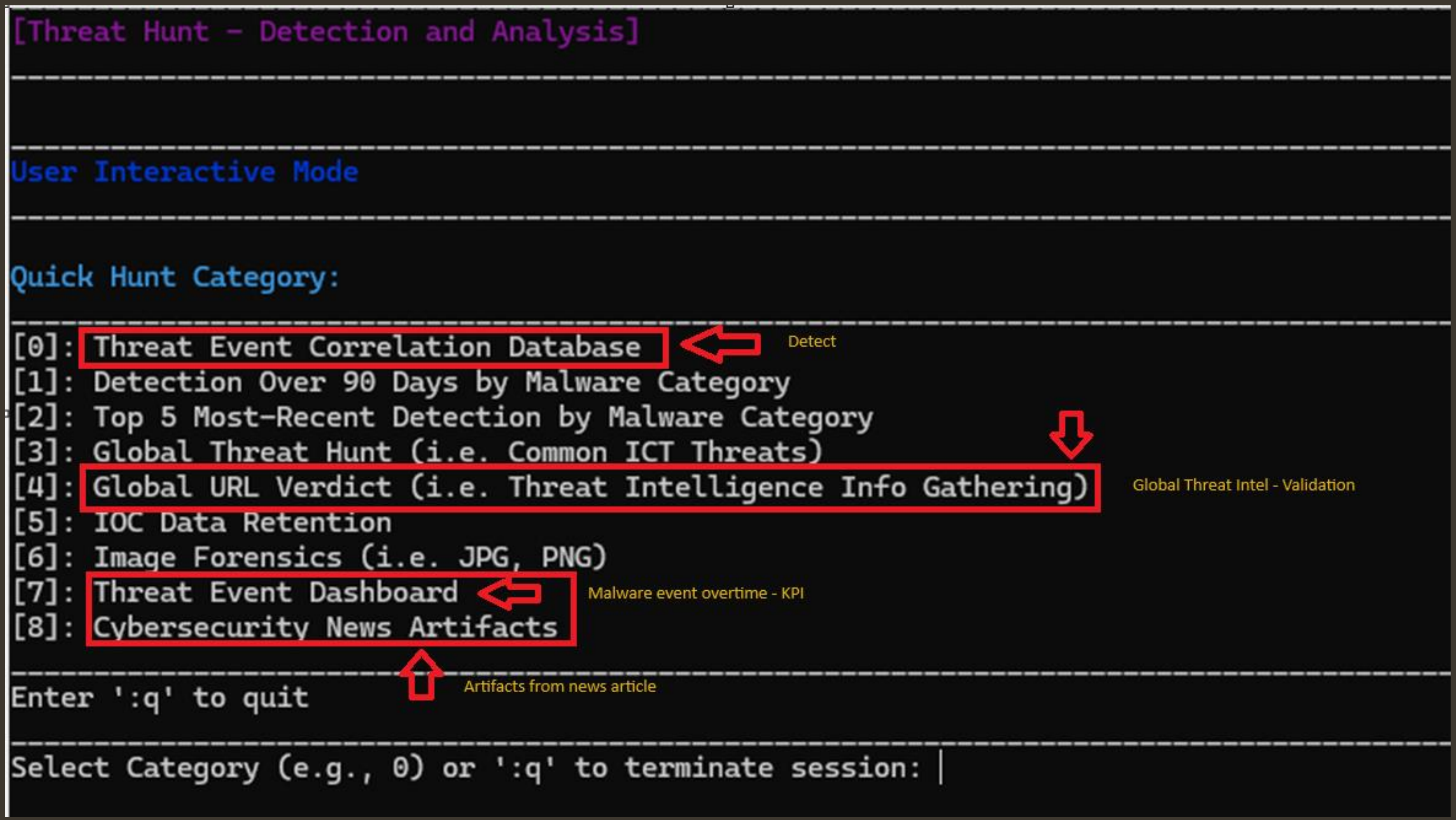
Competitive Intelligence – Supply Chain & Program Modernization

- 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



```
[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:
```

Detect

Global Threat Intel - Validation

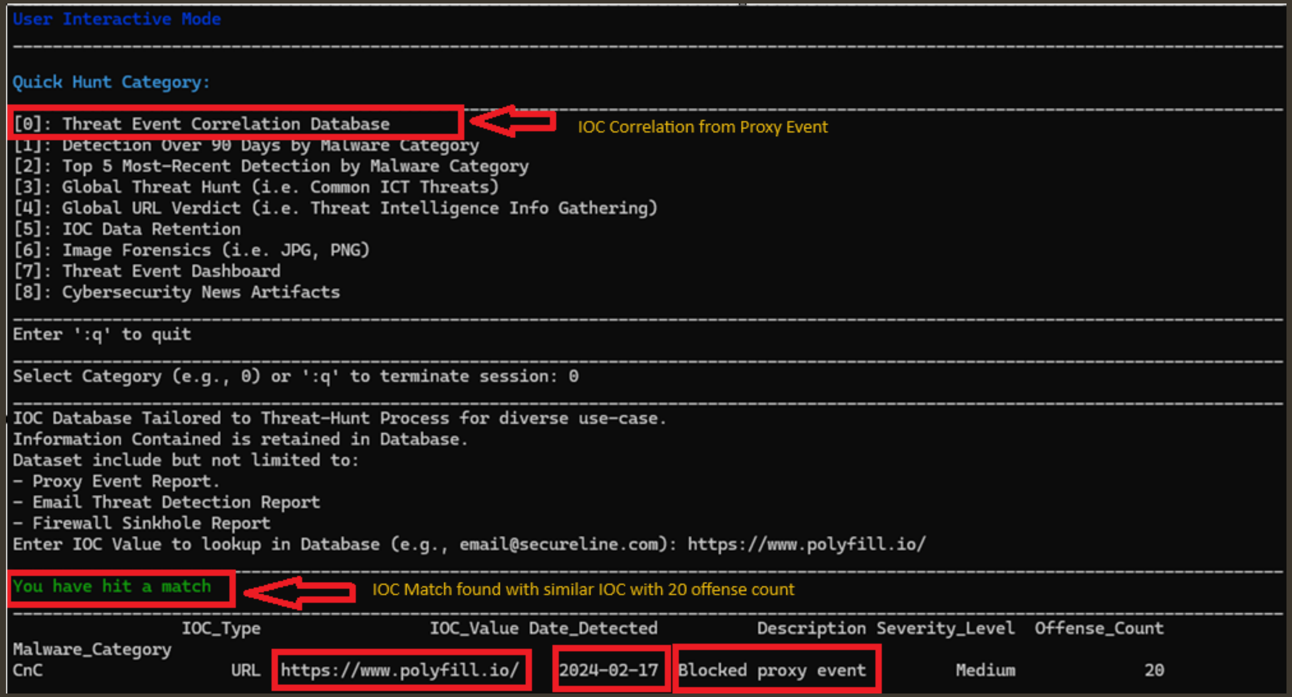
Malware event overtime - KPI

Artifacts from news article

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



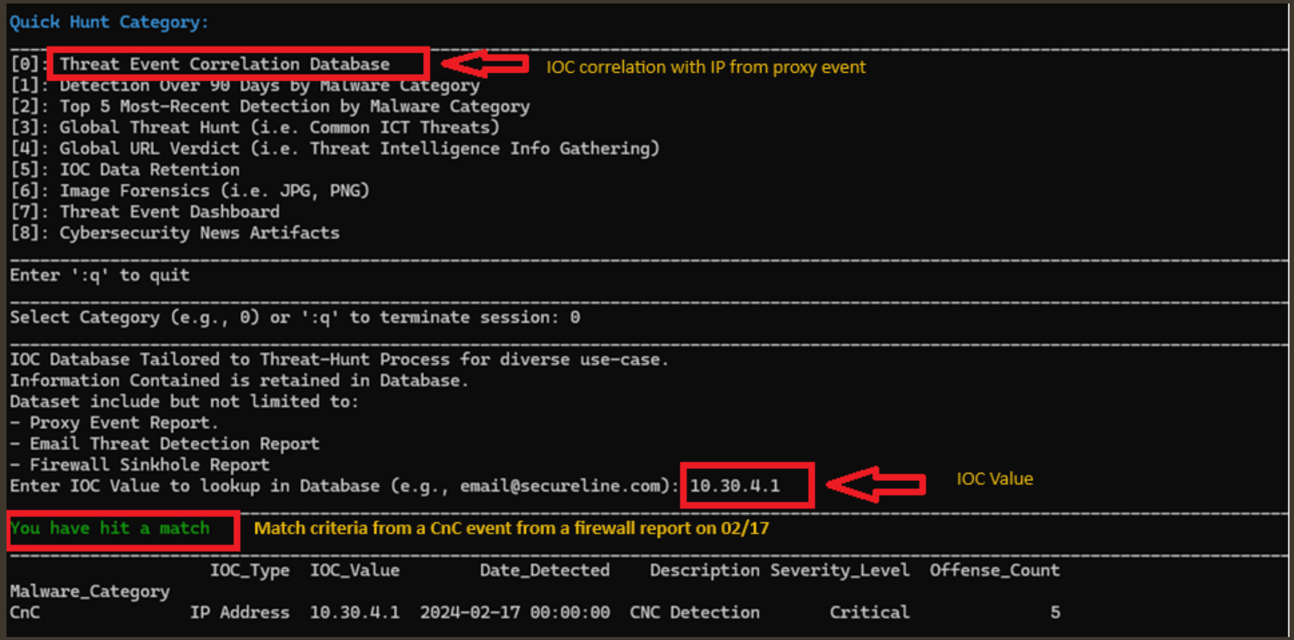
```
User Interactive Mode
--------------------------------------------------------------------------------------------------------------------------------
Quick Hunt Category:
--------------------------------------------------------------------------------------------------------------------------------
[0]: Threat Event Correlation Database
[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_Type                 IOC_Value Date_Detected          Description Severity_Level  Offense_Count
Malware_Category
CnC                   URL  https://www.polyfill.io/   2024-02-17  Blocked proxy event          Medium             20
```

IOC Correlation from Proxy Event

IOC Match found with similar IOC with 20 offense count

- **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
[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
--------------------------------------------------------------------------------------------------------------------------------
You have hit a match
--------------------------------------------------------------------------------------------------------------------------------
                    IOC_Type  IOC_Value        Date_Detected    Description Severity_Level  Offense_Count
Malware_Category
CnC                IP Address  10.30.4.1  2024-02-17 00:00:00  CNC Detection        Critical              5
```

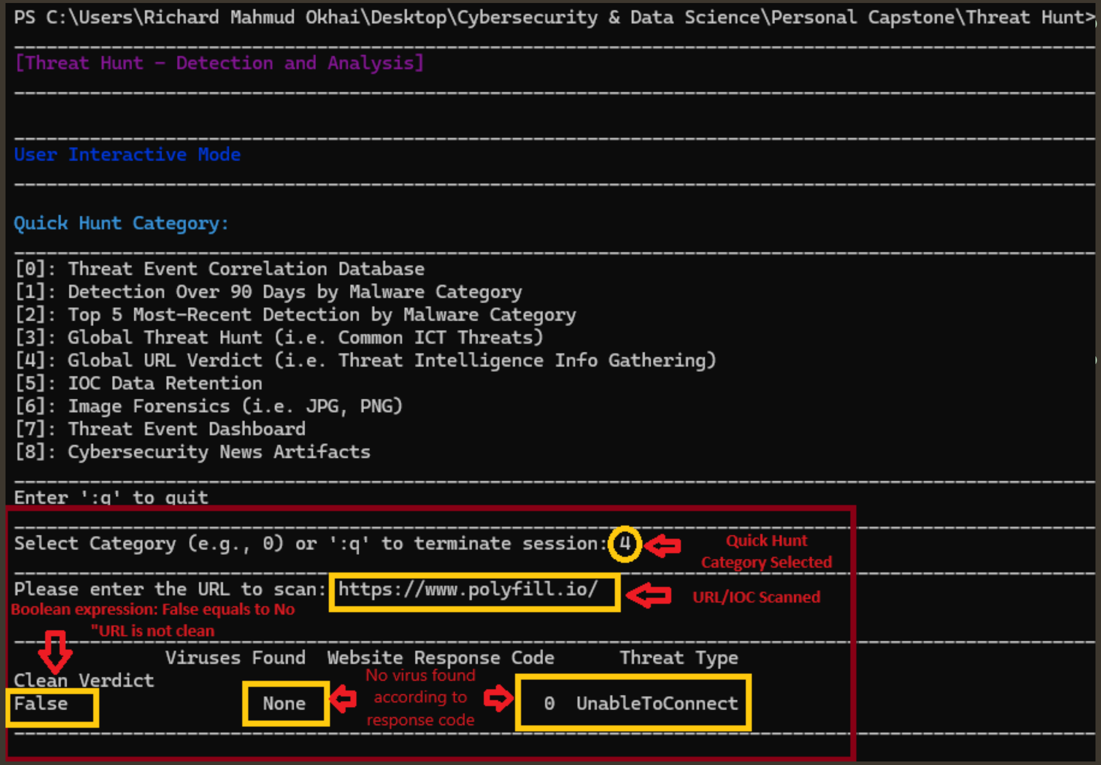
IOC correlation with IP from proxy event

IOC Value

Match criteria from a CnC event from a firewall report on 02/17

- **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
--------------------------------------------------------------------------------------------------
Please enter the URL to scan: https://www.polyfill.io/
--------------------------------------------------------------------------------------------------
              Viruses Found  Website Response Code      Threat Type
Clean Verdict
False                 None                          0  UnableToConnect
--------------------------------------------------------------------------------------------------
```

Quick Hunt Category Selected

URL/IOC Scanned

Boolean expression: False equals to No "URL is not clean

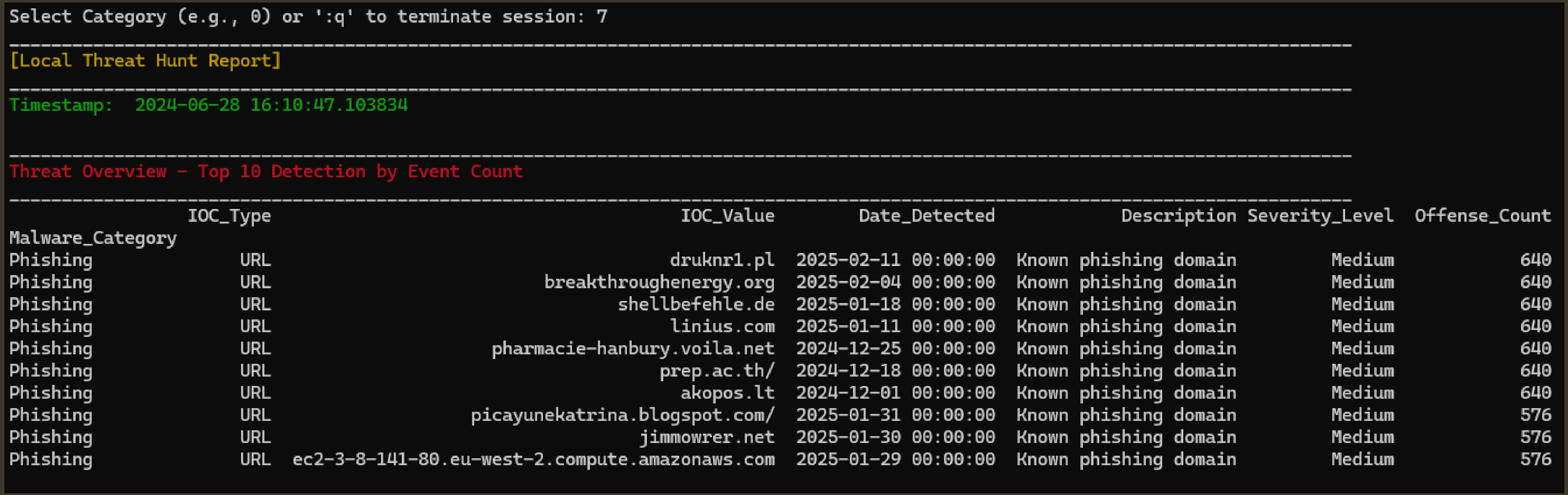
No virus found according to response code

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**”).

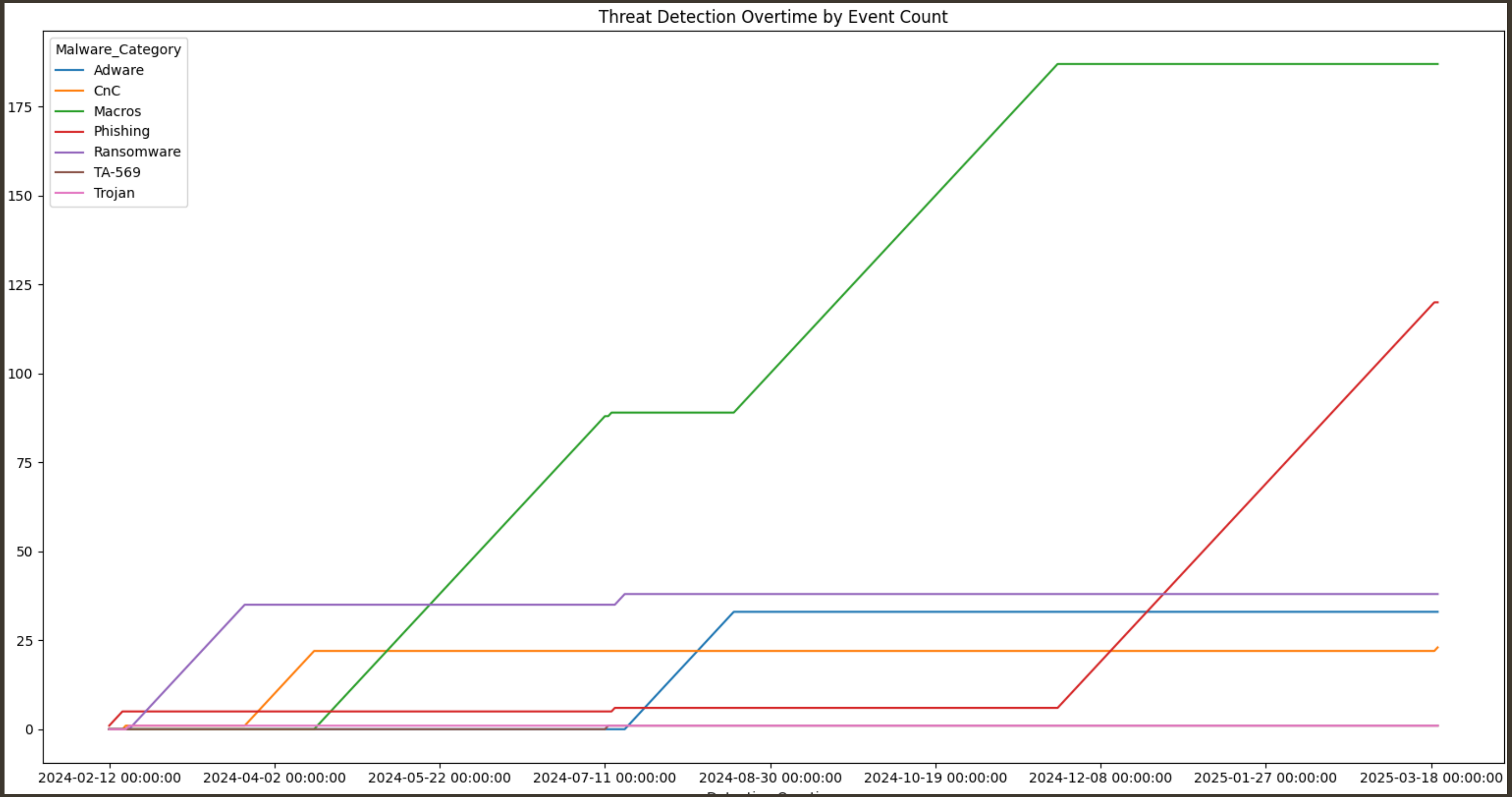
1.4: Incident Response & Malware Forensics

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



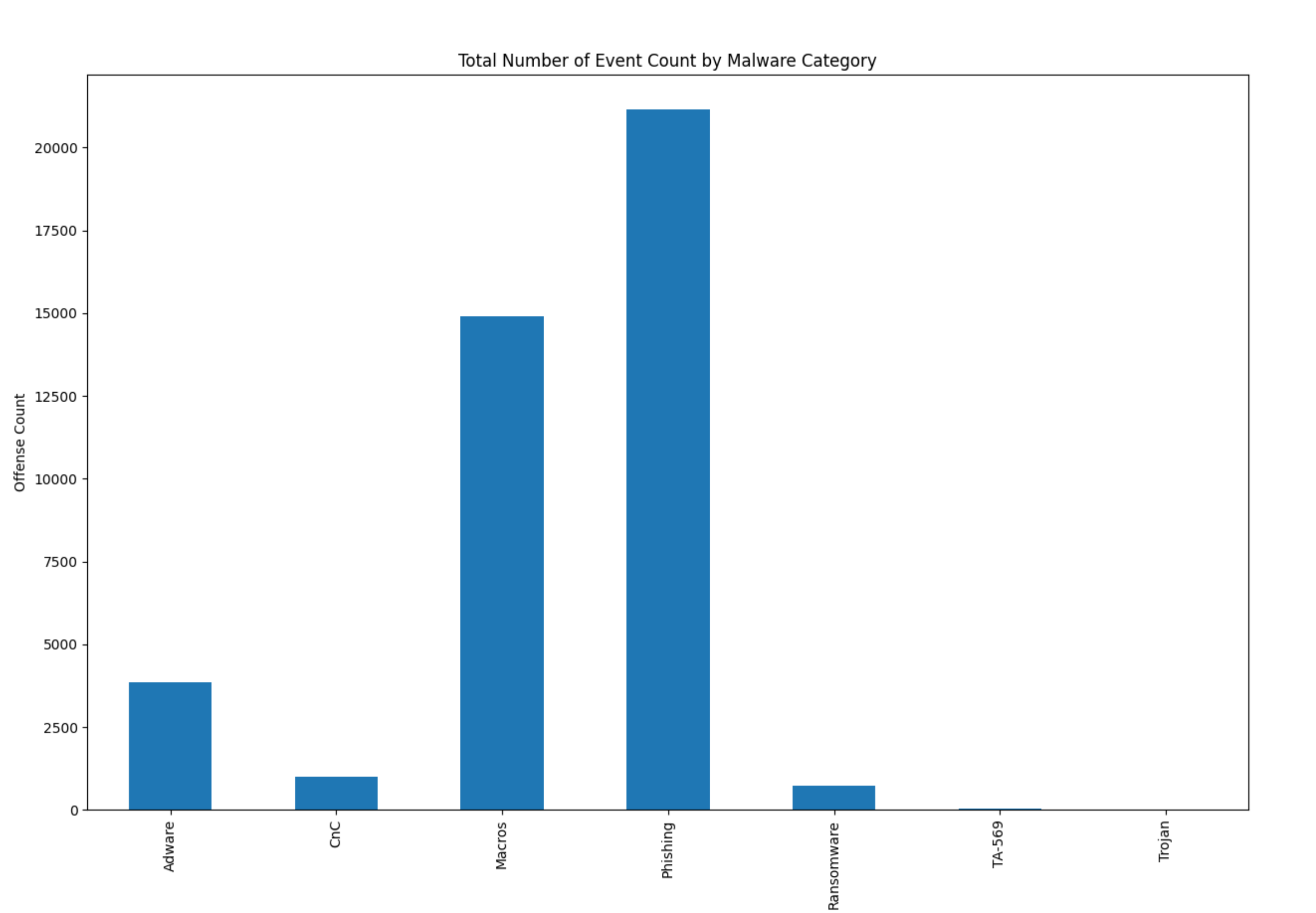
```
Select Category (e.g., 0) or ':q' to terminate session: 7
--------------------------------------------------------------------------------------------------------------------------------
[Local Threat Hunt Report]
--------------------------------------------------------------------------------------------------------------------------------
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


Threat Detection Overtime by Event Count

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

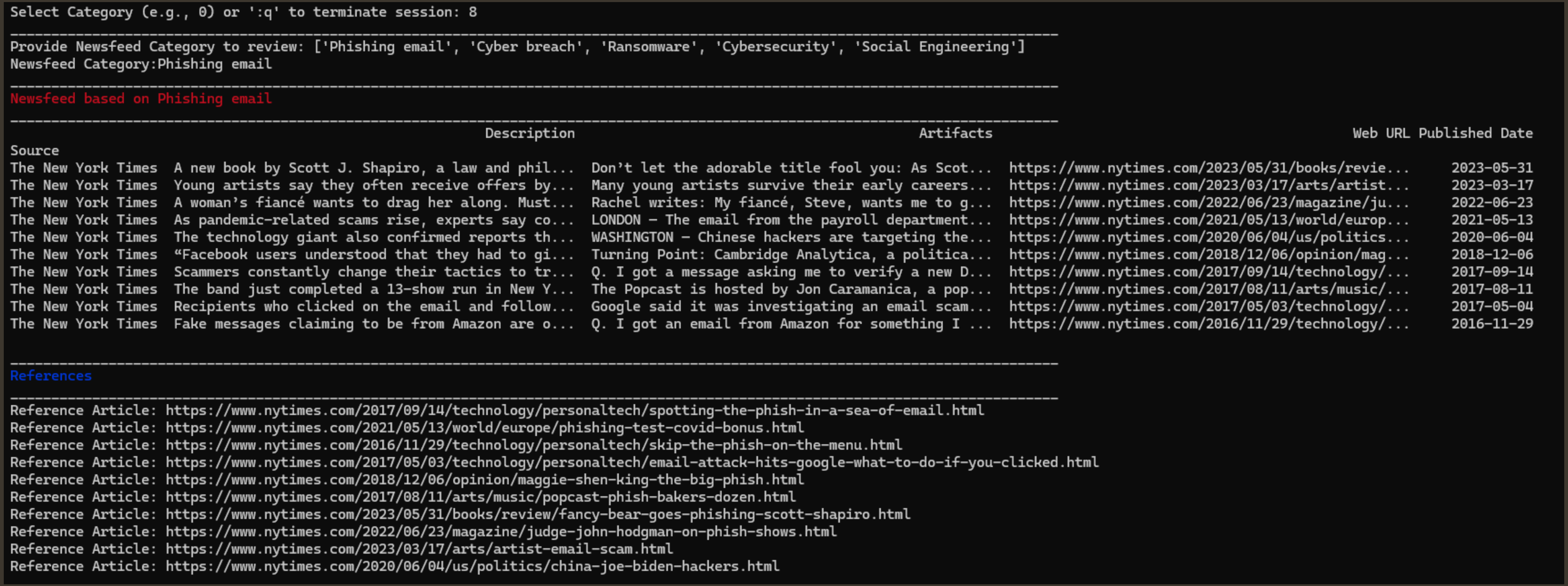
1.5: Incident Response & Malware Forensics



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

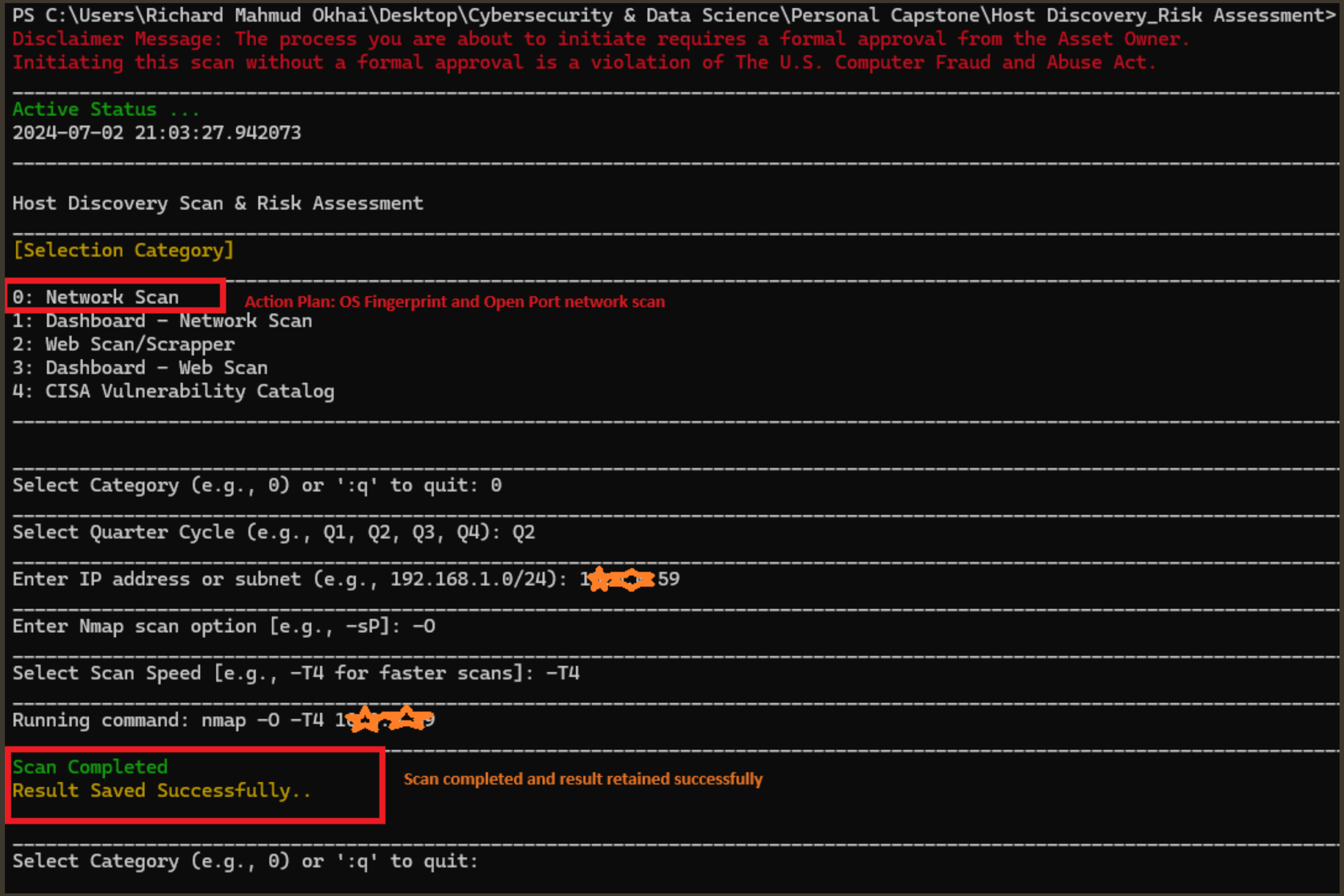
1.6: Incident Response & Malware Forensics

- **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



```
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
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): [redacted]

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

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

--------------------------------------------------------------------------------
Running command: nmap -O -T4 [redacted]

--------------------------------------------------------------------------------
Scan Completed
Result Saved Successfully..


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

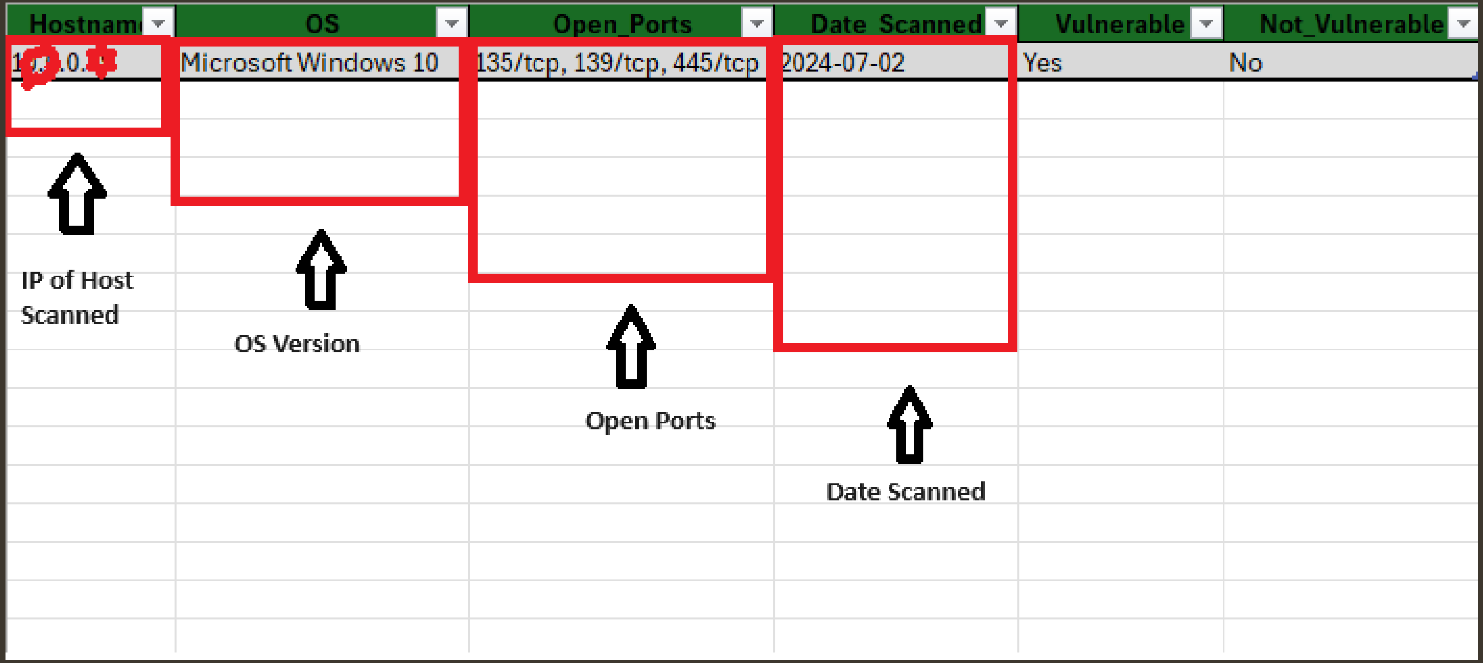
Action Plan: OS Fingerprint and Open Port network scan

Scan completed and result retained successfully

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

1.8: Process Automation – Cybersecurity

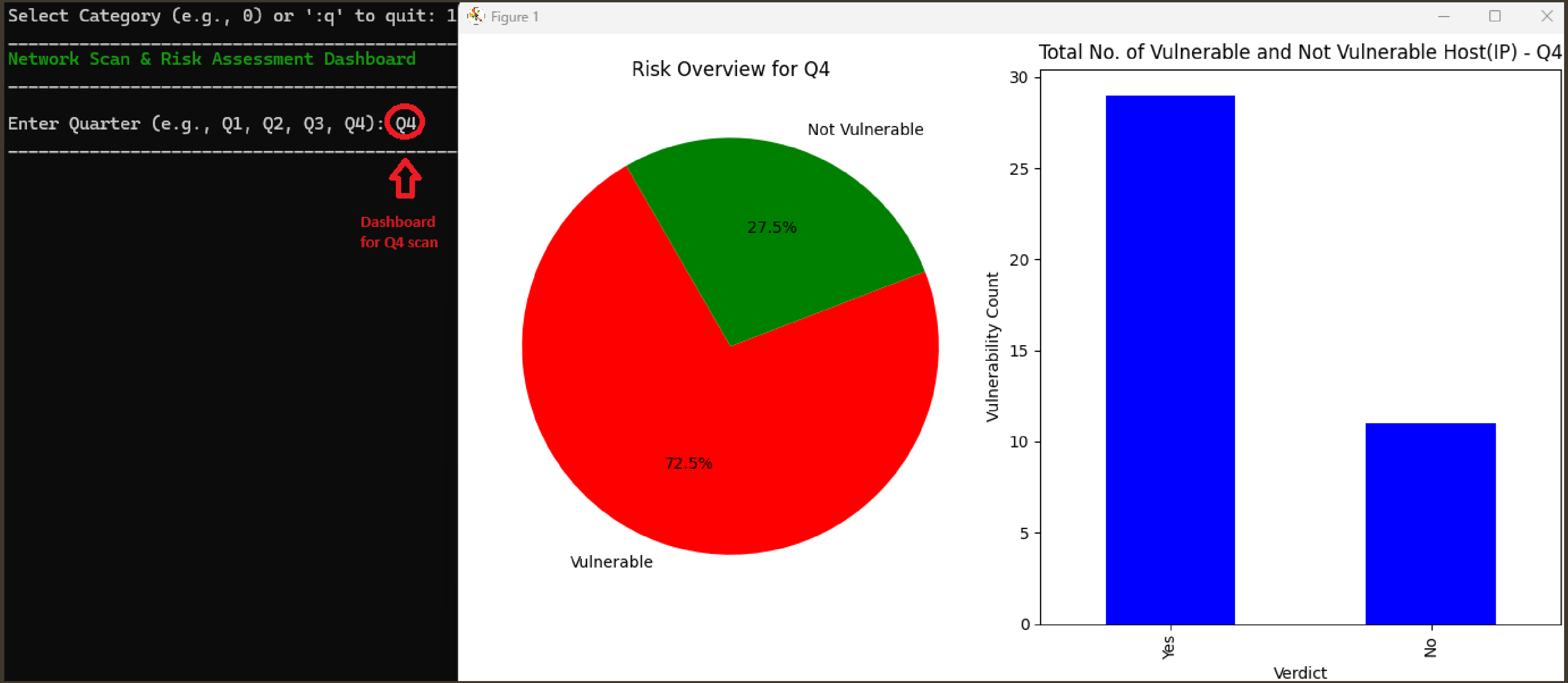
- **Action Plan:** Assess risk with open port and OS fingerprint information:
  - Discovery/Findings: OS Version & Open Port.
    - Vulnerable Justification: After manual test, some services were discovered to be utilizing default credentials.



Hostnam	OS	Open_Ports	Date_Scanned	Vulnerable	Not_Vulnerable
1[redacted].0.[redacted]	Microsoft Windows 10	135/tcp, 139/tcp, 445/tcp	2024-07-02	Yes	No

1.9: Process Automation – Cybersecurity

- **Risk Assessment Dashboard for Process Evaluation:**



```
Select Category (e.g., 0) or ':q' to quit: 1
--------------------------------------------
Network Scan & Risk Assessment Dashboard
--------------------------------------------
Enter Quarter (e.g., Q1, Q2, Q3, Q4): Q4
--------------------------------------------
```

Dashboard for Q4 scan

Domain 2: Supply Chain Optimization

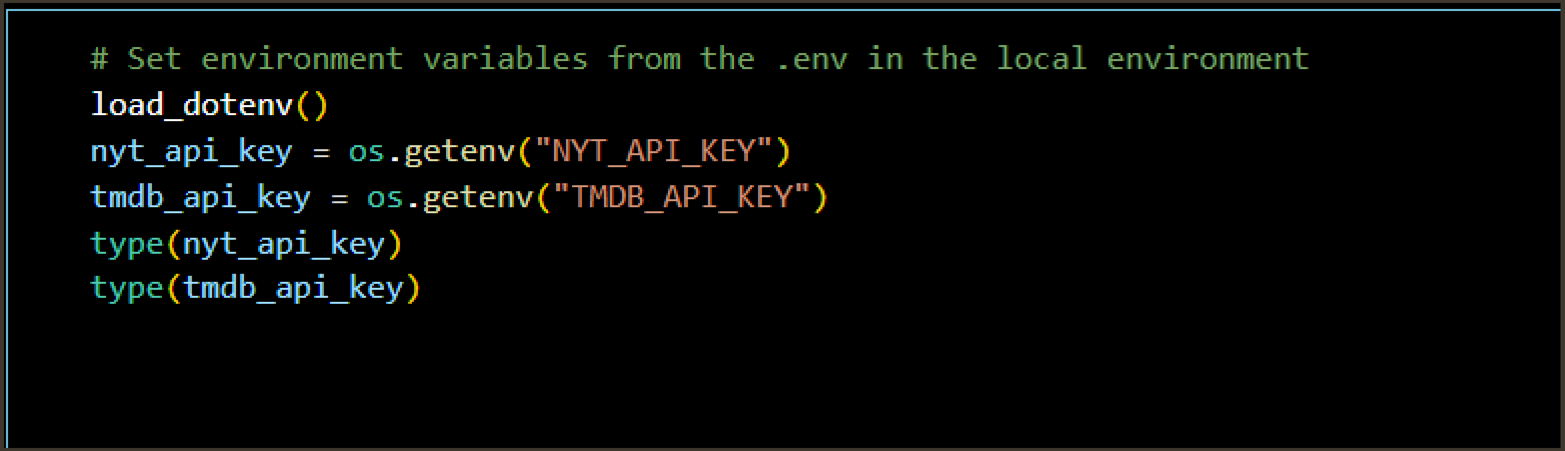
- **Data Science**:
  - Objective: Movie App Automation:
    - Business|Use Case: Address customer movie request latency issue.
      - Automation Task: Implement a BOT to retrieve list of movies by search criteria from Movie Database.
        - Resolution: Process/App modernization and API request limit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

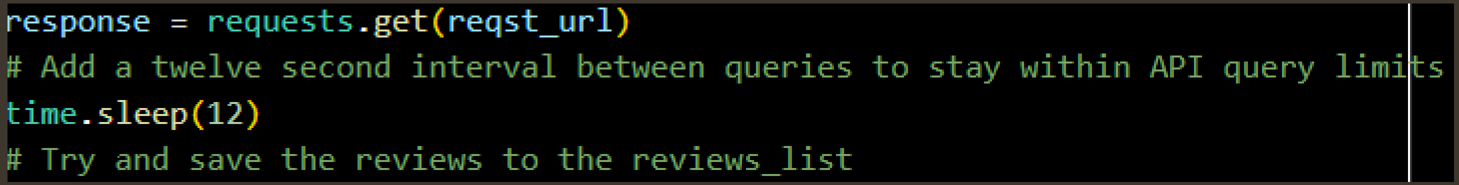
- **API Security**:
  - .ENV Hardcoded into App without revealing API Key to the public.



```
# 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)
```

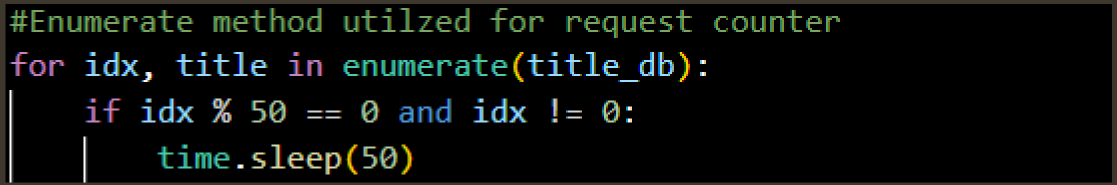
2.5: Movie App Automation - Cybersecurity

- 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:

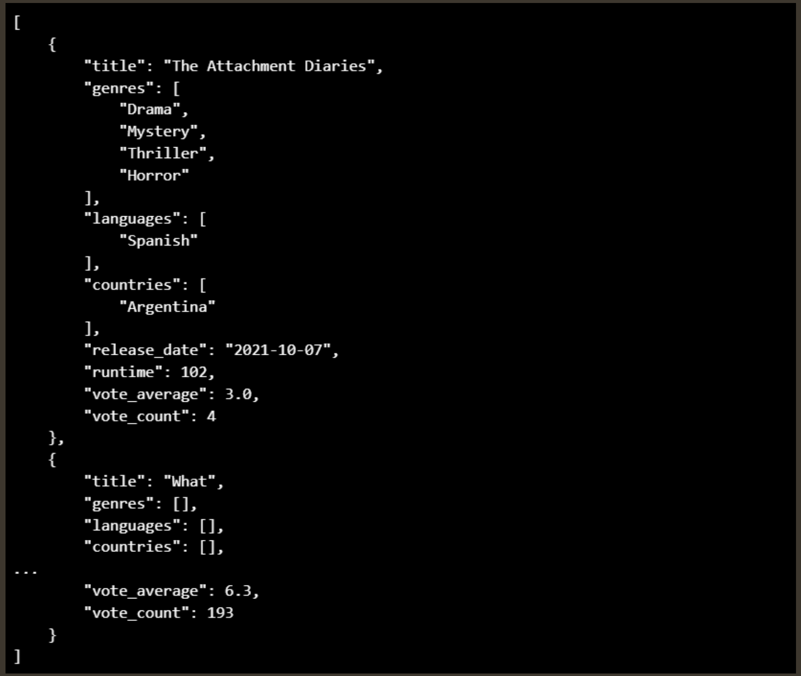


```
#Enumerate method utilzed for request counter
for idx, title in enumerate(title_db):
    if idx % 50 == 0 and idx != 0:
        time.sleep(50)
```

2.6: Movie App Automation – Data Science

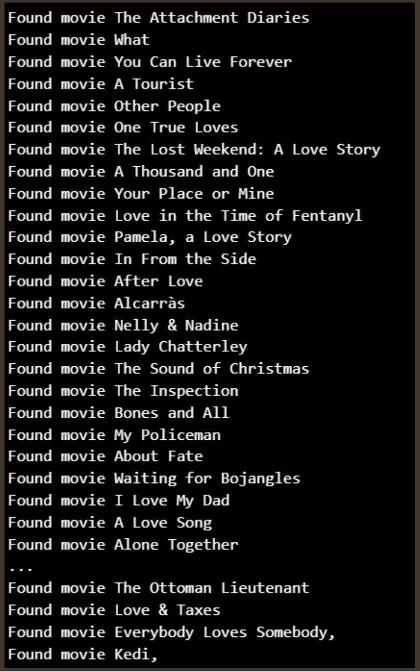
- **Program Modernization:** Bot feature with new request delay.
  - **Movie search, based on keyword and search criteria**:
    - Product Test: Romantic movie search query.

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:



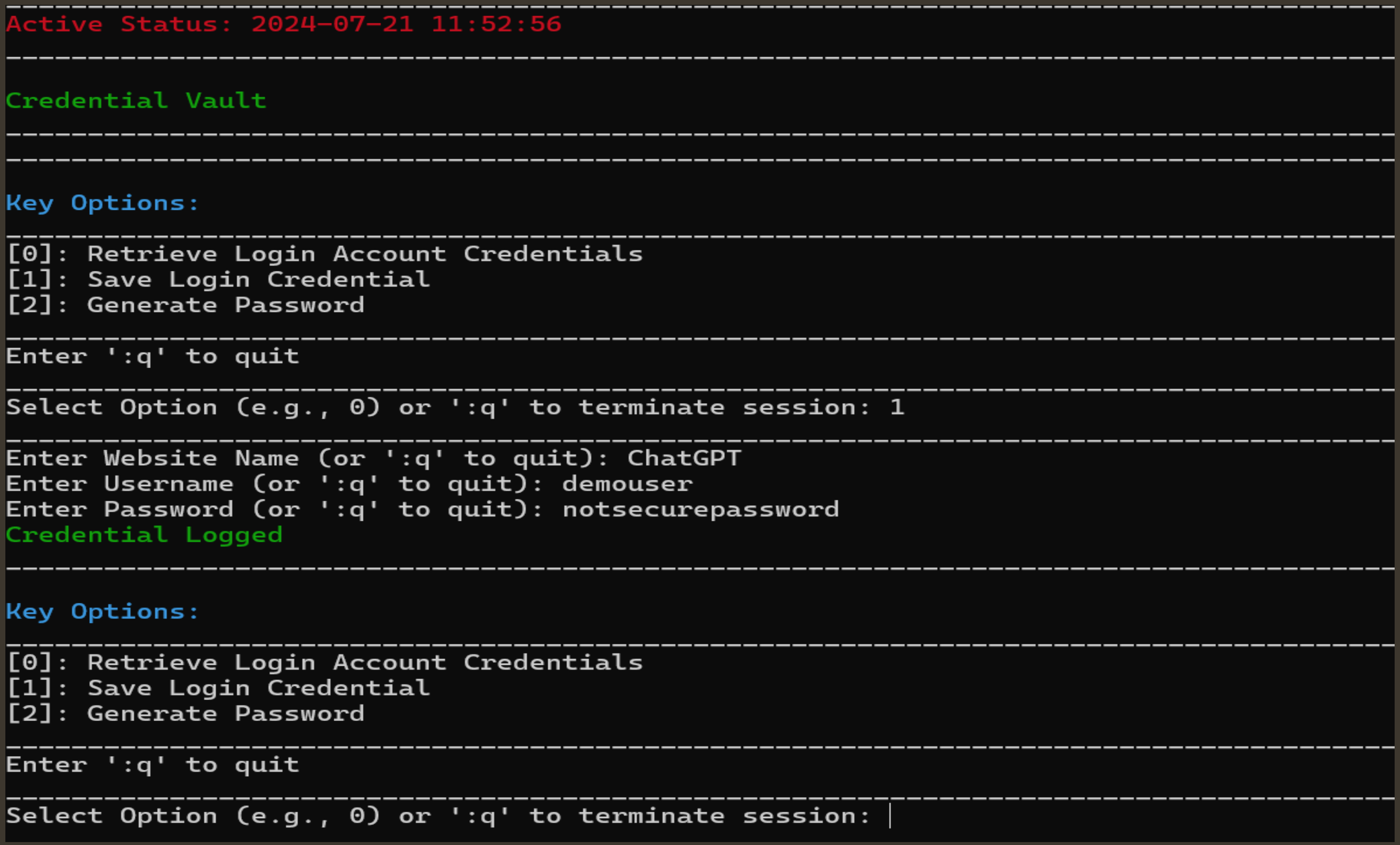
```
Found movie The Attachment Diaries
Found movie What
Found movie You Can Live Forever
Found movie A Tourist
Found movie Other People
Found movie One True Loves
Found movie The Lost Weekend: A Love Story
Found movie A Thousand and One
Found movie Your Place or Mine
Found movie Love in the Time of Fentanyl
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

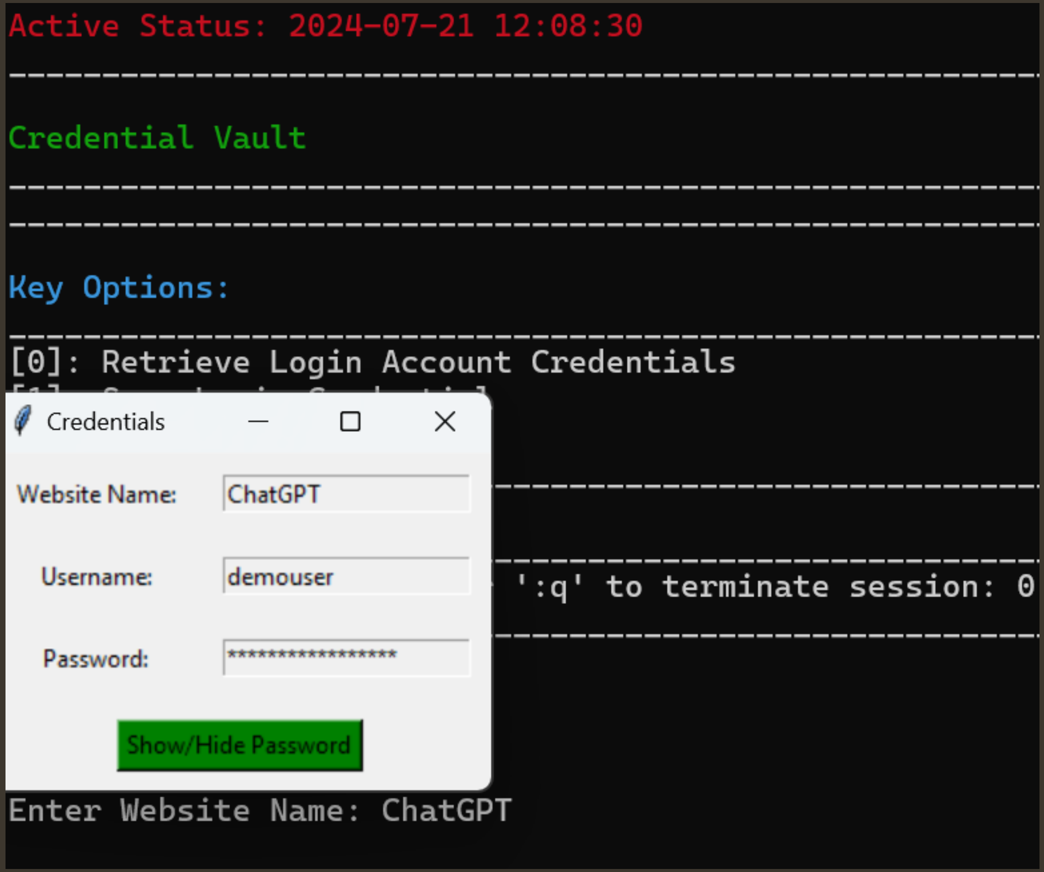
- Credentials Saved in a database table.



```
------------------------------------------------------------------------------------------
Active Status: 2024-07-21 11:52:56
------------------------------------------------------------------------------------------

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): ChatGPT
Enter Username (or ':q' to quit): demouser
Enter Password (or ':q' to quit): notsecurepassword
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: 2024-07-21 12:08:30
-------------------------------------------------------

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

Key Options:
-------------------------------------------------------
[0]: Retrieve Login Account Credentials

                          --------------------------------

                          --------------------------------
                           ':q' to terminate session: 0
                          --------------------------------

Enter Website Name: ChatGPT
```

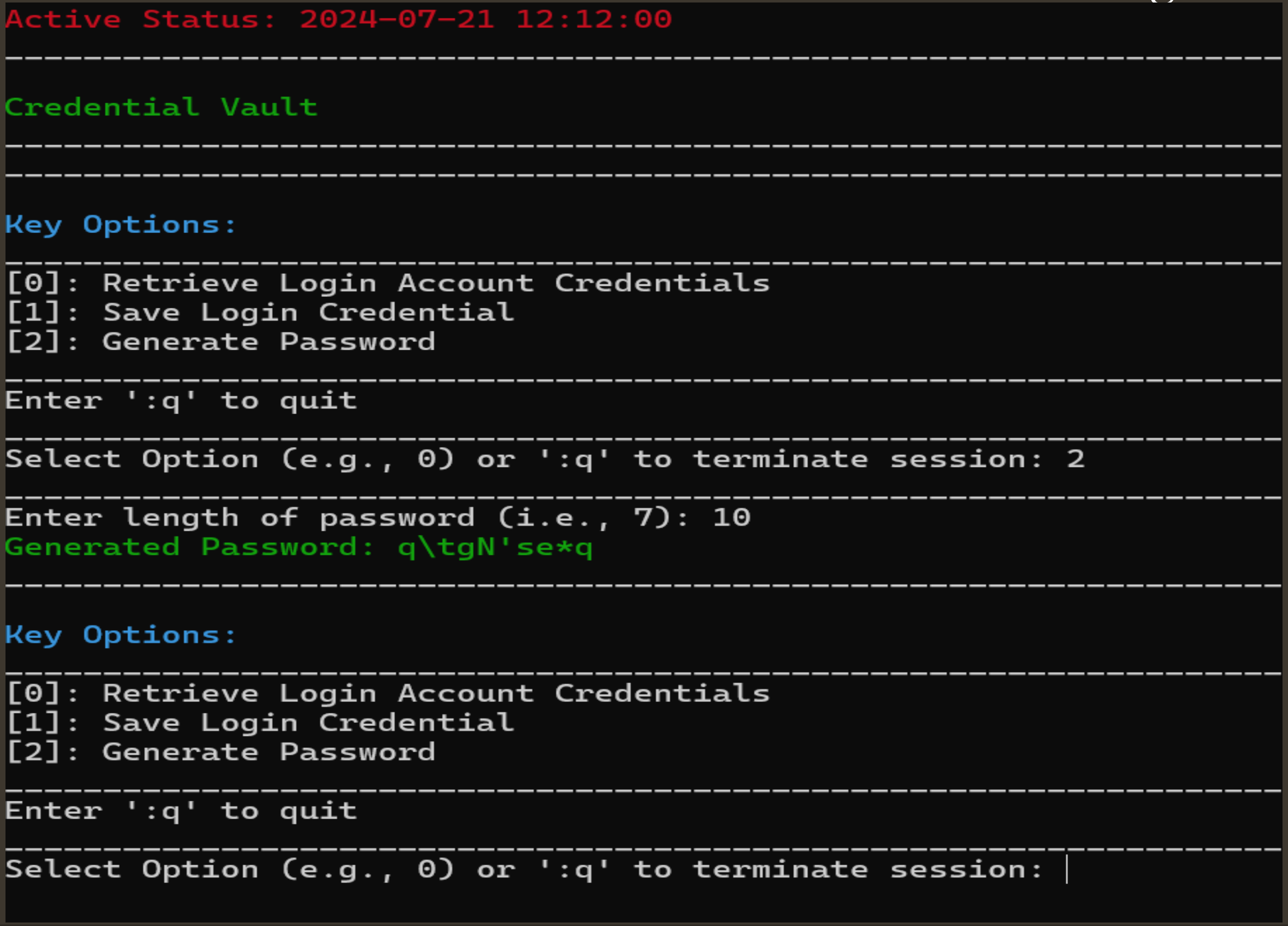
Website Name: ChatGPT

Username: demouser

Password: *****************

2.9: Generate Credentials

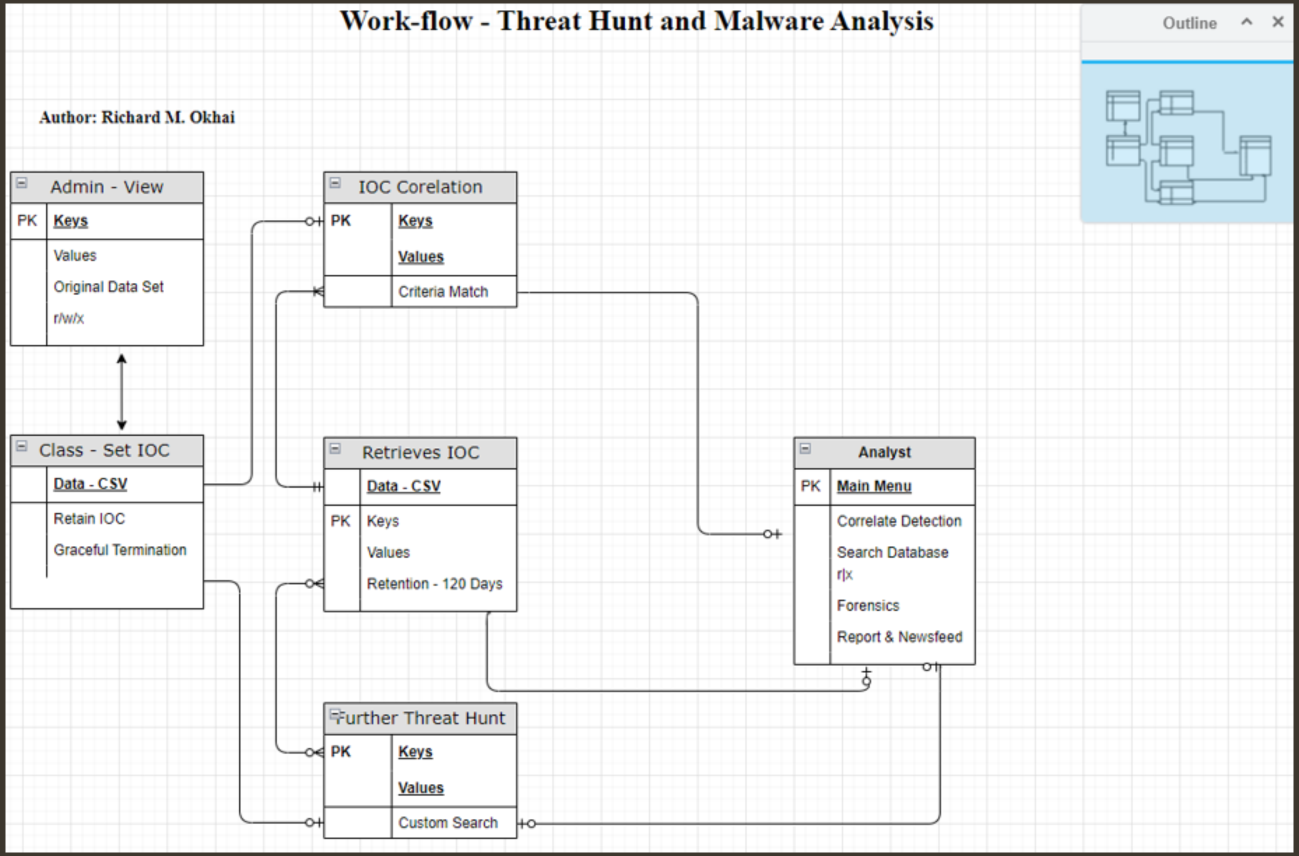
- Generate Credentials on a website for future login.



```
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'se*q
-----------------------------------------------------------------

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: 
```

Appendix

1.0: Workflow: Threat-Hunt Tool



Work-flow - Threat Hunt and Malware Analysis

Author: Richard M. Okhai

Admin - View
PK Keys
Values
Original Data Set
r/w/x

Class - Set IOC
Data - CSV
Retain IOC
Graceful Termination

IOC Corelation
PK Keys
Values
Criteria Match

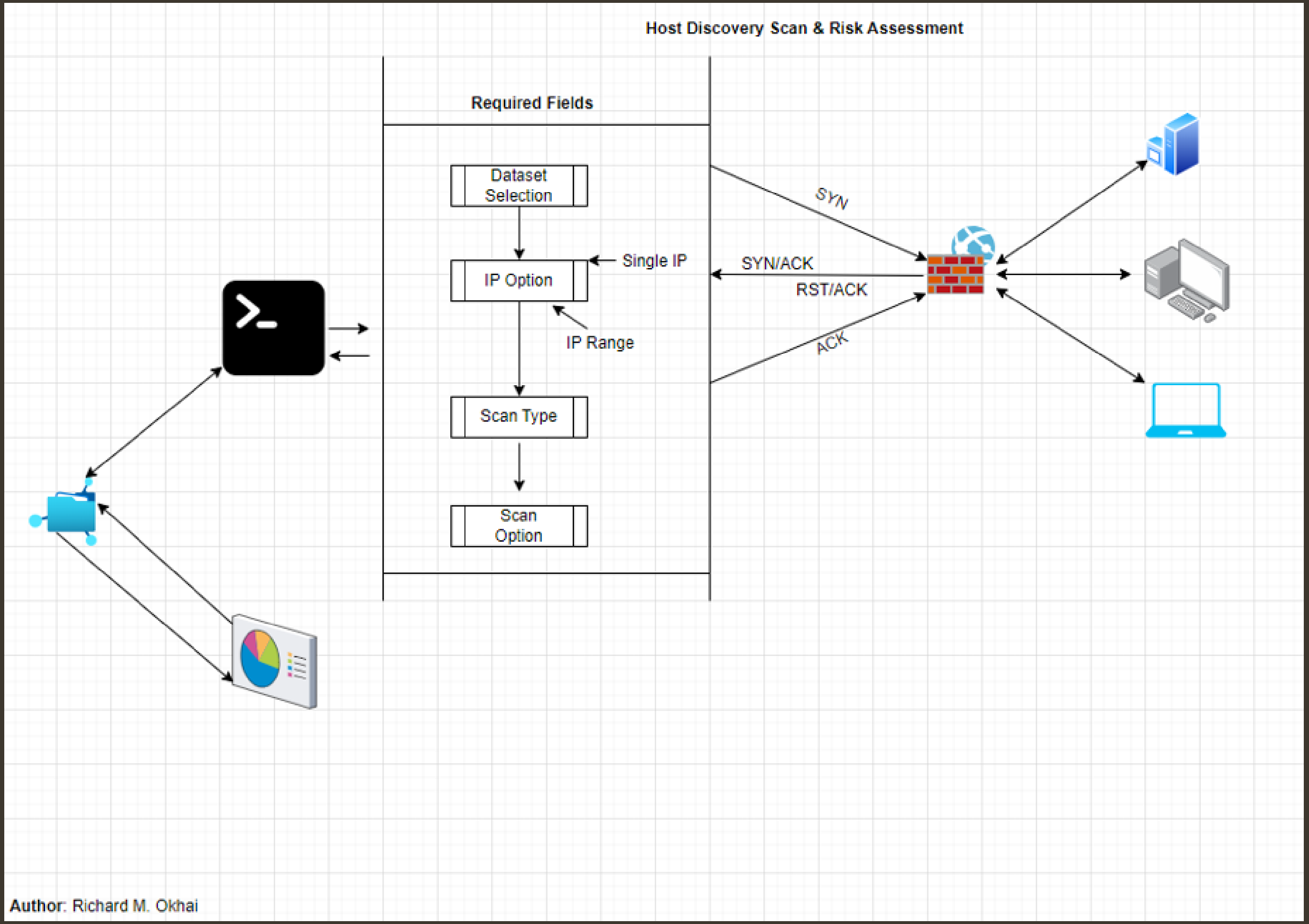
Retrieves IOC
Data - CSV
PK Keys
Values
Retention - 120 Days

Further Threat Hunt
PK Keys
Values
Custom Search

Analyst
PK Main Menu
Correlate Detection
Search Database
r|x
Forensics
Report & Newsfeed

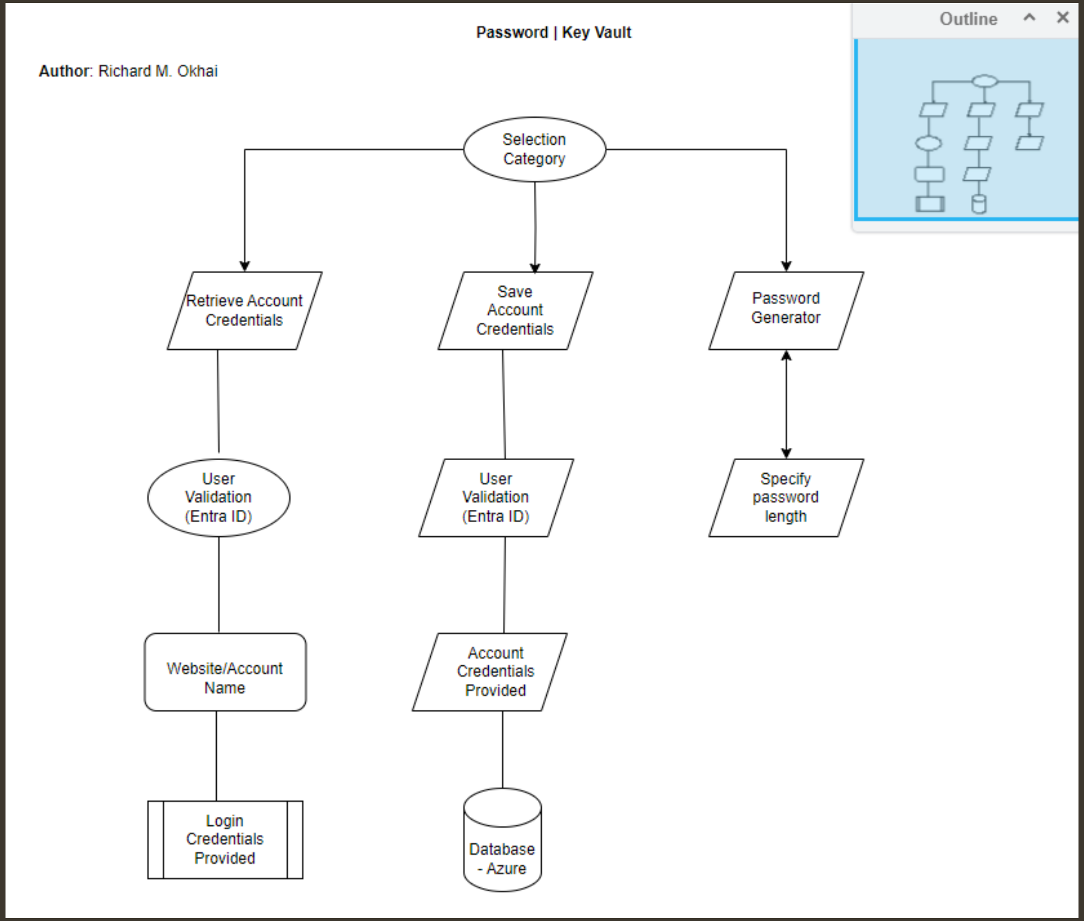
- **Language:** Python
- **Product Type:** Threat-Hunt Tool (Prototype)

1.1: Workflow: Host Discovery & Risk Assessment



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

1.2: Workflow: KeyVault



Password | Key Vault

Author: Richard M. Okhai

Outline
Selection Category
Retrieve Account Credentials
Save Account Credentials
Password Generator
User Validation (Entra ID)
User Validation (Entra ID)
Specify password length
Website/Account Name
Account Credentials Provided
Login Credentials Provided
Database - Azure

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