Perform a query with the Chronicle

In Summary:

While the Chronicle project is optional in the Cybersecurity certification, I view it as an invaluable opportunity to champion my own learning and skill development. Exploring this project allowed me to gain hands-on experience, develop in-demand cybersecurity skills, and practically deepen my understanding of the field. This reflects my commitment to taking the initiative and continuously expanding my expertise beyond mandatory requirements.

Activity Overview

This project represents my first experience using Chronicle, a cloud-native SIEM tool, to investigate a phishing incident. I analyzed a suspicious domain, identified affected assets, evaluated HTTP events, and uncovered additional domains related to the attack. This activity highlights my ability to use investigative tools to respond to security incidents effectively.

Scenario

As a security analyst at a financial services company, I received an alert regarding a phishing email targeting an employee. The email included a suspicious domain: signin.office365x24.com. My task was to determine whether other employees received similar emails, identify if they interacted with the domain, and assess the potential risks.

Step-By-Step Instructions

Step 1: Launch Chronicle

Description:

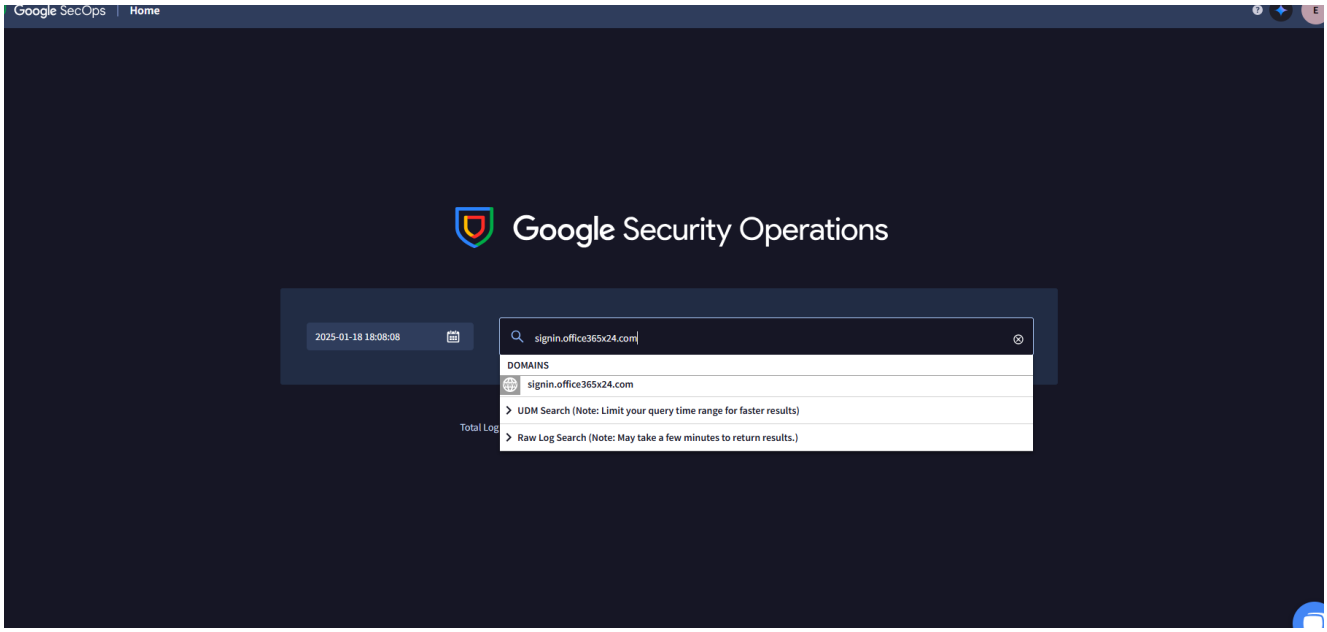
I began my investigation by accessing Chronicle, a cloud-native SIEM tool. On the homepage, the interface displayed key elements, including the current date and time, a search bar, and the total number of log entries available for analysis. This provided a quick overview of the ingested log data and a starting point for my domain investigation.

Additional Note:
To ensure optimal performance and functionality, it is recommended to use the latest version of Google Chrome when accessing Chronicle.

Step 2: Perform a domain search

Part 1: Query the Domain
I initiated the investigation by searching for the domain signin.office365x24.com, which was flagged in a phishing email. This search helps determine if the domain exists in the ingested log data and whether it has been accessed within the network.

1. Accessed the Chronicle search bar.
2. Entered signin.office365x24.com as the query and clicked **Search**.
3. Verified that the domain appeared under the **DOMAINS** section, confirming its presence in the data logs.

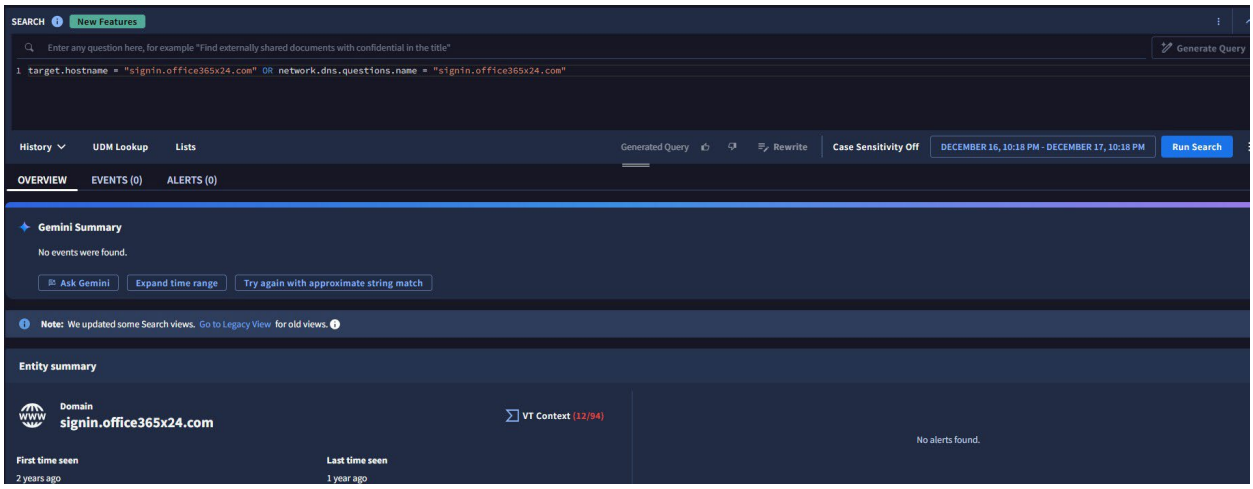


Part 2: Complete the Search

After confirming the presence of signin.office365x24.com in the ingested log data, I proceeded to access detailed information about the domain.

Steps Taken:

1. Accessed the Chronicle search bar.
2. Entered signin.office365x24.com as the query and clicked **Search**.
3. Verified that the domain appeared under the **DOMAINS** section, confirming its presence in the data logs.



Step 3: Evaluate the search results

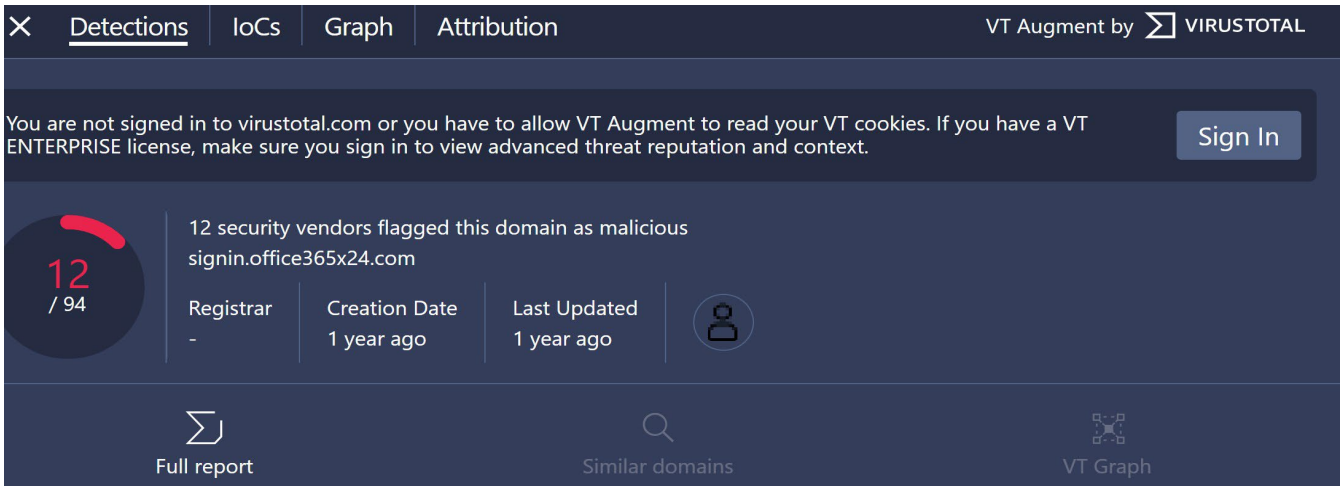
After completing the domain search, I accessed Domain **View**, which provided detailed insights about the domain signin.office365x24.com. This step involved evaluating multiple sections to gather relevant threat intelligence.

Part 1: VT CONTEXT

The **VT CONTEXT** section displays VirusTotal data for the queried domain. This information is critical for assessing the domain's reputation and determining whether it has been flagged as malicious by any security vendors.

Steps Taken:

1. I navigated to the **VT CONTEXT** section within the Domain View.
2. I reviewed the VirusTotal information associated with the domain signin.office365x24.com.
3. I observed that **no VirusTotal information was available** for this domain, indicating it had not been flagged or analyzed by VirusTotal at the time of this evaluation.



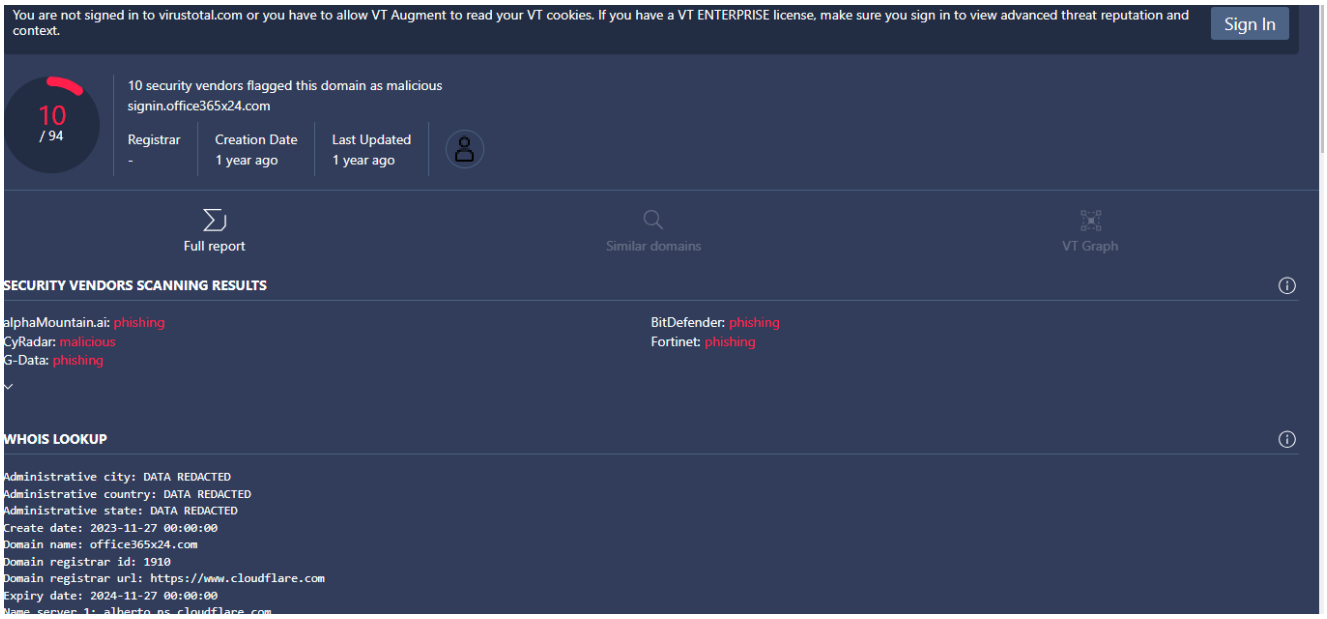
Part 2: WHOIS

The **WHOIS** section provides a summary of ownership and registration information for the domain. This publicly available directory is a critical resource in cybersecurity, offering insights into a domain's reputation and potential association with malicious activity.

Steps Taken:

1. I accessed and reviewed the **WHOIS data** for the domain signin.office365x24.com.
2. The WHOIS data revealed **minimal registration details**, a common characteristic of malicious domains attempting to evade detection.

3. Using this information, I assessed the domain's origin and reputation, noting that the lack of detailed ownership information raised potential concerns.



Part 3: Prevalence

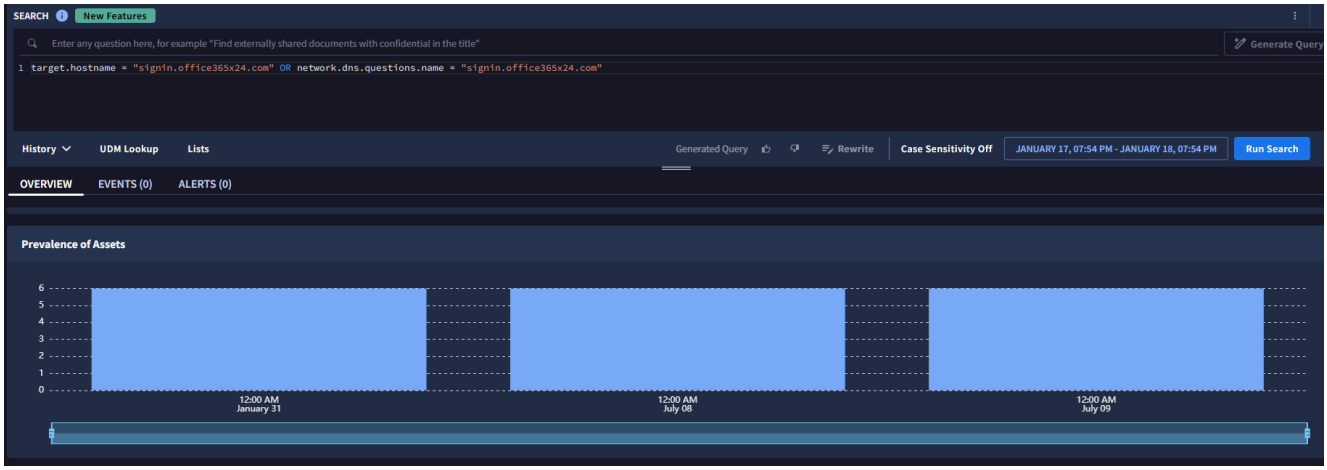
The **Prevalence** section provides a graphical representation of the domain's historical activity, outlining how often it has been accessed over time. This information is essential for evaluating a domain's legitimacy. Domains with low prevalence often signal a greater likelihood of being malicious.

Steps Taken:

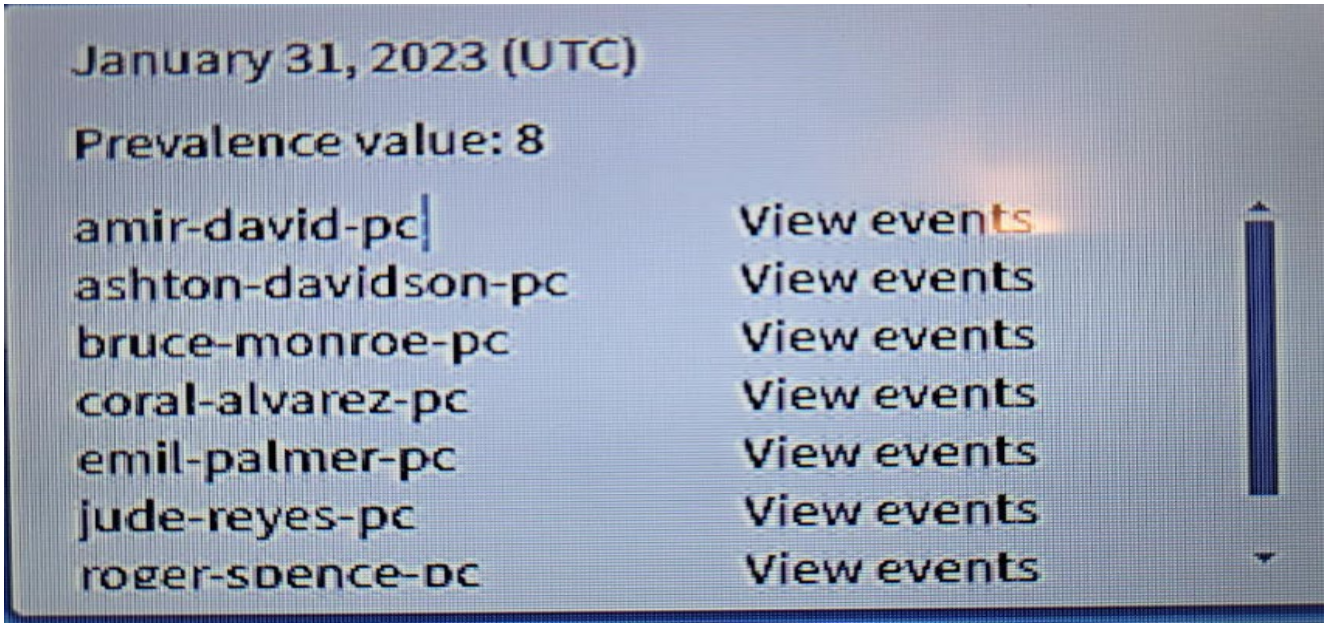
1. I analyzed the **Prevalence graph** for the domain signin.office365x24.com.
2. By hovering over the **blue center area** of the graph, I revealed additional contextual information, such as [insert examples of names/identifiers observed].
3. The graph showed [insert specific observation, e.g., "minimal activity," "a sudden spike in recent access," etc.].

Implications: Domains with limited or suspicious activity, as reflected in the graph, may indicate higher threat levels. The contextual details revealed through hovering provided further insights into potential sources or associations of the domain.

Included Image: A snapshot of the Prevalence graph highlights historical activity and the additional contextual information visible when interacting with the graph.



Caption: "The Prevalence graph for signin.office365x24.com reveals historical activity and additional contextual information, providing a clearer understanding of the domain's behavior and potential threat level." I place the pointer over the blue center to retrieve images of view events.



Part 4: Resolved IPs

The **Resolved IPs** insight card provides additional context about the domain, such as the IP address that maps to signin.office365x24.com, which is 40.100.174.34. By clicking on this IP, a new search is initiated within Chronicle to further investigate its activity.

Insight cards like this are useful for expanding the scope of a domain investigation and determining whether the domain is part of a broader compromise.

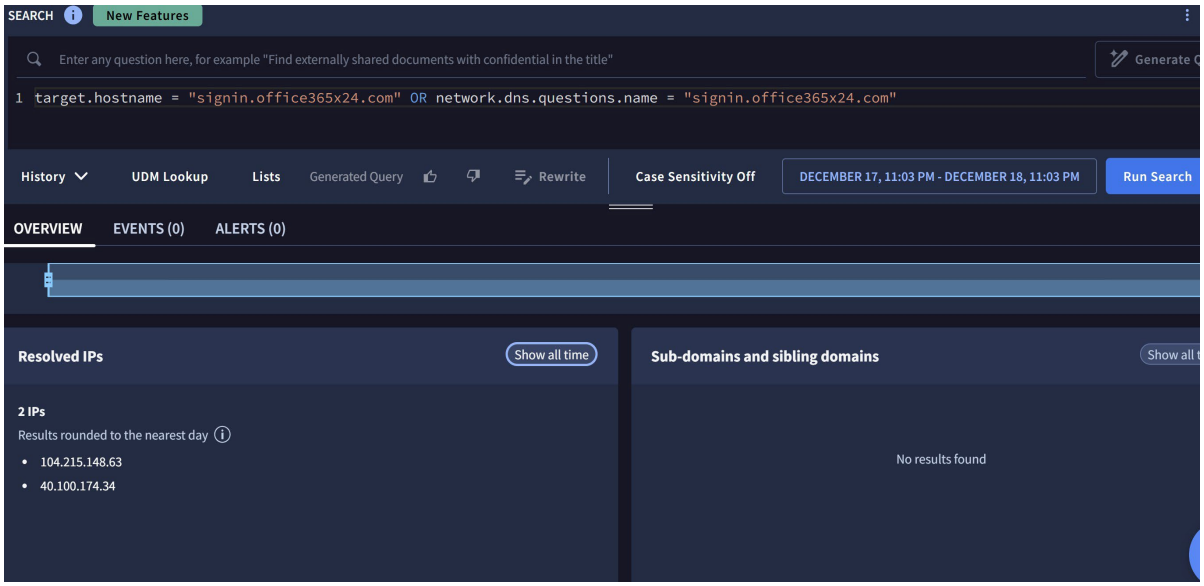
Steps Taken:

1. I reviewed the **Resolved IPs** insight card to identify the mapped IP address.
2. I clicked on the IP address (40.100.174.34) to initiate a detailed search within Chronicle.
3. This allowed me to analyze the IP's historical activity, geolocation, and any associated indicators of compromise.

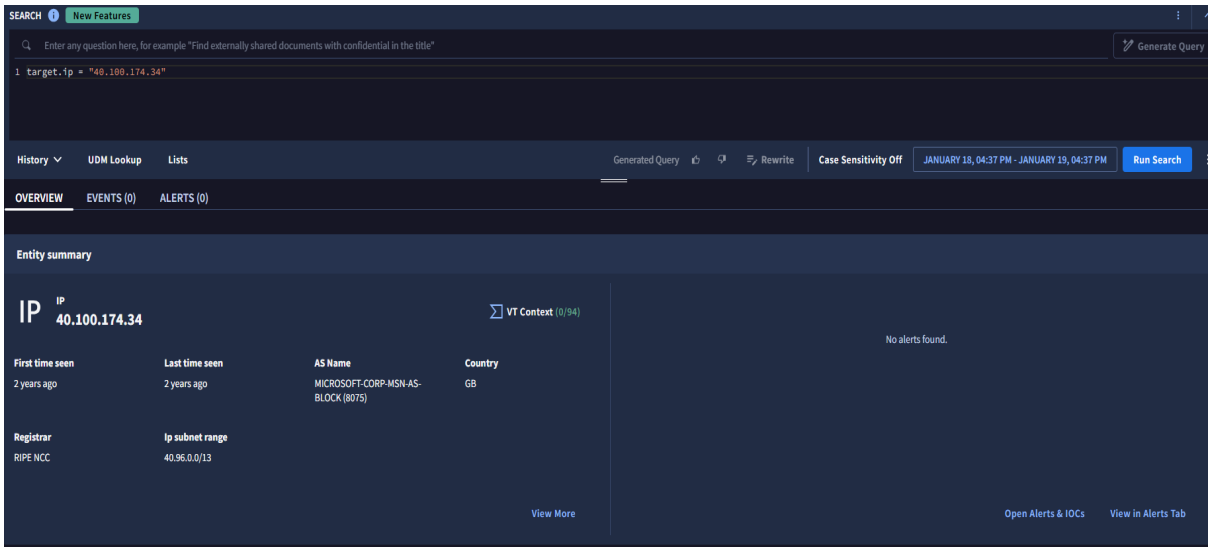
Implications: Leveraging the Resolved IPs insight card enabled me to expand the investigation and gain a deeper understanding of the domain's potential threat level by exploring its network connections.

Included Images:

1. The first image shows the Resolved IP insight card with the IP address displayed.



2.The second image highlights the detailed view of the IP address after clicking on it, showcasing additional context and historical activity.



Caption: "The Resolved IPs insight card for signin.office365x24.com provides both an overview of associated IP addresses and detailed insights into their historical activity and potential threats."

Part 5: Sibling Domains

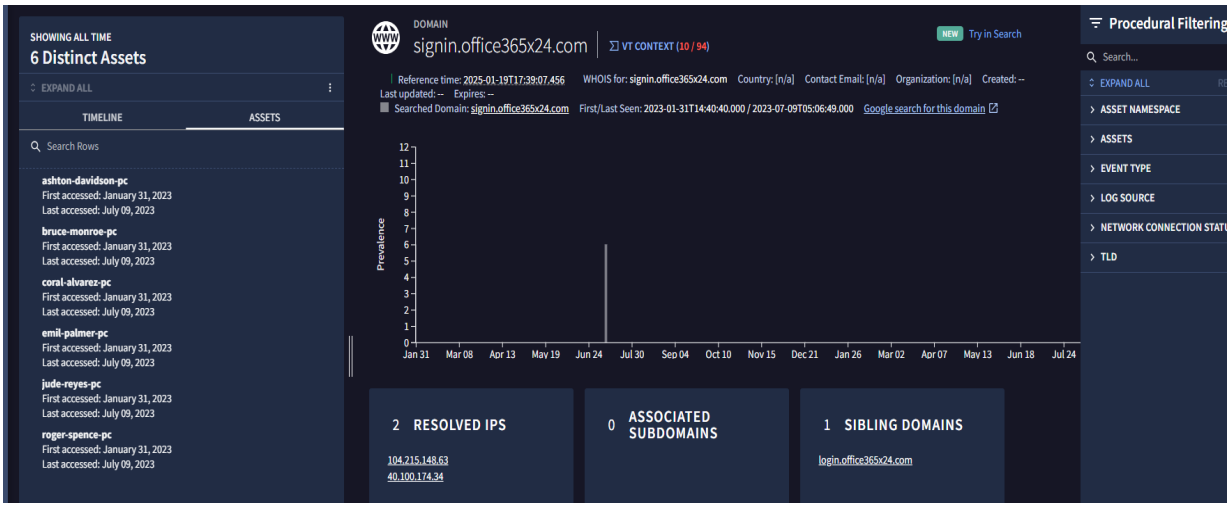
The **Sibling Domains** insight card provides additional context about related domains. Sibling domains share a common top or parent domain. In this case, the sibling domain is listed as login.office365x24.com, which shares the same top domain (office365x24.com) as the domain under investigation (signin.office365x24.com).

Steps Taken:

1. I reviewed the **Sibling Domains** insight card to identify related domains.
2. The sibling domain login.office365x24.com was identified, providing additional context for assessing potential threats within the same domain family.

Implications: Identifying sibling domains expands the scope of investigation by revealing other domains that could potentially be part of a broader threat campaign. These domains can be further analyzed to assess their legitimacy and connections to malicious activity.

Included Image: A snapshot of the Sibling Domains insight card highlights the sibling domain and its relationship to the domain under investigation.



Caption: "The Sibling Domains insight card for signin.office365x24.com identifies related domains, providing additional context for a broader threat analysis."

Part 6: ET Intelligence Rep List

Thee **ET Intelligence Rep List** insight card includes additional context about the domain by leveraging threat intelligence from ProofPoint's Emerging Threats (ET) Intelligence Rep List. This card highlights other known threats related to the domain and its connections.

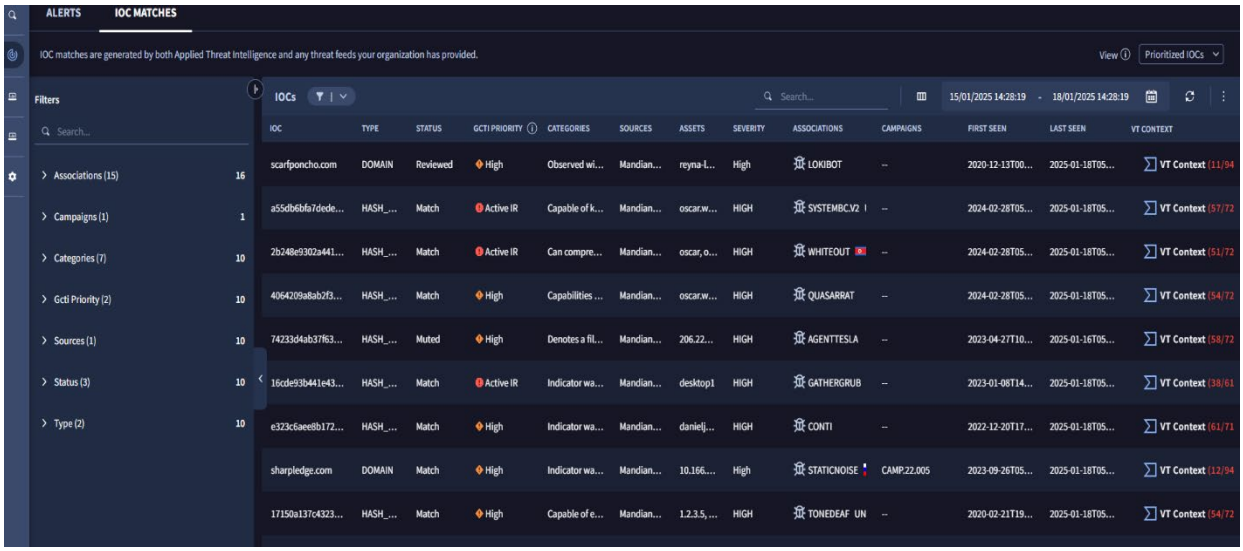
Steps Taken:

1. I reviewed the **ET Intelligence Rep List** insight card to gather additional threat intelligence about signin.office365x24.com.
2. The card provided information about known threats associated with related domains and indicators of compromise.

Implications: Using the ET Intelligence Rep List insight card allowed me to identify potential threat patterns and connections, enabling a deeper understanding of the domain's risk level and its role within a broader threat landscape.

Included Image: A snapshot of the ET Intelligence Rep List insight card highlights related threats and connections for signin.office365x24.com.

Caption: "The ET Intelligence Rep List insight card provides additional threat intelligence, offering deeper context into known threats and related indicators for signin.office365x24.com."



Caption: "The ET Intelligence Rep List insight card provides additional threat intelligence, offering deeper context into known threats and related indicators for signin.office365x24.com."

Part 7: Click **TIMELINE**.

The **Timeline** tab provides detailed information about the events and interactions made with the domain. This includes HTTP requests, which are categorized into **GET** and **POST** requests.

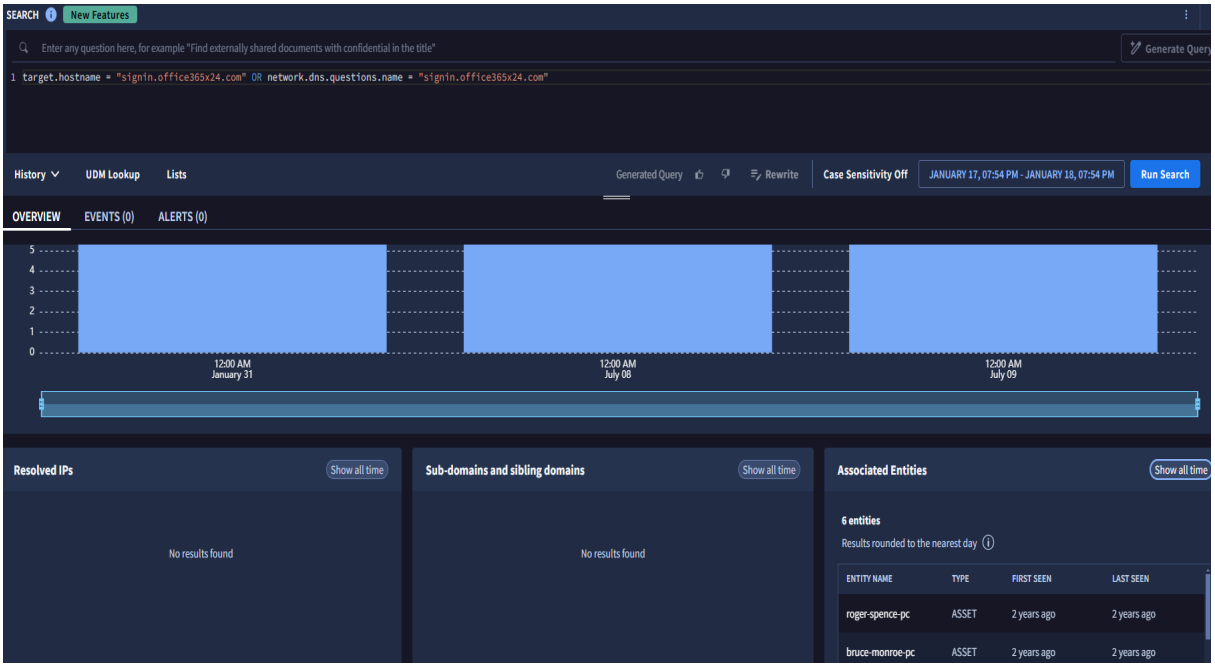
- **GET Request:** Retrieves data from a server.
- **POST Request:** Submits data to a server.

Steps Taken:

1. I clicked on the **Timeline** tab to view the event details.
2. I selected **EXPAND ALL** to reveal the full list of HTTP requests made to the domain.
3. I analyzed the GET and POST requests to identify patterns or suspicious activities.

Implications: Reviewing the Timeline tab allowed me to understand the interactions with the domain and evaluate whether any of these requests posed potential security risks.

Included Image: A snapshot of the Timeline tab highlights the HTTP request details and the expanded view of interactions.



Caption: "The Timeline tab provides detailed insights into HTTP requests made to signin.office365x24.com, offering a clear view of GET and POST request activities."

Part 8: Click **ASSETS**.

The **Assets** tab provides a list of the devices or assets that have accessed the domain. This information helps identify which devices have interacted with the domain and can provide further insights into potential risks or compromises.

Steps Taken:

1. I clicked on the **Assets** tab to view the list of devices associated with the domain signin.office365x24.com.
2. The list displayed six assets, revealing the time and date of the first and last accessed.
3. **Implications:** Reviewing the Assets tab allowed me to pinpoint the devices interacting with the domain, helping to trace potential origins of suspicious activity and assess the scope of a possible compromise.

Included Image: A snapshot of the Assets tab highlights the six devices that accessed the domain.

Caption: "The Assets tab for signin.office365x24.com reveals six devices that accessed the domain, providing insights into potential origins and scope of interaction."

Step 4: Investigate the threat intelligence data

After retrieving the results for the domain name, I focused on determining whether the domain signin.office365x24.com is malicious. Chronicle provides quick access to threat intelligence data from the search results, which I used to support my investigation.

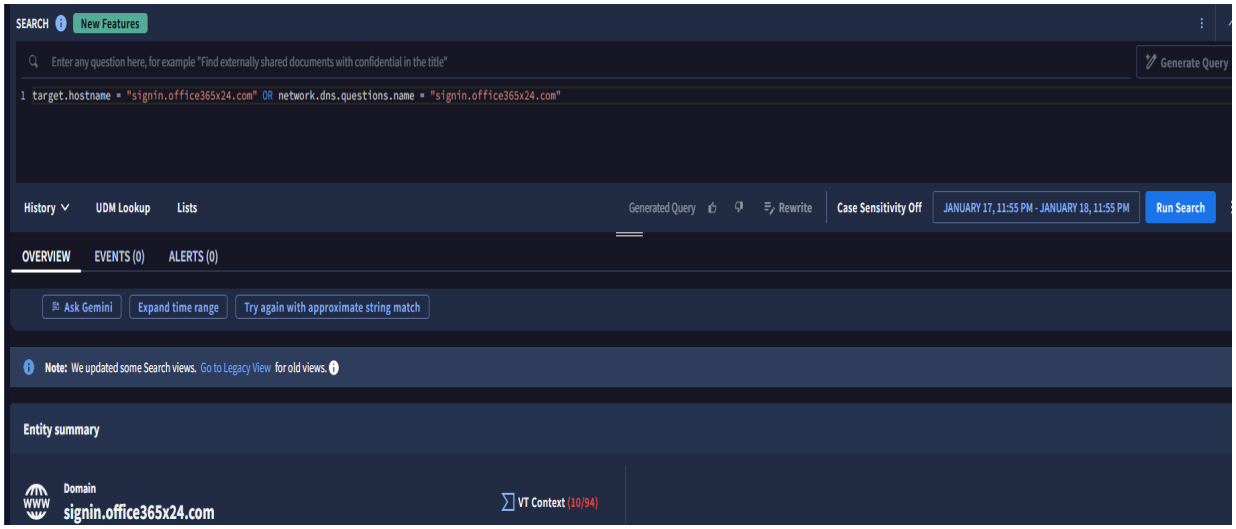
1. Click on **VT CONTEXT** to analyze the available VirusTotal information about this domain. There is no VirusTotal information about this domain. To exit the VT CONTEXT window, click the **X**.

Steps Taken:

1. I clicked on **VT CONTEXT** to analyze the available VirusTotal information for this domain.
2. Upon review, I found that there was **no VirusTotal information available** about this domain, which suggests it had not been flagged or analyzed at the time of the investigation.
3. To exit the VT CONTEXT window, I clicked the **X** in the top-right corner.

Insights: The absence of VirusTotal information raised questions about the domain's activity and prompted me to further investigate its reputation using other tools and indicators.

Included Image: A screenshot of the VT CONTEXT section highlights the lack of VirusTotal information, which was noted in my incident handler's journal for further review.



2. By **Top Private Domain,** click **office365x24.com** to access the domain view for **office365x24.com**. Click **VT CONTEXT** to assess the VirusTotal information about this domain. In the pop up, you can observe that one vendor has flagged this domain as malicious. Exit the VT CONTEXT window. Click the back button in your browser to go back to the domain view for the **signin.office365x24.com** search.

After retrieving the results for the domain name, I continued my analysis to determine whether the domain was malicious. Chronicle's tools provided quick access to relevant threat intelligence data.

Steps Taken:

1. I navigated to **Top Private Domain** and clicked on office365x24.com to access the domain view for this parent domain.
2. I clicked on **VT CONTEXT** to assess the VirusTotal information available for office365x24.com.
    - In the pop-up, I observed that **one vendor flagged this domain as malicious**.
3. I exited the VT CONTEXT window by clicking the **X** in the top-right corner.
4. Using the browser's back button, I returned to the domain view for signin.office365x24.com to continue my investigation.

Insights: The VirusTotal data for office365x24.com revealed a malicious flag, *lu*which raised the overall threat level of its subdomain, signin.office365x24.com. This finding was recorded in my incident handler's journal for further analysis and correlation with other data sources.

Incded Image: A screenshot of the VT CONTEXT section for office365x24.com highlights the malicious flag identified by one vendor.

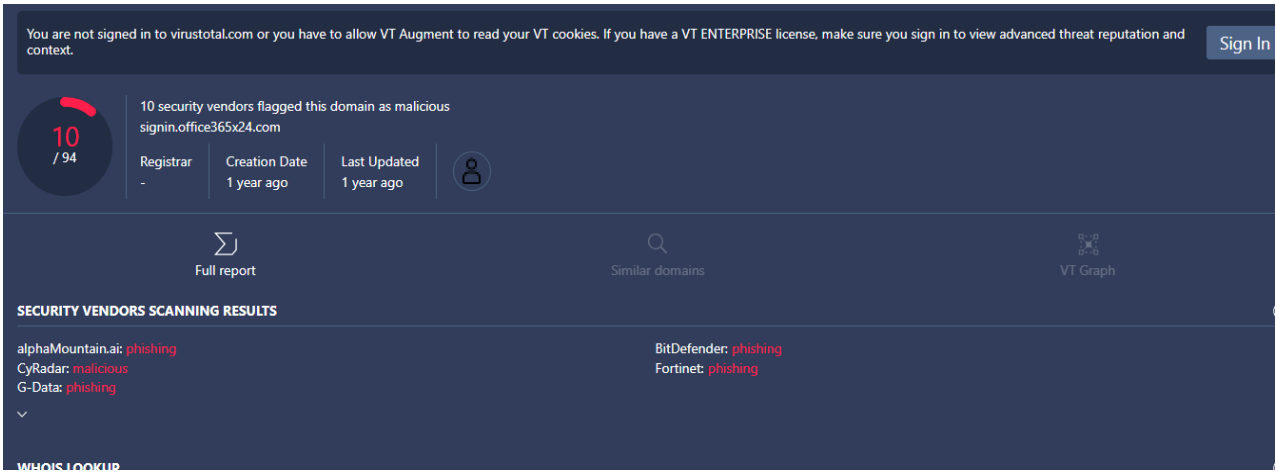
After retrieving the results for the domain name, I continued my analysis to determine whether the domain was malicious. Chronicle's tools provided quick access to relevant threat intelligence data.

Steps Taken:

1. I navigated to **Top Private Domain** and clicked on office365x24.com to access the domain view for this parent domain.
2. I clicked on **VT CONTEXT** to assess the VirusTotal information available for office365x24.com.
    - In the pop-up, I observed that **one vendor flagged this domain as malicious**.
3. I exited the VT CONTEXT window by clicking the **X** in the top-right corner.
4. Using the browser's back button, I returned to the domain view for signin.office365x24.com to continue my investigation.

Insights: The VirusTotal data for office365x24.com revealed a malicious flag, *lu*which raised the overall threat level of its subdomain, signin.office365x24.com. This finding was recorded in my incident handler's journal for further analysis and correlation with other data sources.

Incded Image: A screenshot of the VT CONTEXT section for office365x24.com highlights the malicious flag identified by one vendor.



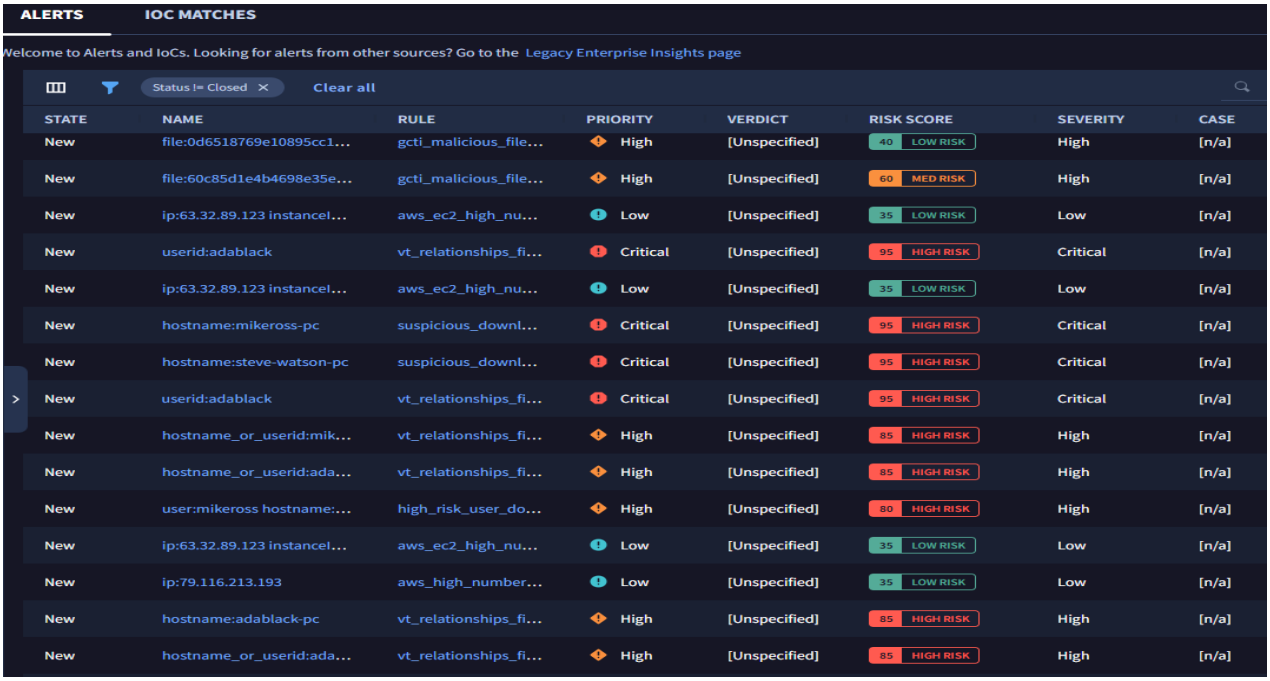
3. Click on the **ET INTELLIGENCE REP LIST** insight card to expand it, if needed. Take note of the category.

I clicked on the **ET INTELLIGENCE REP LIST** insight card to expand it as needed.

- I took note of the **priority levels** listed: low, critical, and high.
- The **risk score indicators** were represented by color codes: blue for low risk, orange for medium risk, and red for high risk.

Insights: The VirusTotal data for office365x24.com revealed a malicious flag, which raised the overall threat level of its subdomain, signin.office365x24.com. Additionally, the **ET INTELLIGENCE REP LIST** provided valuable context for categorizing potential risks. These findings were recorded in my incident handler's journal for further analysis and correlation with other data sources.

Included Image: A screenshot of the VT CONTEXT section for office365x24.com highlights the malicious flag identified by one vendor, while another image showcases the **ET INTELLIGENCE REP LIST** and its priority categories.



Step 5: Investigate the affected assets and events

Information about events and assets relating to the domain is separated into two tabs: **TIMELINE** and **ASSETS**.

- The **TIMELINE** tab shows the timeline of events, including when each asset accessed the domain.
- The **ASSETS** tab lists hostnames, IP addresses, MAC addresses, or devices that have accessed the domain.

Steps Taken:

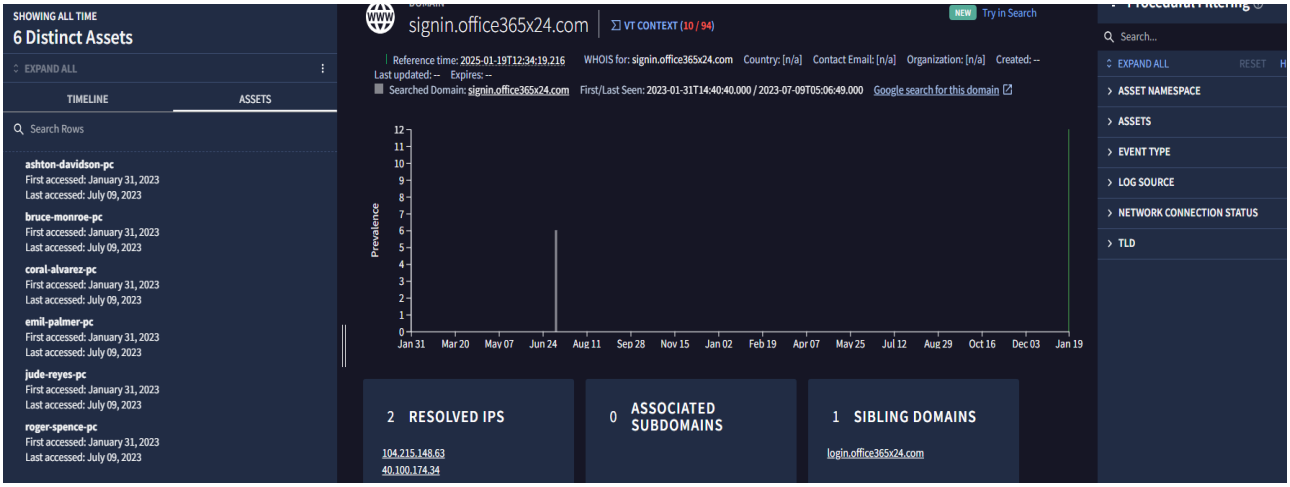
1. **ASSETS Tab**

    - I reviewed the ASSETS tab, which displayed several different assets that had accessed the domain.

- The list included the **date and time of access** for each asset.
- Using my incident handler's journal, I recorded the **name and number of assets** that interacted with the domain.

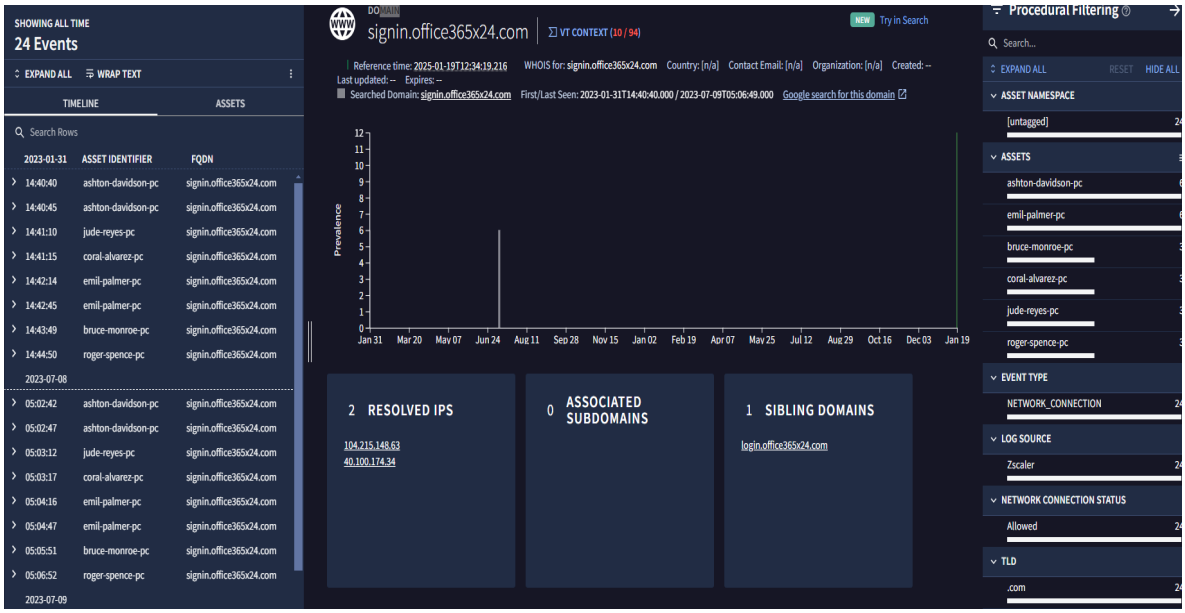
Insights: Investigating the ASSETS tab provided a detailed understanding of the devices and systems interacting with the domain. This information is critical for identifying potential points of compromise and evaluating the overall scope of the threat.

Included Image: A snapshot of the ASSETS tab highlights the recorded devices, their names, and access times.



2.. TIMELINE Tab

- I clicked on the **TIMELINE** tab and selected **EXPAND ALL** to reveal details about the HTTP requests made to the domain.
- I focused on the **POST requests** to the /login.php page, which indicated that data was sent to the domain. This suggested a possible successful phishing attempt.
- For additional details about the connections, I opened the raw log viewer by clicking the open icon.
- I recorded the POST requests and their associated details in my incident handler's journal.



Step 6: Investigate the resolved IP address

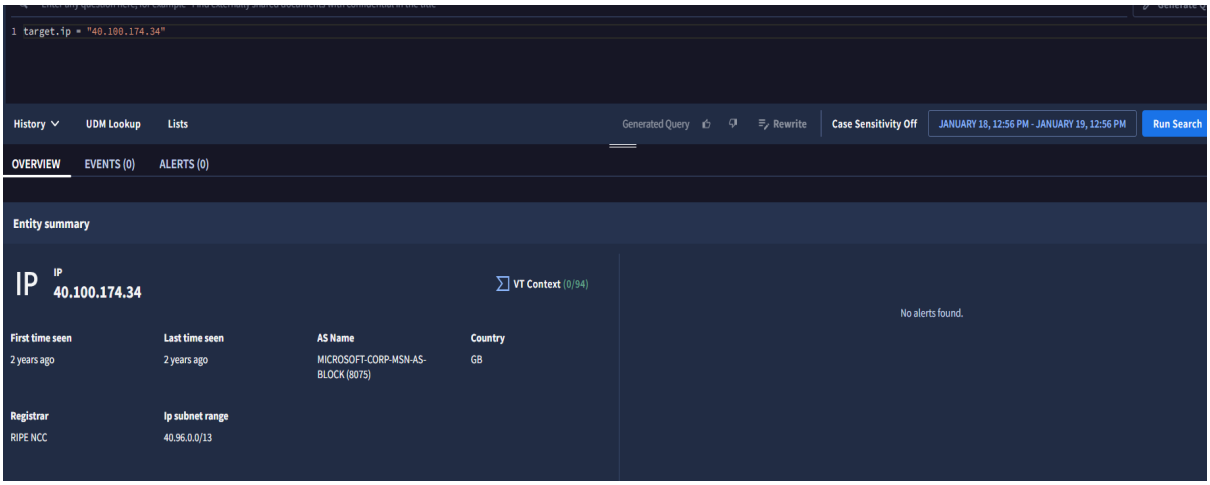
So far, I have collected information about the domain's reputation using threat intelligence and identified the assets and events associated with the domain. Based on this information, it is clear that this domain is suspicious and most likely malicious. However, before confirming, there is one last step to investigate.

Attackers sometimes reuse infrastructure for multiple attacks. In these cases, multiple domain names resolve to the same IP address. I investigated the IP address found under the **RESOLVED IPS** insight card to identify whether the signin.office365x24.com domain uses another domain.

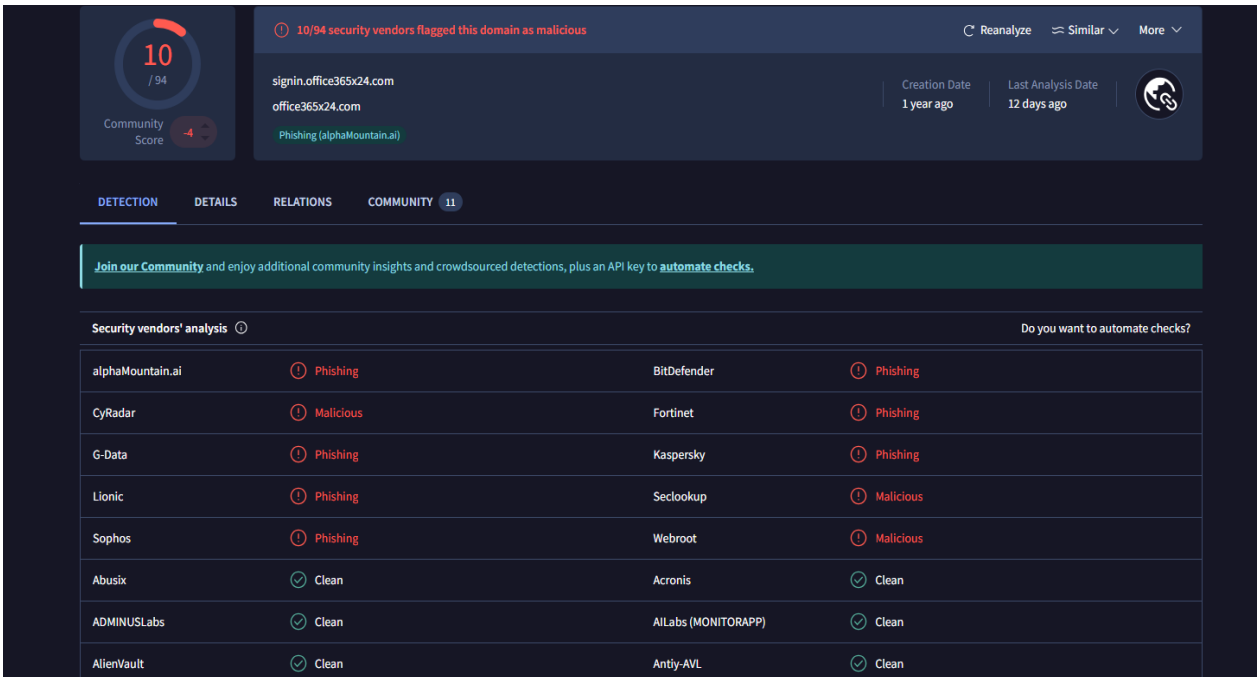
Insights: By investigating the resolved IP address, I was able to identify the assets associated with this domain. This analysis helped establish a clearer understanding of the potential points of compromise and the overall scope of the threat.

Steps Taken:

1. **RESOLVED IPS Insight Card**
    - I clicked on the IP address 40.100.174.34 listed under the RESOLVED IPS insight card.

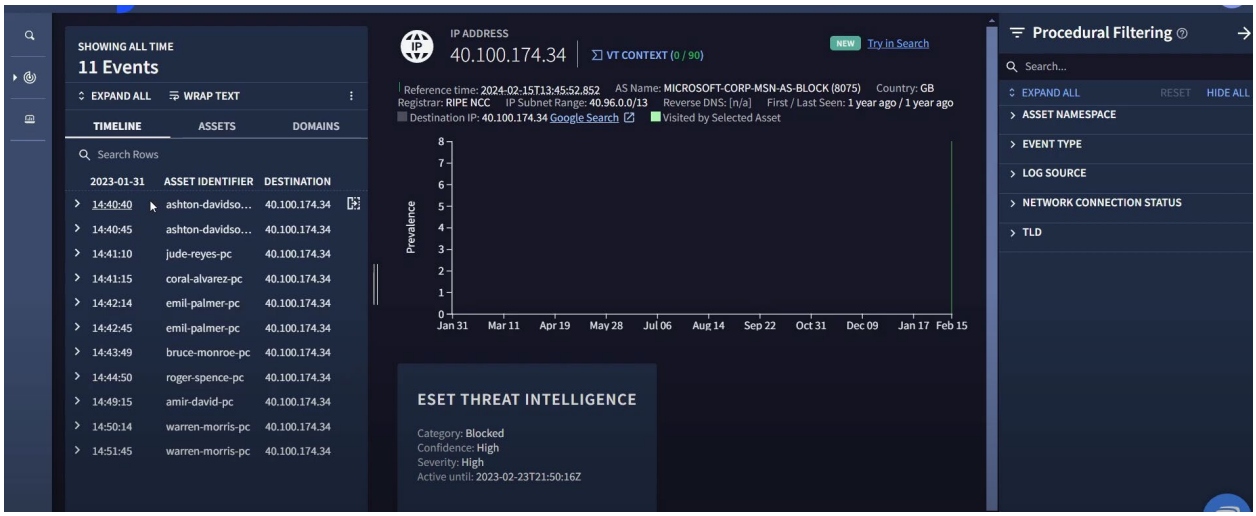


2. **TIMELINE**
    - I evaluated the search results for this IP address and took note of an additional **POST request** to the /login.php page.
    - A new POST suggests that an asset may have been phished.
    - Using my incident handler's journal, I recorded the POST request and its significance.



3. A**SSETS Tab**
    - I reviewed the assets associated with this domain and recorded their first and last access dates in my journal. The identified assets were:

- **ashton-davidson-pc**: First accessed: January 31, 2023, Last accessed: July 9, 2023
- **bruce-monro-pc**: First accessed: January 31, 2023, Last accessed: July 9, 2023
- **coral-alvarez-pc**: First accessed: January 31, 2023
- **emil-palmer-pc**: First accessed: January 31, 2023, Last accessed: July 9, 2023
- **jud-reyes-pc**: First accessed: January 31, 2023, Last accessed: July 9, 2023



Incident handler's journal

Date: Record the date of the journal entry.	**Entry:** January 31, 2023
Description	Performed an analysis of the resolved IP address 40.100.174.34 associated with the phishing domain signin.office365x24.com. Identified two additional suspicious domains (signin.accounts-gooqle.com and signin.office365x24.com) and confirmed POST requests from affected assets.
Tool(s) used	**Chronicle SIEM** for IP and domain relationship analysis; **ET Intelligence Rep List** for categorizing threats.

The 5 W's	Capture the 5 W's of an incident. • **Who** caused the incident? Six attackers sent the phishing email. • **What** happened? An employee received a phishing email containing a suspicious domain signin.office365x24.com. • **When** did the incident occur? The incident was detected on [Jan. 31, 2023]. • **Where** did the incident happen? The incident occurred at a financial services company. • **Why** did the incident happen? The phishing email aimed to steal credentials or sensitive information.
Additional notes	Include any additional thoughts, questions, or findings.

Insights: By investigating the resolved IP address, I was able to identify the assets associated with this domain. This analysis helped establish a clearer understanding of the potential points of compromise and the overall scope of the threat.

Step 7: Answer Questions About the Domain Investigation

Use the notes from your incident handler's journal and Chronicle search results to answer the following questions. Ensure you query the correct domain listed in each question.

---

1. According to the available ET Intelligence Rep List, how is signin.office365x24.com categorized?

- ☐ Command and control server
- ☑ Drop site for logs or stolen credentials
- ☐ Spam site
- ☐ Phishing site

---

2. Which assets accessed the signin.office365x24.com domain? *(Select three answers)*

- ☐ thomas-garcia-pc
- ☑ roger-spence-pc
- ☑ emil-palmer-pc
- ☑ coral-alvarez-pc

---

3. Which IP address does the signin.office365x24.com domain resolve to?

- ☐ 10.0.29.22
- ☐ 10.0.0.222
- ☐ 45.32.8.8
- ☑ 40.100.174.34

---

4. How many POST requests were made to the signin.office365x24.com domain?

- ☐ 8
- ☐11
- ☐1
- ☑3

---

5. What is the target URL of the POST requests made to signin.office365x24.com?

- ☐ http://accounts-google.com/login.php
- ☐ http://office365x24.com/login.exe
- ☐ http://accounts-google.com/login.txt
- ☑ http://signin.office365x24.com/login.php

---

6. Which domains does the IP address 40.100.174.34 resolve to? *(Select two answers)*

- ☑ signin.office365x24.com
- ☑ signin.accounts-gooqle.com
- ☐ euw.adserver.snapads.com
- ☐ cloud2.xdnscloud.com

Key Takeaways

In this activity, I used Chronicle to investigate a suspicious domain associated with a phishing email. By leveraging Chronicle's features, I was able to:

- Access threat intelligence reports to assess the domain’s reputation.
- Identify the assets that interacted with the domain.
- Evaluate the HTTP events, including POST requests, associated with the domain.
- Determine which assets submitted login information to the domain.
- Uncover additional domains linked to the resolved IP address.
