Activity Overview

In this activity, you will use Chronicle, a cloud-native tool, to investigate a security incident involving phishing and answer a series of questions.
You've learned about how SIEM tools like Chronicle provide a platform for collecting, analyzing, and reporting on data from different data sources. As a security analyst, you'll use SIEM tools to identify and respond to security incidents.
Please note that this activity is optional and will not affect your completion of the course.

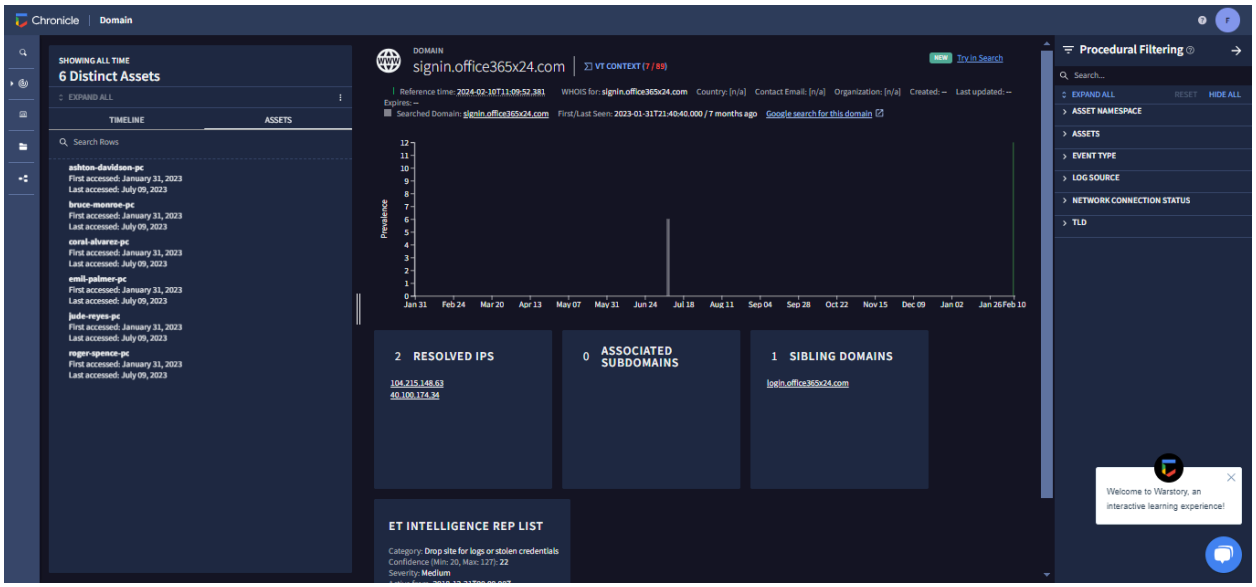
Scenario

Review the following scenario. Then complete the step-by-step instructions.
You are a security analyst at a financial services company. You receive an alert that an employee received a phishing email in their inbox. You review the alert and identify a suspicious domain name contained in the email's body: **`signin.office365x24.com`**. You need to determine whether any other employees have received phishing emails containing this domain and whether they have visited the domain. You will use Chronicle to investigate this domain.

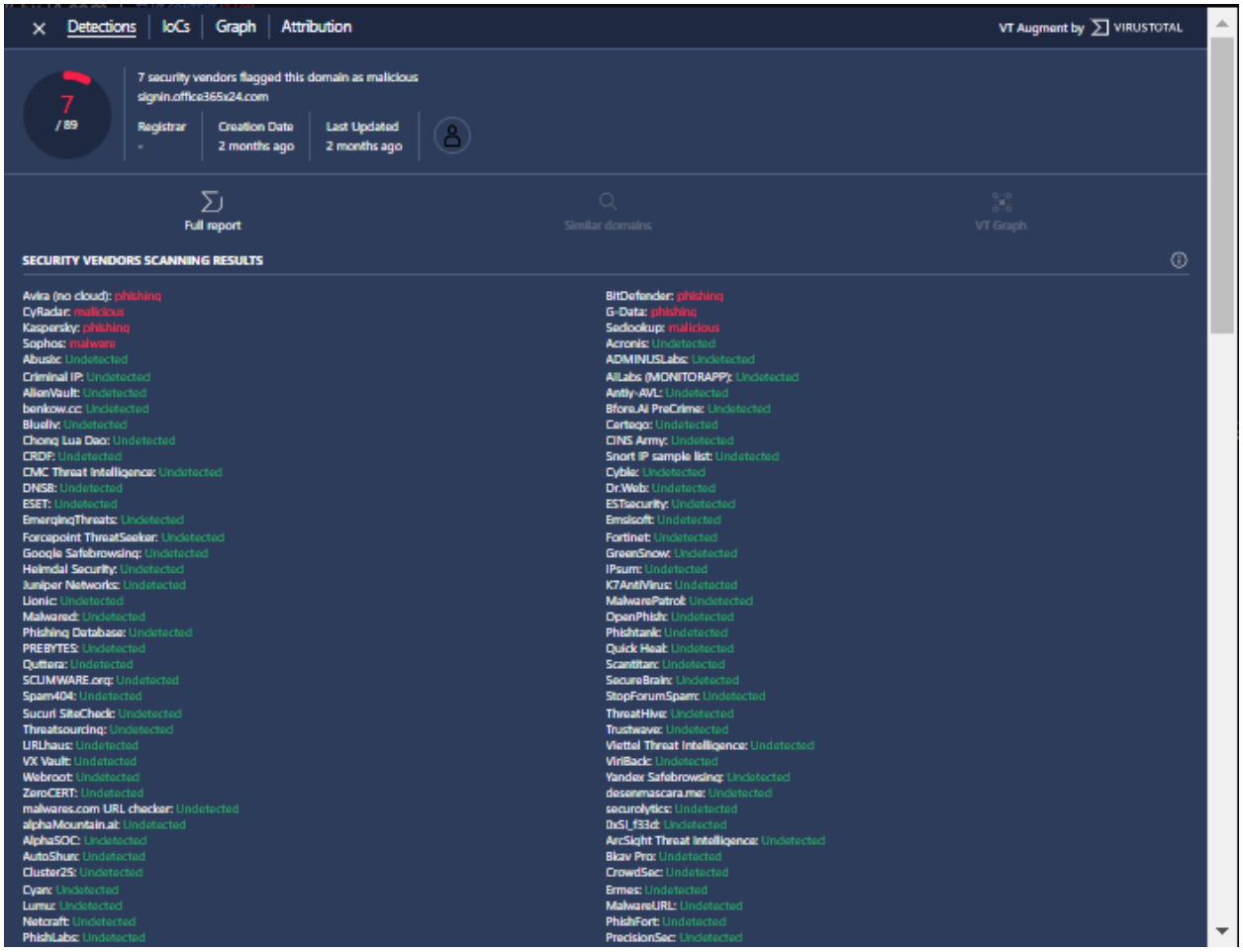
Step-by-step

1. Launch Chronicle.
2. Perform a domain search.

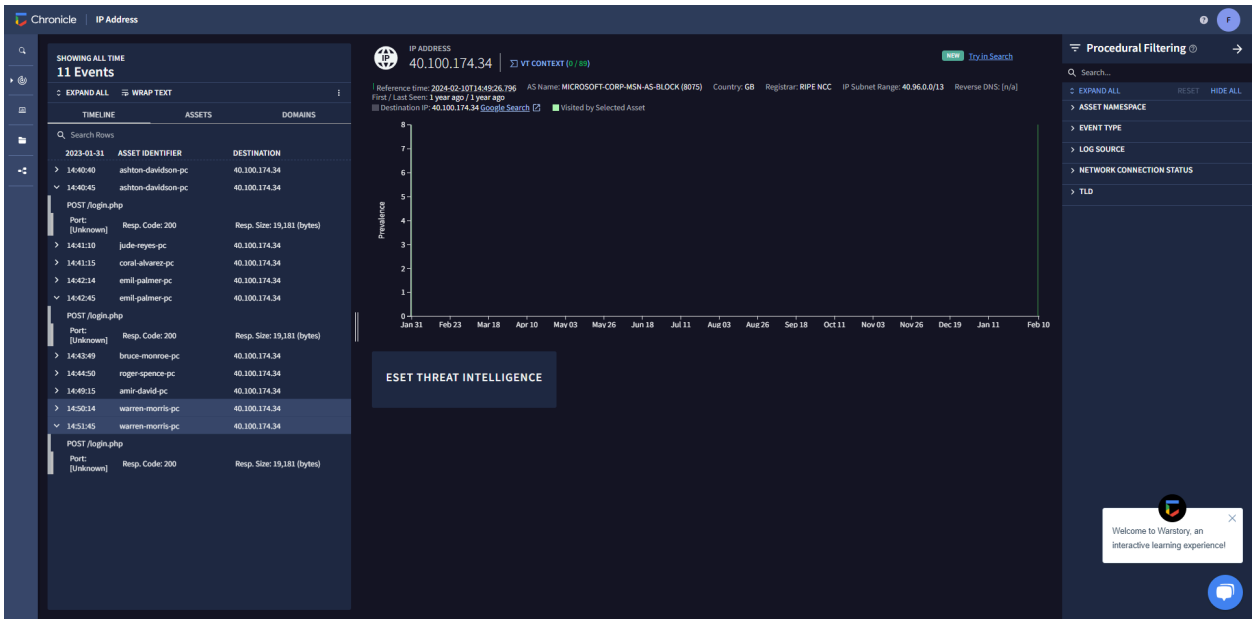
- In the search bar, type `signin.office365x24.com` and click Search. Under `DOMAINS`, click signin.office365x24.com to complete the search. Below are the screenshots of the legacy view, VT, and IP address `40.100.174.34`.
    - Image 1 Legacy View



- Image 2 VT



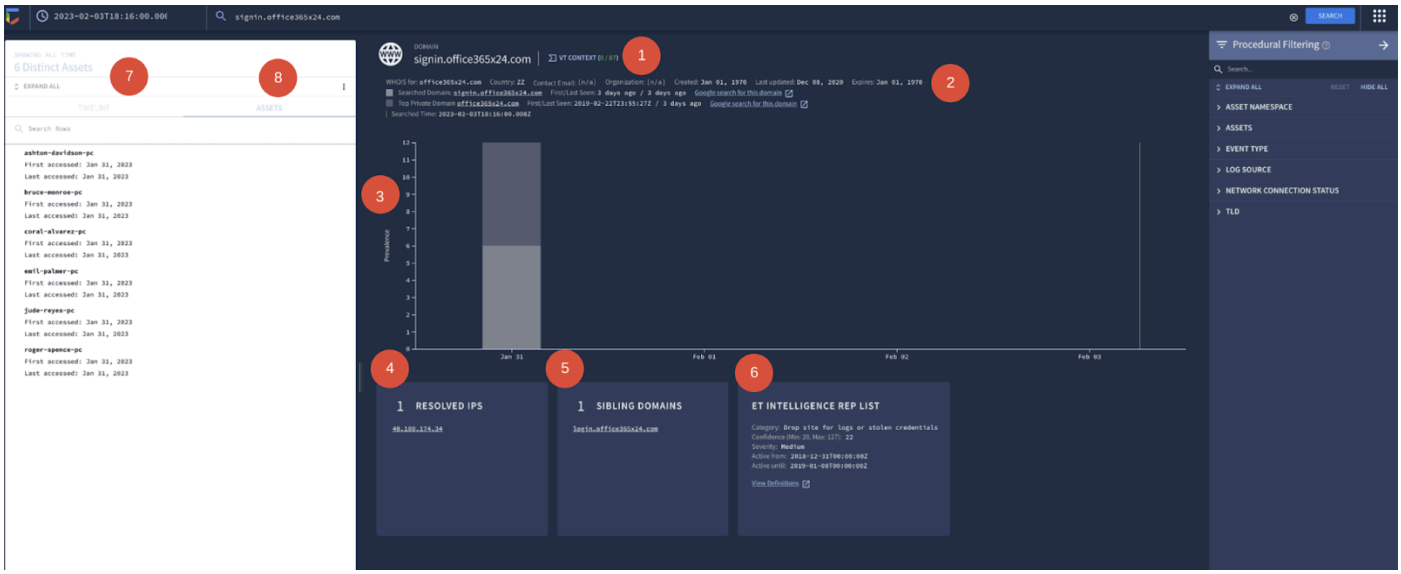
- Image 3 IP address 40.100.174.34



Step 3. After performing a domain search, you'll be in the domain view. Evaluate the search results and observe the following:

1. VT CONTEXT: This section provides the VirusTotal information available for the domain.
2. WHOIS: This section provides a summary of information about the domain using WHOIS, a free and publicly available directory that includes information about registered domain names, such as the name and contact information of the domain owner. In cybersecurity, this information is helpful in assessing a domain's reputation and determining the origin of malicious websites.
3. Prevalence: This section provides a graph which outlines the historical prevalence of the domain. This can be helpful when you need to determine whether the domain has been accessed previously. Usually, less prevalent domains may indicate a greater threat.
4. RESOLVED IPS: This 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`**. Clicking on this IP will run a new search for the IP address in Chronicle. Insight cards can be helpful in expanding the domain investigation and further investigating an indicator to determine whether there is a broader compromise.
5. SIBLING DOMAINS: This insight card provides additional context about the domain. Sibling domains share a common top or parent domain. For example, here the sibling domain is listed as **`login.office365x24.com`**, which shares the same top domain **`office365x24.com`** with the domain you're investigating: **`signin.office365x24.com`**.
6. Click TIMELINE. This tab provides information about the events and interactions made with this domain. Click EXPAND ALL to reveal the details about the HTTP requests made including **`GET`** and **`POST`** requests. A GET request retrieves data from a server while a POST request submits data to a server.

7. Click ASSETS. This tab provides a list of the assets that have accessed the domain.

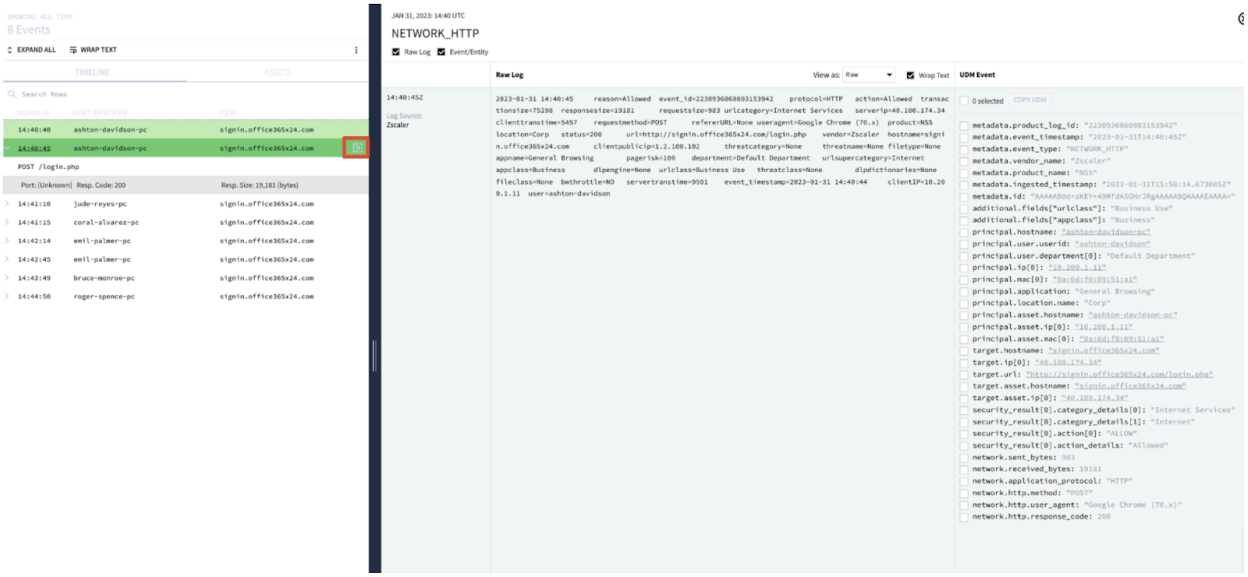


Step 4. Now that you've retrieved results for the domain name, the next step is to determine whether the domain is malicious. Chronicle provides quick access to threat intelligence data from the search results that you can use to help your investigation. Follow these steps to analyze the threat intelligence data and use your incident handler's journal to record interesting data:

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.
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.

Step 5. Information about the events and assets relating to the domain are separated into the two tabs: TIMELINE and ASSETS. TIMELINE shows the timeline of events that includes when each asset accessed the domain. ASSETS list hostnames, IP addresses, MAC addresses, or devices that have accessed the domain. Investigate the affected assets and events by exploring the tabs:

1. ASSETS: There are several different assets that have accessed the domain, along with the date and time of access. Using your incident handler's journal, record the name and number of assets that have accessed the domain.
2. TIMELINE: Click EXPAND ALL to reveal the details about the HTTP requests made, including **`GET`** and **`POST`** requests. The **`POST`** information is especially useful because it means that data was sent to the domain. It also suggests a possible successful phish. Using your incident handler's journal, take note of the **`POST`** requests to the **`/login.php`** page. For more details about the connections, open the raw log viewer by clicking the open icon.



Step 6. So far, you have collected information about the domain's reputation using threat intelligence, and you've identified the assets and events associated with the domain. Based on this information, it's clear that this domain is suspicious and most likely malicious. But before you can confirm that it is malicious, there's one last thing to investigate.

Attackers sometimes reuse infrastructure for multiple attacks. In these cases, multiple domain names resolve to the same IP address.

Investigate the IP address found under the RESOLVED IPS insight card to identify if the **`signin.office365x24.com`** domain uses another domain. Follow these steps:

1. Under RESOLVED IPS, click the IP address **`40.100.174.34`**.
2. Evaluate the search results for this IP address and use your incident handler's journal to take note of the following:
    a. TIMELINE: Take note of the additional **`POST`** request. A new **`POST`** suggests that an asset may have been phished.
    b. ASSETS: Take note of the additional affected assets.
    c. DOMAINS: Take note of the additional domains associated with this IP address.

Step 7: Answer questions about the domain investigation

- According to ET Intelligence Rep List, `signin.office365x24.com` is categorized as "Drop site for logs or stolen credentials".
- The following assets are those who accessed the domain:
    - `ashton-davidson-pc`
    - `bruce-monroe-pc`
    - `coral-alvarez-pc`
    - `emil-palmer-pc`
    - `jude-reyes-pc`
    - `roger-spence-pc`
- We found 2 IP addresses that map to `signin.office365x24.com`: `104.215.148.63` & `40.100.174.34`.
- The IP address `40.100.174.34` resolves to `signin.office365x24.com` and `signin.accounts-google.com`.

- As we can see from image 2 above, there are three `POST` requets made to `40.100.174.34`.
- Some `POST` requests were made to `signin.office365x24.com`. Their target URL of the web page were sent to `http://signin.office365x24.com/login.php`.