Query For Events with Chronicle and Splunk

SPLUNK
index=main fail
index=main: This is the beginning of the search command that tells Splunk to retrieve events from an *index* named *main*. An index stores event data that's been collected and processed by Splunk.*fail*: This is the search term. This tells Splunk to return any event that contains the term *fail*.

index=main fail | chart count by host
chart count by host: This command tells Splunk to transform the search results by creating a chart according to the count or number of events. The argument by host tells Splunk to list the events by host, which are the names of the devices the events come from. This command can be helpful in identifying hosts with excessive failure counts in an environment.

CHRONICLE
metadata.event_type = "USER_LOGIN"
metadata.event_type = "USER_LOGIN": This UDM field *metadata.event_type* contains information about the event type. This includes information like timestamp, network connection, user authentication, and more. Here, the event type specifies *USER_LOGIN*, which searches for events relating to authentication. Using just the metadata fields, you can quickly start searching for events

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.

Note: *Use the incident handler's journal you started in a previous activity*

to take notes during the activity and keep track of your findings.

Step-By-Step Instructions

Follow the instructions and answer the series of questions to complete the activity.

Click the link to launch Chronicle

.

On the Chronicle home page, you'll find the current date and time, a search bar, and details about the total number of log entries. There are already a significant number of log events ingested into the Chronicle instance.

***Note**: Chronicle supports Google Chrome. You may experience limited functionality if you use browsers like Firefox, Edge, or Safari. For the best experience using Chronicle, [install the latest version of Chrome]*

.

To begin, complete these steps to perform a domain search for the domain contained in the phishing email. Then, search for events using information like hostnames, domains, IP addresses, URLs, email addresses, usernames, and file hashes.

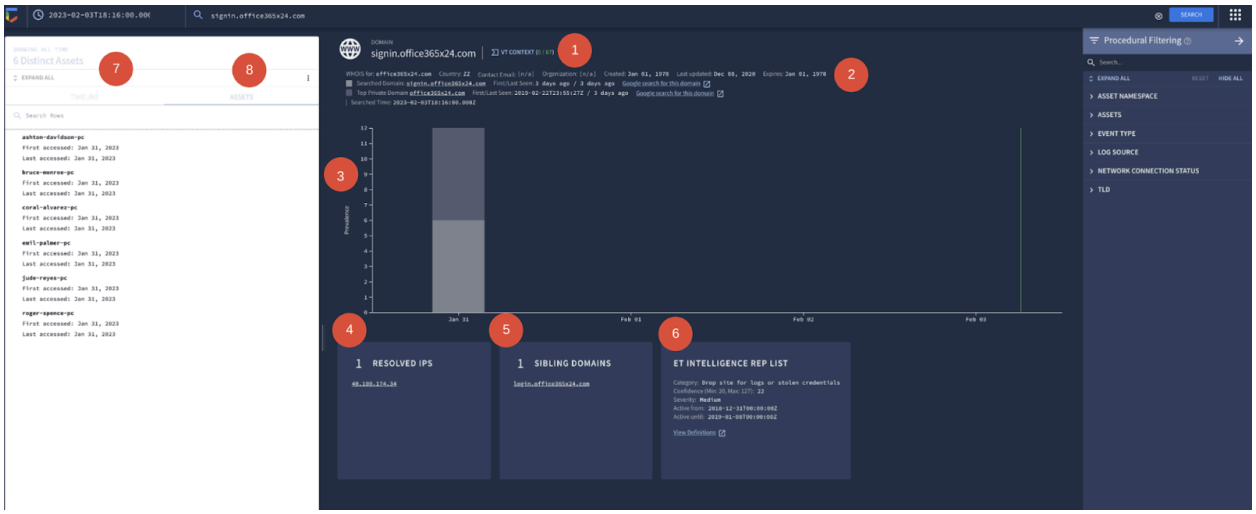
1. In the search bar, type *signin.office365x24.com* and click **Search**. Under **DOMAINS**, *signin.office365x24.com* will be listed. This tells you that the domain exists in the ingested data.
2. Click *signin.office365x24.com* to complete the search.
3. Click *Go to Legacy View* to use the original chronicle interface.

**Note: These instructions are to be updated for the new Chronicle interface*

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. **ET INTELLIGENCE REP LIST**: This insight card includes additional context on the domain. It provides threat intelligence information, such as other known threats related to the domains using ProofPoint's Emerging Threats (ET) Intelligence Rep List.
7. 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.
8. Click **ASSETS**. This tab provides a list of the assets that have accessed the domain.



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:

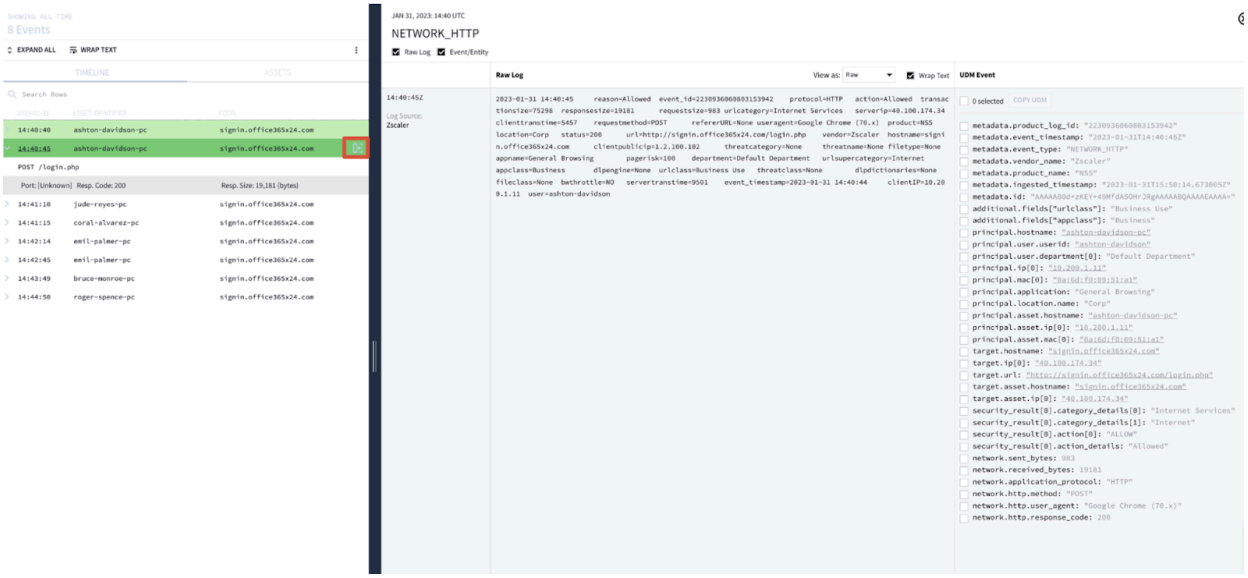
1. Click on **VT CONTEXT** to analyze the available VirusTotal information about this domain. There is no VirusTotal information about this domain. To exit the VT CONTEXT window, click the **X**.

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

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.



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:
    1. **TIMELINE**: Take note of the additional *POST* request. A new *POST* suggests that an asset may have been phished.
    2. **ASSETS**: Take note of the additional affected assets.
    3. **DOMAINS**: Take note of the additional domains associated with this IP address.