Perform a Query with Chronicle

Scenario

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.

Project Description

Creating effective searches is an important skill because it enables you to quickly and accurately find the information you are looking for within a large amount of data. Quick and accurate searching is especially useful during incident response, because you might need to swiftly identify and address a security incident. Effective search techniques also help you efficiently identify patterns, trends, and anomalies within data.

Launch Chronicle

- 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.

Perform a Domain Search

- In the search bar, type *signin.office365x24.com* and click **Search**. Under **DOMAINS**, *signin.office365x24.com* will be listed. This shows that the domain exists in the ingested data.
- Click *signin.office365x24.com* to complete the search.

Evaluate Search results

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

Investigate the Threat intelligence data

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

Investigate the affected assets and events by exploring the tabs:

- **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.
- **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.

Investigate the resolved IP address:

- Under **RESOLVED IPS**, click the IP address *40.100.174.34*.
- 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.

Access threat intelligence reports on the domain

- Identify the assets that accessed the domain
- Evaluate the HTTP events associated with the domain
- Identify which assets submitted login information to the domain
- Identify additional domains