Perform 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.

**Background:**

Chronicle is an open-source SIEM tool, a product of Google. It allows to search based on 2 sceanrio’s .

1. Unified data motel search (UDM search) – This is for searching the data after its being normalized.
2. Raw Log search – It allows to search from the all the raw logs

Below are the some fields that helps the determine the criticality, type of malware and all the information required.

Search results can be evaluated using the below fields:

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.

**Steps to Access Chronicle for investigating domain:**

1. Visit the Chronicle website

A screenshot of a computer

Description automatically generated

1. In the search field provide the email’s body and enter search. The below screen appears

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

**Observations:**

According to ET Intelligence Rep List signin.office365x24.com categorized as Drop site for logs or stolen credentials.

Assets accessed the signin.office365x24.com domain are ashton-davidson-pc , bruce-monroe-pc , coral-alvarez-pc , emil-palmer-pc , jude-reyes-pc and roger-spence-pc

IP address signin.office365x24.com domain resolve to are 104.215.148.63 and 40.100.174.34

HTTP POST requests were made to the signin.office365x24.com domain are 2 and the requests made are for website <http://signin.office365x24.com/login.php>

The domains IP address 40.100.174.34 resolve to are signin.accounts-googlecom and signin.office365\*24.com which can be accessed by clicking the IP address under Resolved Tips