**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.

***Note***: *Use the incident handler's journal you started in* [*a previous activity*](https://www.coursera.org/learn/detection-and-response/exam/ghRgc/portfolio-activity-document-an-incident-with-an-incident-handlers-journal) *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.

Step 1: Launch Chronicle

Click the link to launch [Chronicle](http://goo.gle/chroniclelab).

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*](https://www.google.com/chrome/)*.*

Step 2: Perform a domain search

Step 3: Evaluate the search results

Step 4: Investigate the threat intelligence data

Step 5: Investigate the affected assets and events

Step 6: Investigate the resolved IP address

Step 7: Answer questions about the domain investigation

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

Drop site for logs or stolen credentials

Phishing site

Command and control server

Spam site

1. Which assets accessed the **signin.office365x24.com** domain? Select three answers.

**roger-spence-pc**

**coral-alvarez-pc**

**thomas-garcia-pc**

**emil-palmer-pc**

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

**10.0.29.22**

**10.0.0.222**

**40.100.174.34**

**45.32.8.8**

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

11

1

8

3

1. Some **POST** requests were made to **signin.office365x24.com**. What is the target URL of the web page that the **POST** requests were made to?

**http://office365x24.com/login.exe**

**http://accounts-gooqle.com/login.php**

**http://accounts-gooqle.com/login.txt**

**http://signin.office365x24.com/login.php**

1. Which domains does the IP address **40.100.174.34** resolve to? Select two answers.

**signin.accounts-gooqle.com**

**euw.adserver.snapads.com**

**cloud2.xdnscloud.com**

**signin.office365x24.com**