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.

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.