Perform **Splunk** Query, Evaluate search results, Locate Failed login

The lab focus is on using Splunk, a SIEM tool, to analyze data from Buttercup Games' mail servers and identify possible security issues. I performed searches using Splunk's querying language to narrow down the events and find failed SSH logins for the root account on the mail server.

For each event the fields are host, source, and sourcetype.
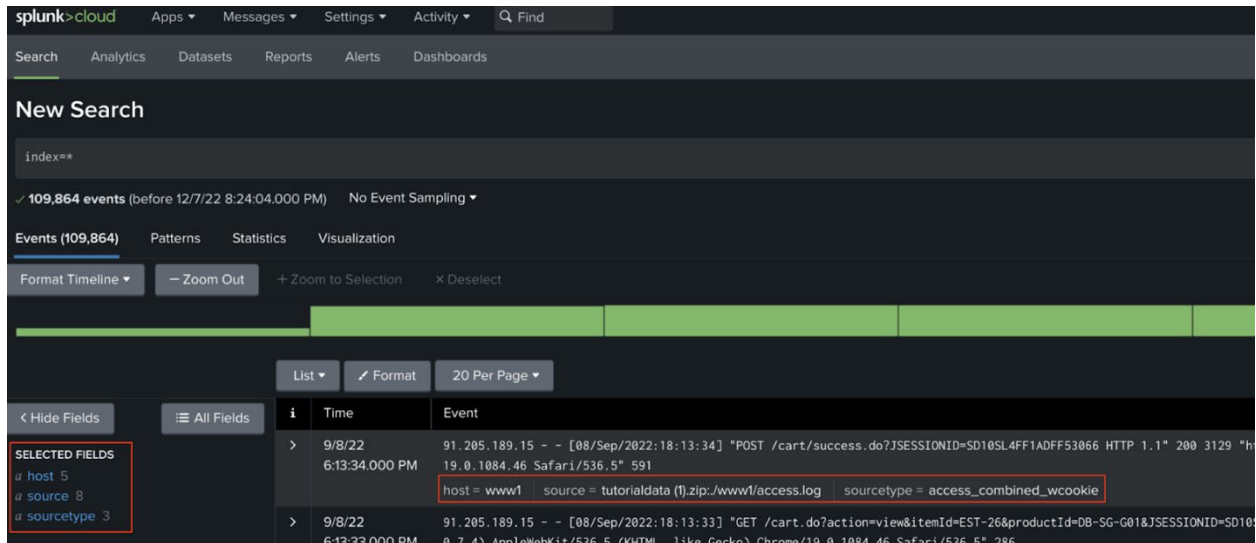
- **host**: specifies the name of the network host from which the event originated. In this search there are five hosts:

  - **mailsv** - Buttercup Games' mail server. Examine events generated from this host.

  - **www1** - This is one of Buttercup Games' web applications.

  - **www2** - This is one of Buttercup Games' web applications.

  - **www3** - This is one of Buttercup Games' web applications.

  - **vendor_sales** - Information about Buttercup Games' retail sales.

- **source**: The source field indicates the file name from which the event originates. You should identify eight sources. Notice **/mailsv/secure.log**, which is a log file that contains information related to authentication and authorization attempts on the mail server.

- **sourcetype**: The sourcetype determines how data is formatted. You should observe three sourcetypes. Examine **secure-2**.

While completing this activity, I learned how to upload data into Splunk for analysis. I also gained experience in using Splunk's search functionality and learned about the importance of effective search techniques in incident response and data analysis. Additionally, I familiarized myself with Splunk's interface, including the app panel, Explore Splunk panel, and Splunk bar. These skills will be valuable for me as a cybersecurity professional, as Splunk is a widely used SIEM tool in the industry for managing and analyzing security-related data.

Perform **Chronicle** Query, Evaluate search results, Locate Failed login

The lab focus is on using Chronicle, a cloud-native tool, to investigate a security incident involving a phishing email. As a security analyst at a financial services company, I received an alert about an employee receiving a phishing email. The goal is to determine whether other employees received similar emails and if they visited the suspicious domain mentioned in the email. By using Chronicle, I can search for the domain, analyze threat intelligence data, explore affected assets and events, and investigate related IP addresses.

Evaluating the search results:
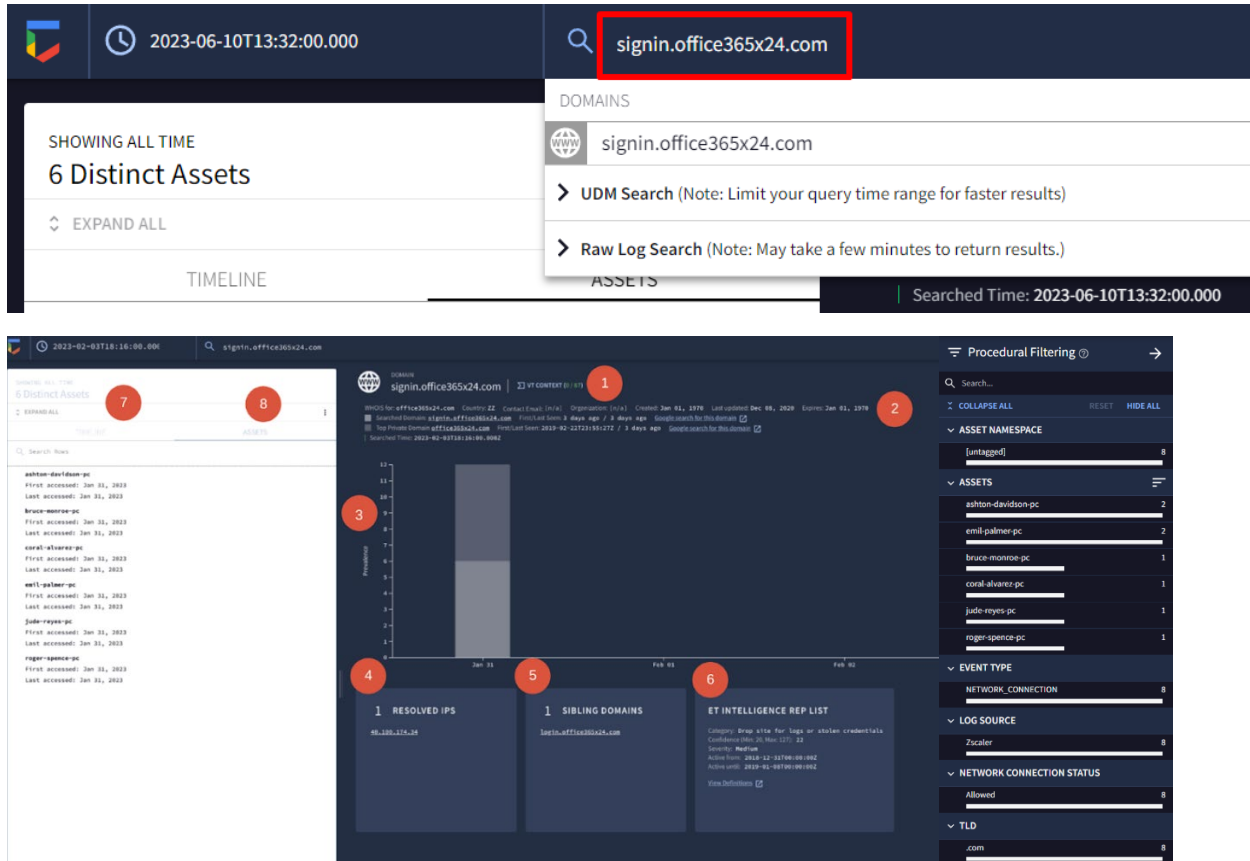
1. **VT CONTEXT**: This section provides the VirusTotal information available for the domain.

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. **TIMELINE**. This tab provides information about the events and interactions made with this domain.

    EXPAND ALL 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. **ASSETS**. This tab provides a list of the assets that have accessed the domain.

TIMELINE → 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.

Conclusion

Completing this activity, I learned several important skills. First, I gained hands-on experience using SIEM tools to investigate a security incident. I learned how to search for specific domains, analyze threat intelligence information, and explore asset and event details. This activity also enhanced my understanding of phishing incidents and their indicators, such as suspicious domains and HTTP requests. I practiced documenting my findings in an incident handler's journal, which is crucial for maintaining a record of the investigation process. Overall, this activity strengthened my ability to detect and respond to security incidents effectively using SIEM tools and threat intelligence data.