Lab: False Positives

# Learning Objectives:

* Gain an understanding of how to identify the differences between false positives and real threats within the company.
* Search through alerts to understand what populates the threats and why they are populated.
* Understanding the differences between false positives and real threats will assist you in optimizing your SIEM appropriately.

# Overview:

You are doing a security audit of all the threats that transpired in your company Glass inc. Going through the alerts, you notice malware executable (.exe) files flagging in your alerts and then you notice company files like Excel Spreadsheets flagging as a malicious file. Going through all the alerts you notice there is an alarming amount of false positives between real threats. False positives account for nearly half of all alerts causing a lot of noise and concerns over determining what is a real threat versus a fake threat. Your goal is to assess what alerts stand out as false positives and what alerts stand out as true threats.

# Scenario:

It is the end of the month when you, a security analyst, perform security audits to assess the threats that have alarmed within your company. You go through ABC\_CloudHosting, 123\_RETAIL\_TEST, and XYZ\_CONSULTING and begin to note the amount of threats, the severity of threats, the event types, the workstations, IP and MAC addresses, and the files that flagged the alerts.

Going through the file names, you notice that there are a couple of files that are safe files used by employees that have been flagged as a threat. There are document and excel files that are apparent to be legitimate work files while there are some document and excel files that are malicious malware files. With this in mind, you report to your reporting supervisor to discuss the concerns about false positives and the discovery of legitimate files flagging as malicious malware.

You are assigned to evaluate the files and search for any discrepancies that could aid in your investigation for false positives.

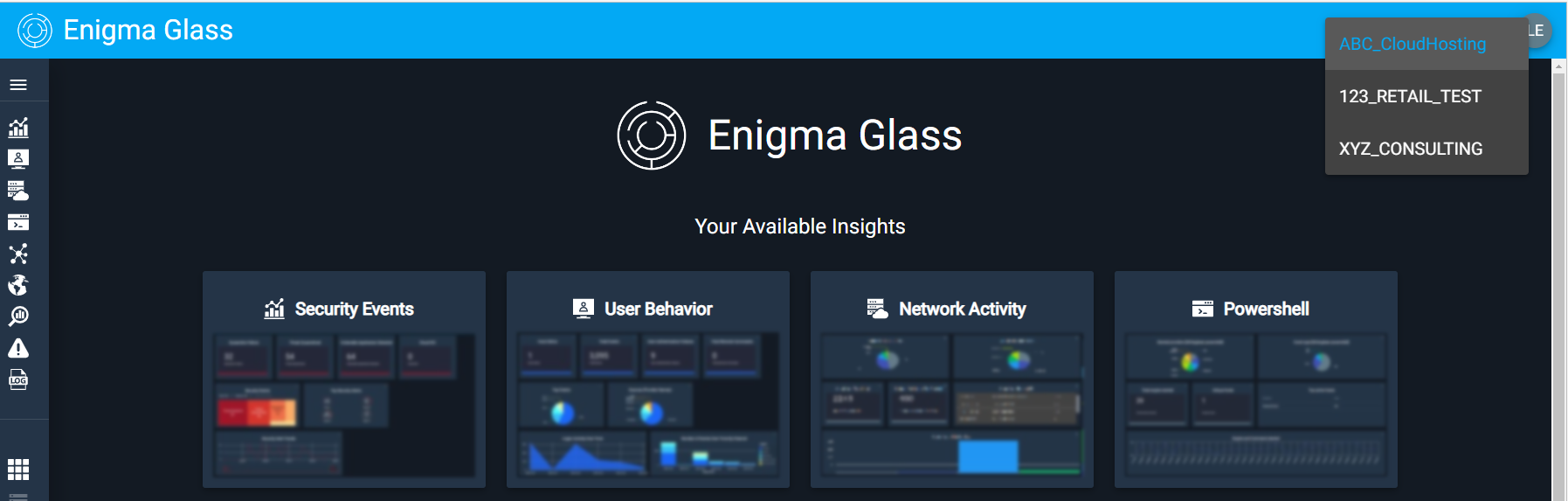
# SIEM Workflow Module:

In this module you will use artifacts from the SIEM (Enigma Glass) to find out more about a specific threat identified within your environment. Read through the below steps and record your answer for each **Question** **(4)** in the SIEM Workflow Module of this lab guide.

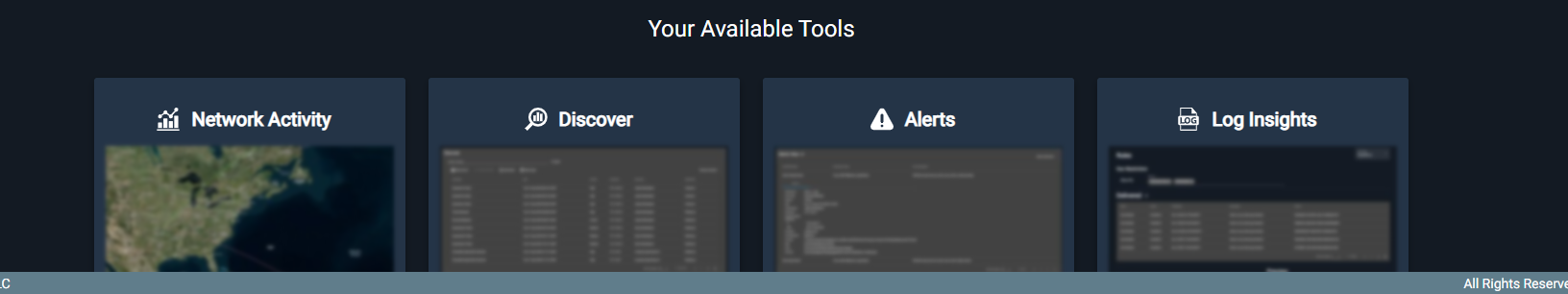
*Steps:*

1. Log into Enigma Glass: <https://www.enigmaglass.com/>

* Set the dataset to ‘ABC\_CloudHosting on the upper-right corner



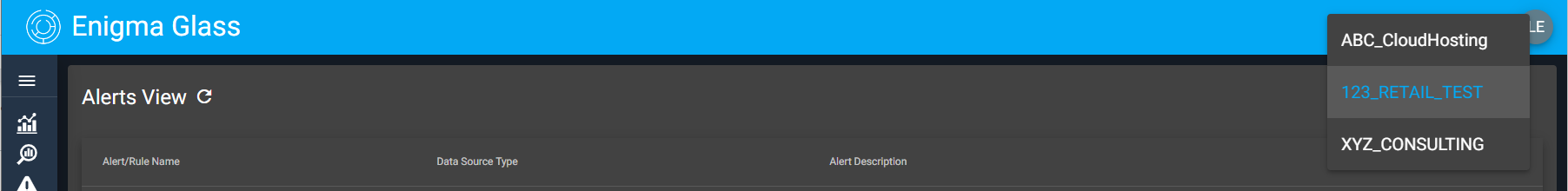
1. Go down the side tab and click on the ‘Alerts’ page or click the ‘Alerts’ tab under ‘Your Available Tools’.



.

* **Question 1:** In total, how many alerts are there?
* Answer:
* **Question 2:** Looking at each event, are there any events that stand out to you as a possible false alarms? (*Hint:* *Official Business Documents are comprised of invoices and spreadsheets about salary)*
* Answer:
* **Question 3:** What helped you determine what files were false positives and what files were malicious files?
* Answer:

1. Set the database to ‘123\_RETAIL\_TESTlon the upper-right corner.



* **Question 4:** Do you think Urgent.doc is a legitimate document? If not, why? (*Hint: In most cases files that contain details that require you to click on it immediately can be flagged as malicious*)
* Answer:

# Threat Research Module:

1. How many alerts in total do you think are false positives? How many alerts in total are there that are legitimate alerts?
2. What are the negative effects of dealing with false positives?
3. What could you change or implement to help deal with false positives?
4. Are there any other methods to identify false positives? If yes, what are the other methods?

# 

# Threat Intelligence Report:

| **CATEGORY** | **DESCRIPTION** | **HINT** |
| --- | --- | --- |
| **Event** (general - what type of event occurred against your organization) |  | *Quick overview of the event. You can find this information in in the alerts pane of Enigma Glass and through your analysis* |
| **Target** |  | *You can find this information in the alerts pane of Enigma Glass* |
| **Attack Type** |  | *Internet Research; What type of campaign was this?* |
| **Remediation Actions** |  | *Read* the *following article to determine* [*remediation actions*](https://www.ironnet.com/blog/a-practical-way-to-rule-out-false-positives) |
| **Preventative Actions** (Lessons Learned) |  | *Internet Research: List some potential security measures that could prevent this type of event* |

|  |
| --- |