

Lab: Data Integrity

# Background:

You work as a Cybersecurity Analyst for an up and coming cloud computing company. One (out of many) of your daily responsibilities as an analyst is to review your company's SIEM (security information event management) alerts for signs of abnormal or malicious activity. Some events pose a threat to the integrity of company data.

# Scenario:

One morning while monitoring security events, you notice there have been a few alarming things. The first thing that draws your attention is how many times some users have triggered the AV. This could mean a serious risk for data integrity of the company since malware can pose a threat to modifying existing files on the workstations of authorized users. Being the cybersecurity expert that you are, you take a closer look at this to get to the root cause.

# Notes:

ENSURE YOU ARE MONITORING **ABC\_CloudHosting**

1. Log into Enigma Glass using the provided account: <https://www.enigmaglass.com/>
   1. Set the dataset to “ABC\_CloudHosting” in the upper right hand corner of the screen.





1. Click on “Security Events” on the left hand panel.

# 

# 

# Lab Questions:

1. Which user had the most events?
2. Did that host have any event trigger that may pose a threat to the integrity of his existing files? If so, what was the file name and type?
3. Are there any files in the list that look like they may contain sensitive information? If so, can you name one that is of critical severity?
4. What are some signs that your data could be at risk?
5. BONUS: What are the names of the 6 different types of data integrity?

|  |
| --- |