Lab: Data Integrity

# Learning Objectives:

* Gain an understanding of data integrity issues, as well as the risks associated with data integrity loss
* Utilize the SIEM platform to investigate for signs of data integrity loss

# 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.

# SIEM Workflow Module:

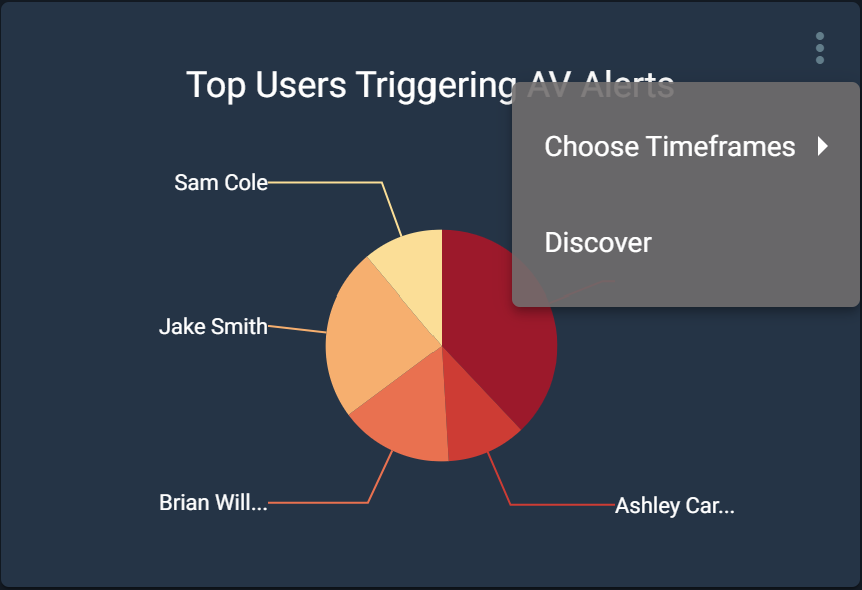
This lab uses data in the Enigma Glass SIEM to find information pertaining to a specific threat in the environment. Read through the below steps, and record your answer for each **Question** in the SIEM Workflow Module of this lab guide.

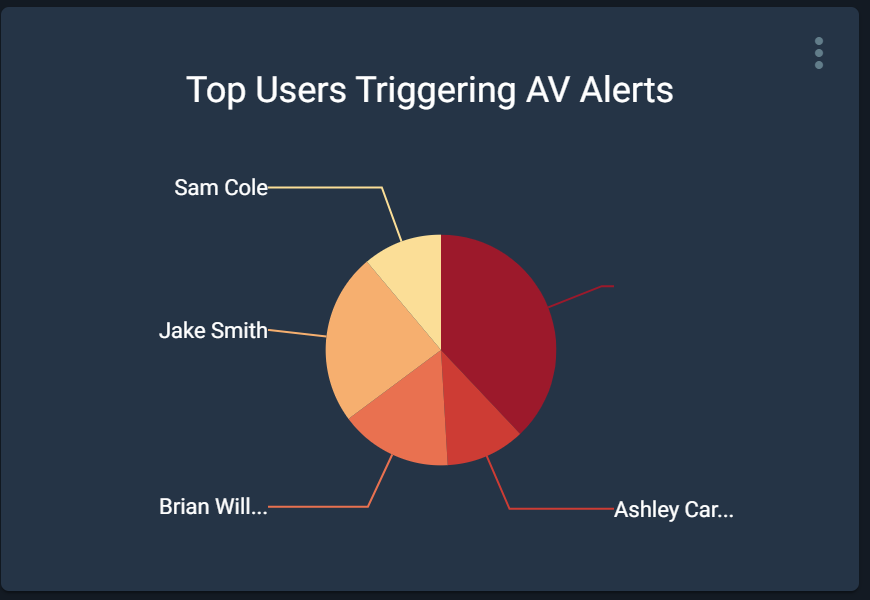
ENSURE YOU ARE MONITORING **ABC\_CloudHosting**

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.
2. Navigate to the “Top Users Triggering AV Alerts” Panel. Click on the three vertical dots, and click on “Discover”



**Question 1: Which user had the most events? How many events did they have?**

1. Next to the Quick Search text box, click “To Advanced”



1. In the search tab, enter the name of the user from Question 1 and hit enter.

**Question 2: Did that user have any event triggers that may pose a threat to the integrity of their existing files? If so, what was the file name and type?**

1. Next, clear the search results so you can view the entire dataset. (Hint: Adjust your view to show 100 records per page)

**Question 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?**

# Threat Research Module:

1. What are some signs that your data could be at risk?
2. What would the impact of a data integrity issue be?
3. How can the company protect themselves from data integrity issues?
4. BONUS: What are the names of the 6 different types of data integrity?

# 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://practical365.com/security/remediating-account-breaches-in-office-365/) |
| **Preventative Actions** (Lessons Learned) |  | *Internet Research: List some potential security measures that could prevent this type of event* |

|  |
| --- |