Lab: Insider Threat

# 

# Learning Objectives:

* Gain an understanding of the background, issues, and threats posed by attacks occurring from within the company
* Gain knowledge of the SIEM platform, and the uses of said platform
* Discuss and learn mitigation strategies for preventing insider threat attacks

# Overview:

You work in the IT department of a mid sized company. The company, Glass inc., has expressed fears over falling victim to an insider attack. Recently, the IT team has noted a surge of failed login attempts for the “admin” and “test” username. This has raised concerns that an employee has been attempting to access data that their account would not normally be granted access to. Working in IT, you understand that insider threats account for approximately 60% of data breaches. With this knowledge in mind, you are tasked with detecting the threat using the various tools and resources at your disposal.

# Scenario:

Recently, employees have noted a change in the behavior of one of their coworkers, Jake. Jake is normally one of the highest performing employees in the company, but recently his performance has taken a noticeable dip. In addition to this, Jake has been seen getting into verbal confrontations with coworkers. Employees have also noted that Jake has been spending an excessive amount of time on the phone, and he has been overheard mentioning financial issues.

While individually these changes are not a major issue, combined they raise concerns that Jake may plan on misusing company resources. The IT Director has asked you to observe Jake’s activity on the company network, and report anything suspicious.

As soon as you receive this request, you log into the Enigma Glass SIEM to see if you can identify any suspicious activity.

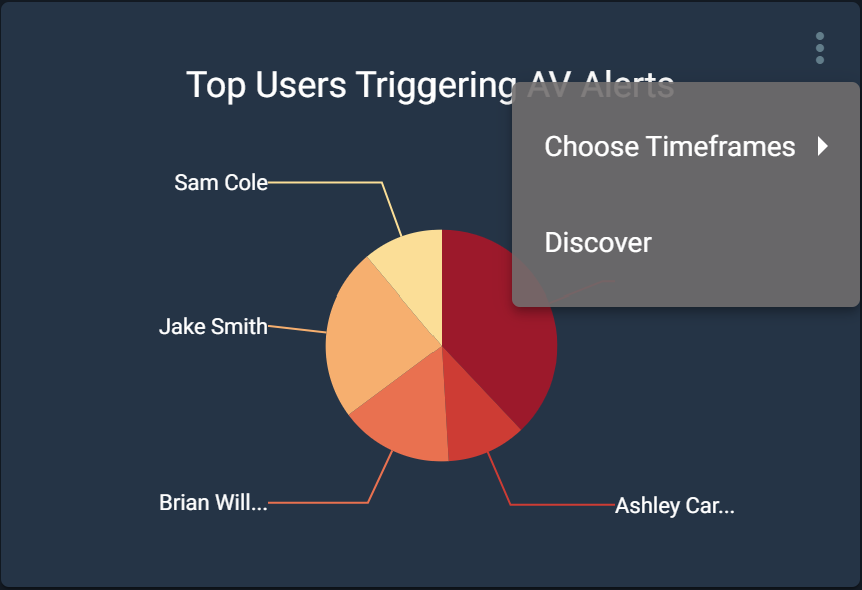
# SIEM Workflow Module:

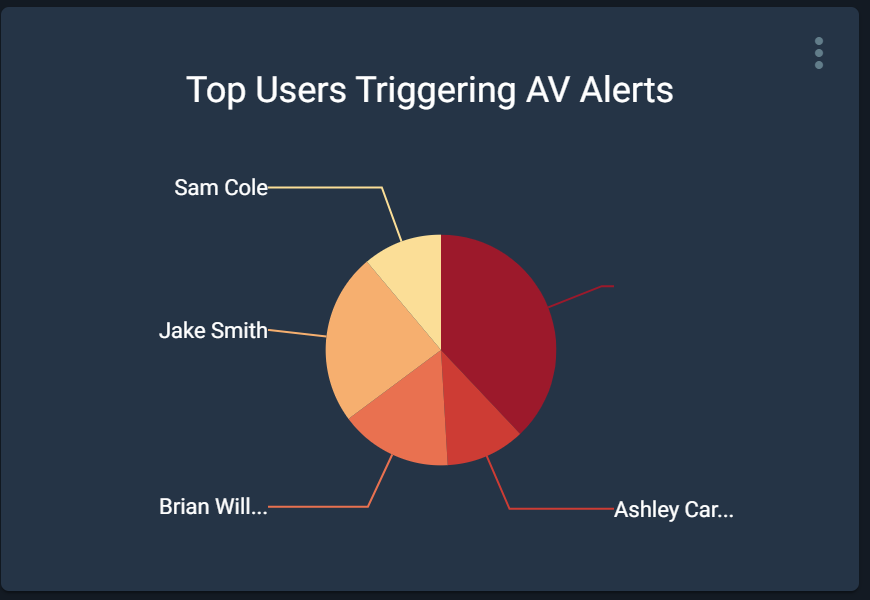
This lab uses data in the Enigma Glass SIEM to find information pertaining to a specific threat in the environment. Read through the below steps, and record your answer for each **Question** in the SIEM Workflow Module of this lab guide.

*Steps:*

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”



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

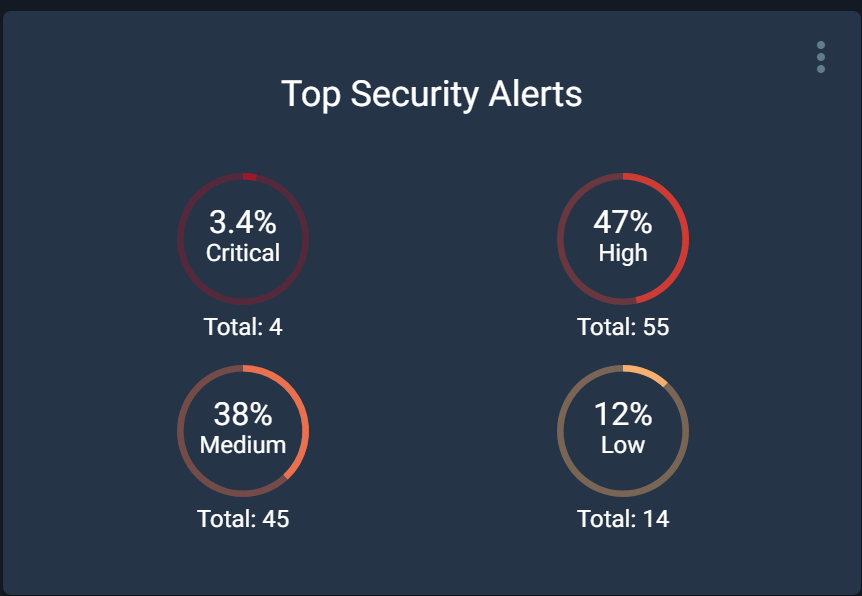


1. Next, in the “Search Strings” text box, type “Jake” and hit enter.

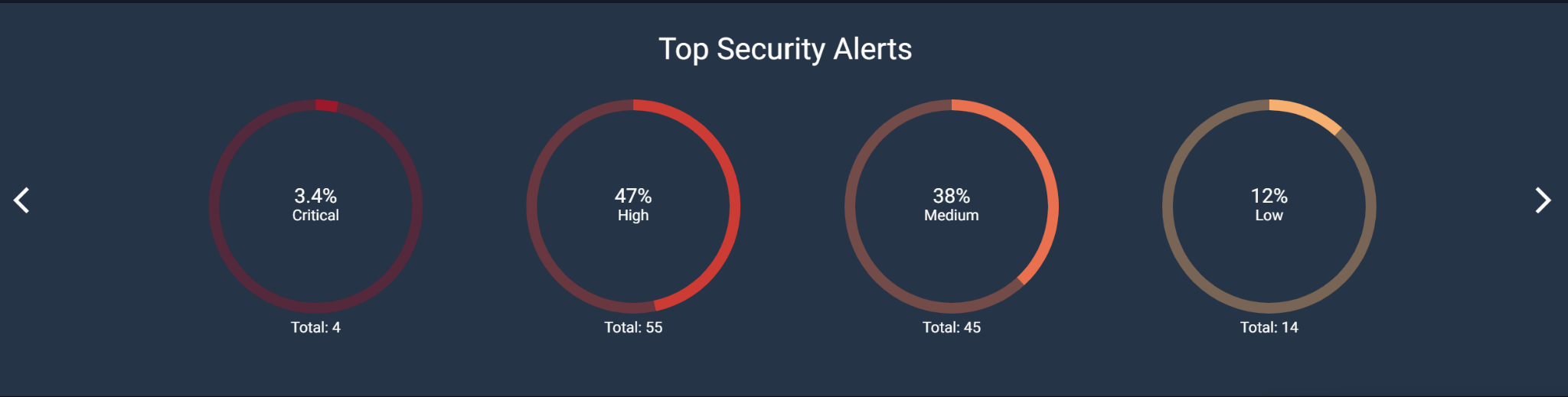
**Question 1: how many alerts were triggered by Jakes-Workstation?**

**Question 2: Do you see any alerts that raise immediate concern? Which ones and why?**

1. Click on “Security Events” in the left hand panel again. 
2. Navigate to the “Top Security Events” panel. Click on the three dots, and click on “Discover”.



1. At the top of the discover panel, you can see a visualization of all the threats in the dataset



**Question 3: How many threats were found on Jakes-Workstation? How many threats are in each category?**

**Question 4: How many alerts from Jakes-Workstation were flagged as Malicious?**

**Question 5: Do you think any alerts are False Positives? Which ones and why?**

# Threat Research Module:

1. Given the activity found on Jakes-Workstation, do you think he is an insider threat? Why or why not?
2. Why are insider threats so difficult to detect?
3. What kind of damage can an insider threat cause?
4. What are some indicators of a potential Insider Threat?
5. Perform some research on Insider Threats. What is the impact of Insider threats industry wide? What are companies doing to attempt to prevent them?
6. What should Glass Inc. do to strengthen their defenses against Insider threats?

# 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* |

|  |
| --- |