# **Enigma Glass documentation**

# Learning Objectives:

* To provide the user with the basic information they need in order to navigate Enigma Glass
* To provide an organized document that can be used as a reference at any time

# Overview:

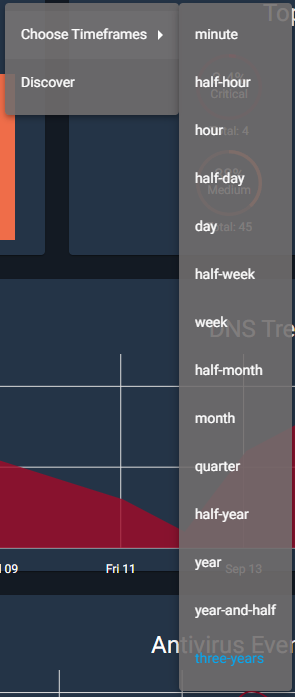
This is a basic document that will drill down into every aspect of Enigma Glass in hopes of providing an easy-to-use resource that can be used to understand the workings of this platform. This resource will be laid out in the order that sections show up on the platform, starting with security events and ending with log insight.

# 

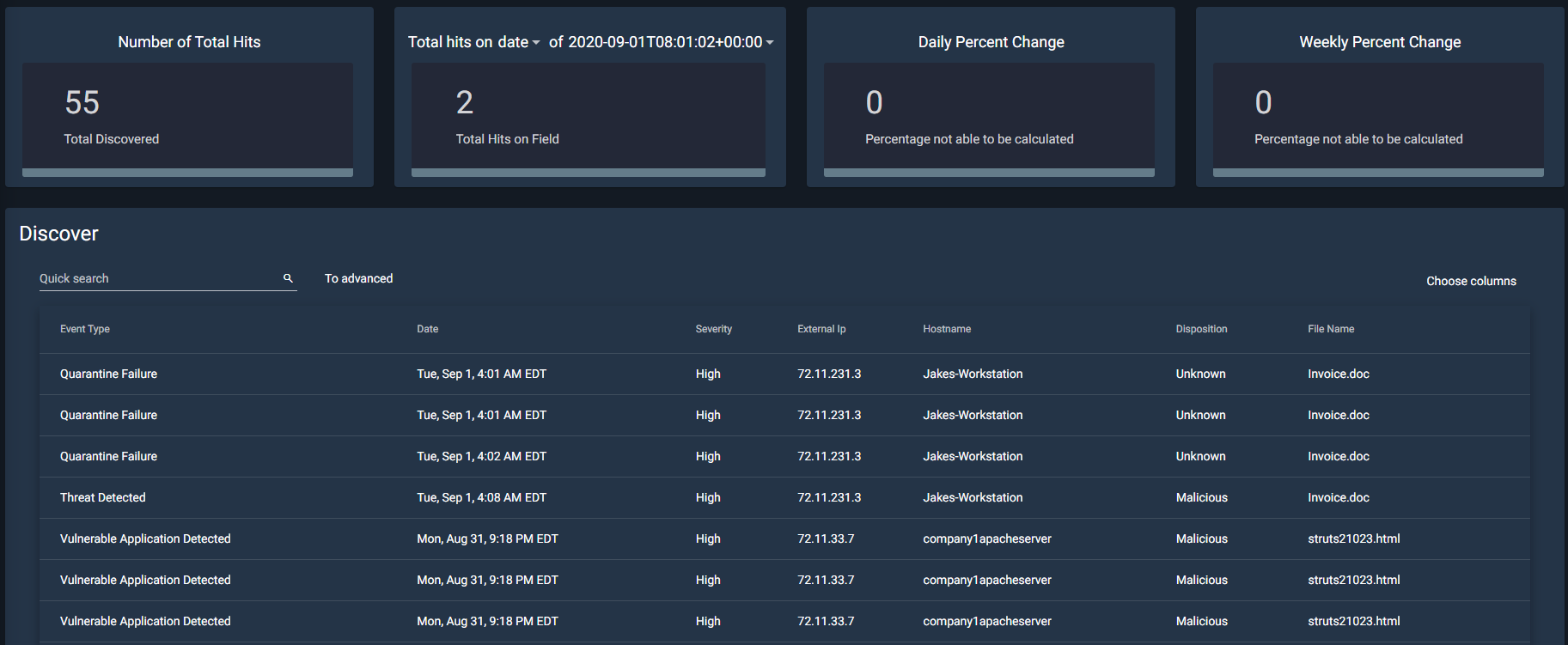
# Security Events:

There are currently 9 different widgets available when you open security events from the dashboard. Each one works similarly to the other; in that, you have the option to “Choose Timeframes” and “Discover.”

The choose timeframes option allows you to choose between 14 different intervals. These intervals will determine the timeframe of the data that the infographic will show. For example, if you have it set to a half-hour, the infographic will only show data that was gathered in the last half-hour. It is also worth noting that the currently selected option is highlighted in blue.



The Discover option is a bit more complex. Choosing this option will take you to a new page as shown below. This page will show you the corresponding infographic as well as the total number of hits for that category. In this example, there were 55 total discovered security events.



| The next tile is especially useful for information gathering. It allows you to sort through information using one of eleven different filters, such as data, event type, hostname, etc. So, if I were to select external IP, the next dropdown would include all available IP addresses to choose from. Then it will calculate the number of hits from that IP address.    The next two tiles both deal with calculating both the daily and weekly percentage change for the total number of hits.  At the bottom of the page, you will find the actual discover panel. Here it shows in depth information about each security event that has occurred. You can either page through this data with the arrows at the bottom, or you can change the total number of items per page, next to the arrows.  You can do a quick search from the search bar in the top right. This is just a simple search field that allows users to quickly find something specific they are looking for. For example, if a user is looking for an IP that contains 237, they can type that into the search bar and filter through.  There is, however, an advanced search option as well. The main benefit of this option is that you can search multiple strings at once. For example, if you are looking for a specific IP address that has high severity, you can type both of those in and they will search as different strings. |
| --- |



Enigma Glass also gives you the option to select which columns to view at once, through a dropdown with checkboxes. It also allows you to export data to 5 different data types including CSV, JSON, and XLS.