DEVSECCIOS BOOTCAMP

BUILDING RUGGED SOFTWARE

YEAR ONE / WEEK FOUR/ LESSON ONE

Agenda

- Splunk Search
- Field Extraction
- Field Extraction with Regular Expressions
- Statistics

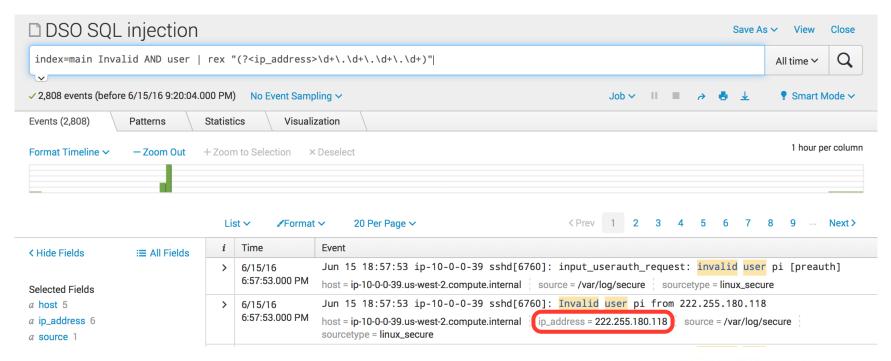


- Splunk Search
 - Retrieves events from indexes
 - Filters results of a previous search
 - Uses Search Processing Language
 - Implicit command when a search is performed or can be used further filter search results, e.g., index=main sourcetype=linux_secure | search field=value



- Field Extraction
 - Key value pairs extracted by Splunk or by custom field extraction
 - Used by splunk to
 - Commands used to perform field extraction: rex, rename, stats, etc.

- Field Extraction with Regular Expressions
 - rex uses Perl like regular expression to extract fields from search results

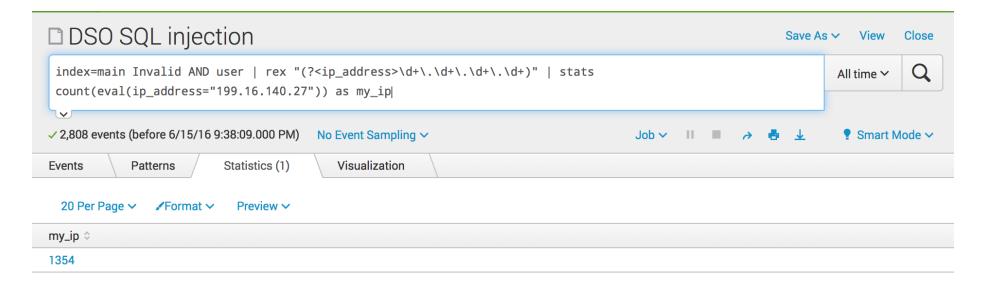


Statistics

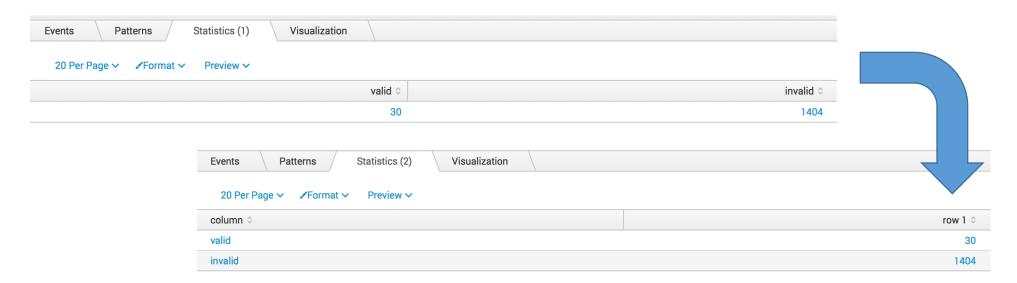
 stats command - calculates statistics such as counts, averages, min and max values



- Evaluating Fields
 - To narow in on a specific IP address for example, we could use a combination of count and eval to perform our query



- Tables and Visualization
 - transpose converts rows into columns
 - helps us create charts souch as pie charts



Lab 2

- If you weren't here last week team up with someone who was or quickly do week 3 lab 2 (get AWS credentials from Instructor)
- If you were here last week:
 - Run through the exercises in week 3 lab 3 if Splunk searches return no data