Lab 8 - Find the "needle in the haystack"

This lab teaches you how to use LogReduce to distill unique messages from large log data sets.

Explore the functionality of LogReduce, which allows you to distill unique messages from the noise by identifying recurring Signatures in your data.

1. Search for all messages that have the word "error" across all your data. Then click on LogReduce to get a summarized view of all messages.

```
error | logreduce
```

2. In a new search, run LogReduce on your Snort security data to identify unusual activity (intrusions).

```
_sourceCategory=labs/snort

| logreduce
```

3. Sort your results by count to identify those that happen only once. Click on the count (1) to view the unusual message. Now click on the host to view surrounding messages to identify the context of the intrusion.

```
<table>
<thead>
<tr>
<th>Time</th>
<th>Message</th>
</tr>
</thead>
</table>
```

+/- 1 Minute
+/- 5 Minutes
+/- 10 Minutes