Logcompare in SUMO Logic is an operator that helps identify differences in log patterns between two specified time periods or data sets. Logcompare creates a baseline query and compares it to the current query. Logs from both queries are grouped into patterns called signatures, then compared and ranked on the significance of change. It is especially valuable for SOC analysts when investigating anomalies or conducting threat hunts.

You can use logcompare to spot new types of failed login attempts as well as detecting unusual login patterns e.g. service account logging in from a new workstation. You can also identify new user accounts that have not been seen in the baseline period. Using logcompare can also show new types of blocked traffic, spikes, or drops in behaviour that can indicate a security incident.

We will use logcompare on logs coming from the Apache webserver. You will need to run the following query.

Query - _sourceCategory=Labs/Apache/Access and status_code=404

| logcompare timeshift -24h

#	Count	Score	Actions	Signature
10	3 -57%	1.48		***** - - [$DATE] "GET /***** HTTP/1.1" ***** "http://www.google.com" "Mozilla/5.0 (Windows NT 6.2) AppleWebKit/537. Gecko) Chrome/28.0.1467.0 Safari/537.36"
11	3 new	7.12		***** -*- [$DATE] "GET ***.* HTTP*1.*" * * "http:*/www*bing.com/search?q=*****&src=IE-SearchBox&FORM*IE11SR" "Mozill Googlebot/2.1; +http://www.google.com/bot.html)"
12	3 +15%	0.03		*****DATE]*** /***/master.js ****/1.1" *****
13	2 new	5.05		/_includes/wp/blog/wp-content/plugins/us/31063765-bpfull.phpi?&w=50&id=6&random=1331063765
14	2 +131%	0.43		*****200 *****.1" *Mozilla/5.0 (*;*CPU OS 6_0 like Mac OS X) AppleWebKit**.* (KHTML, like Gecko) Version/*.0 Mobile/

You can see a column called “Count,” which indicates the number of occurrences of the given signature, and a percentage change compared to a baseline period. If the signature has not been seen in the baseline period, it will be marked as “new”. The “Score” column is calculated based on the significance of the change in the occurrence of that specific pattern, compared to the baseline. So the higher the score, the more significant the change in this message.