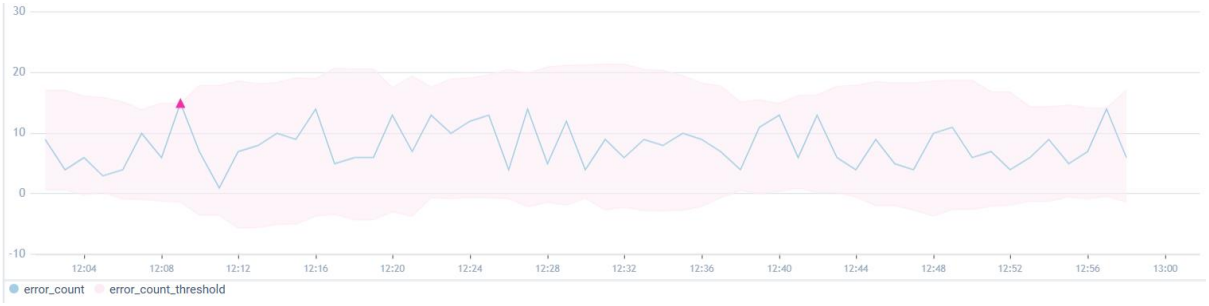
In Sumo Logic, using the “outlier” operator in a query can identify values in a sequence that seem unexpected, and would identify an alert or violation, for example, for a scheduled search. Essentially, it helps you identify when something unusual or statistically significant is happening.

To use ‘outlier’ effectively in SUMO SIEM, you have to perform the following query.

Query - _sourceCategory=Labs/Apache/Access status_code=404
| timeslice 1m
| count(status_code) as error_count by _timeslice
| outlier error_count window=10, consecutive=1, threshold=3, direction=+-

The source category section helps us to detect which source of logs we want to check; additionally status code of 404 indicates a wrong request. The Timeslice section tells Sumo Logic to group the events by a 1-minute period. “Count” field is responsible for renaming status_code column into error_count, and grouping it by the earlier indicated Timeslice. And finally outlier field focuses on error count, indicating that the window section sets the trailing number of data points to calculate the mean and sigma, threshold section sets the number of standard deviations for calculating violations and finally the consecutive section sets the required number of consecutive indicator data points (outliers) to trigger a violation. The direction section uses +-, +, or -, to specify which direction should trigger violations. We are using +- for positive or negative deviations.
After running this query, this will be a result presented in a line chart.



We can see that the red colour indicates the error count threshold. And the red triangle indicates where the error count reaches the threshold.

It can be used to find possible server errors over time, or various events, such as privilege changes or account tampering, in AWS Cloudtrail.
It can also track firewall logs to search for possible DDOS attacks.