Data validation for API responses

When a Splunk user hits the endpoint for their check with an API key, you want to make sure that a “200 OK” response code is returned, along with the data set for the correct ID that matches the endpoint.

Procedure

To validate that an API response code is not only expected, but that the right data comes back in the right format, create an external, synthetic test to hit the check endpoint at a set frequency from multiple locations.

1. Make a request with an API key to Splunk API’s endpoint for real browser check data.
2. Assert that the response code contains the value ‘200.’
3. Extract the check ID from the JSON using JSON path.
4. Assert that the check ID extracted from the JSON path is the expected value.

Next steps

This simple user flow helps you test:

- Availability. The check will fail if the API returns a response code that’s not 200 OK.
- Data Format. If the data comes back from the API in a format other than JSON then the step to extract a value using JSON path will fail the check.
- Data Quality. If you’re able to extract a value for the ID but it doesn’t match the expected value, then the assert step will fail the check.
Finally, you might be interested in other processes associated with the Monitoring API transactions use case.