For using Splunk with the eCommerce application I performed the following steps:

First, I added log4j messages throughout the application to log specific events such as failed authentication attempts:

Graphical user interface, text, application, email

Description automatically generated

Next, I ran the application from the command line and output all logs to a file and then used Postman to query various endpoints to generate some logs:

Graphical user interface

Description automatically generated

Graphical user interface, text, email

Description automatically generated

I then uploaded my output.log file to Splunk and searched it for errors which should have been present via the log4j error logging:

A screenshot of a computer

Description automatically generated

Graphical user interface, text

Description automatically generated

Graphical user interface, text, email

Description automatically generated

I then created a search for errors:

Graphical user interface, text, application, email

Description automatically generated

I then created an alert using that search to check for more than 100 errors per hour and email me if that condition was met:

Graphical user interface, application, website

Description automatically generated

I then created a new Dashboard using the same search:

Graphical user interface, application, Teams

Description automatically generated

Graphical user interface

Description automatically generated with low confidence