| Cybersecurity |
| --- |
| Module 19 Challenge Submission File |

## Let’s Go Splunking!

Make a copy of this document to work in, and then respond to each question below the prompt. Save and submit this completed file as your Challenge deliverable.

### Step 1: The Need for Speed

1. Based on the report you created, what is the approximate date and time of the attack?

| 2020-02-23 14:30:00 |
| --- |

1. How long did it take your systems to recover?

| Approximately 9 hours |
| --- |

Provide a screenshot of your report:

|  |
| --- |

### Step 2: Are We Vulnerable?

Provide a screenshot of your report:

|  |
| --- |

Provide a screenshot showing that the alert has been created:

|  |
| --- |

### Step 3: Drawing the (Base)line

1. When did the brute force attack occur?

| On Friday, February 21, 2020 from approximately 9am to 2pm. |
| --- |

1. Determine a baseline of normal activity and a threshold that would alert if a brute force attack is occurring:

| Reviewing the results from outside of the attack timeframe, it appears normal to have anywhere from 10-24 failed logon attempts. Therefore creating an alert of 25 or more failed logon attempts could be the result of a brute force attack. |
| --- |

1. Provide a screenshot showing that the alert has been created:

|  |
| --- |

© 2022 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.