| 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?

| The attack was launched on February 23, 2020 at 14:30:00 |
| --- |

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

| It took the system 8 hours to recover |
| --- |

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?

| The brute force attack occurred between 9:00 AM and 1:00 PM on February 21, 2020. |
| --- |

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

| Normal levels of failed login attempts usually range from 6 to 20 per hour. However, during the attack, there was a significant increase in the number of failed login attempts, with counts of 124, 101, 121, 95, and 123 recorded in each hour. As a reference, a baseline of 25 failed login attempts per hour is considered normal, and any increase beyond 50 attempts per hour will trigger an alert. |
| --- |

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

|  |
| --- |

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