| 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 approximate date and time of the attack was at 14:30 on 02-23-2020 and ended at 20:30 on 02-23-2020. |
| --- |

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

| It took 6 hours for our systems to recover from the attack. |
| --- |

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 the hours of 09:00 and 14:00 on 02-21-2020. |
| --- |

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

| A baseline for normal activity would be 18 logins per hour. A threshold that would alert if a brute force attack is occuring would be 25 failed login attempts. After that, an email gets sent to SOC@vandaly.com |
| --- |

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

|  |
| --- |

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