## **Let’s Go Splunking!**

### **Step 1: The Need for Speed**

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

|  |
| --- |
| At 2/22/2020 Between 11:30am and 2:30pm |

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

|  |
| --- |
| 2:30 pm to 11:30am the next day so about 21 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?

|  |
| --- |
| Feb 21, 2020 from 9am to 2pm |

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

|  |
| --- |
| Average is about a dozen logins. Around 8am which is standard time for most people to log in to work, it was about 20 people logging in. An above average would be 30 logins or above for an alert. |

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

|  |
| --- |
|  |