Lets Go Splunking! Report

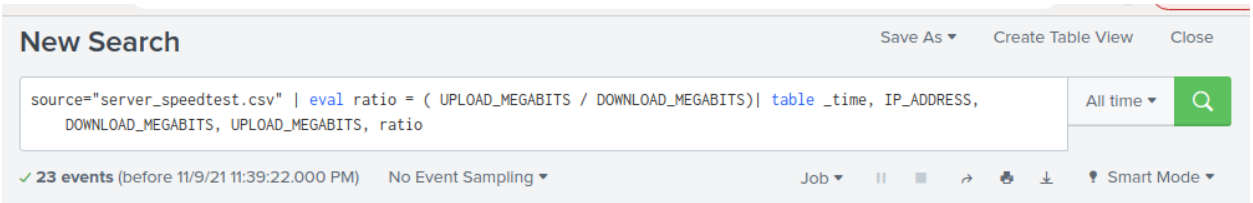
JasonS@Vandalay.com

11/8/2021

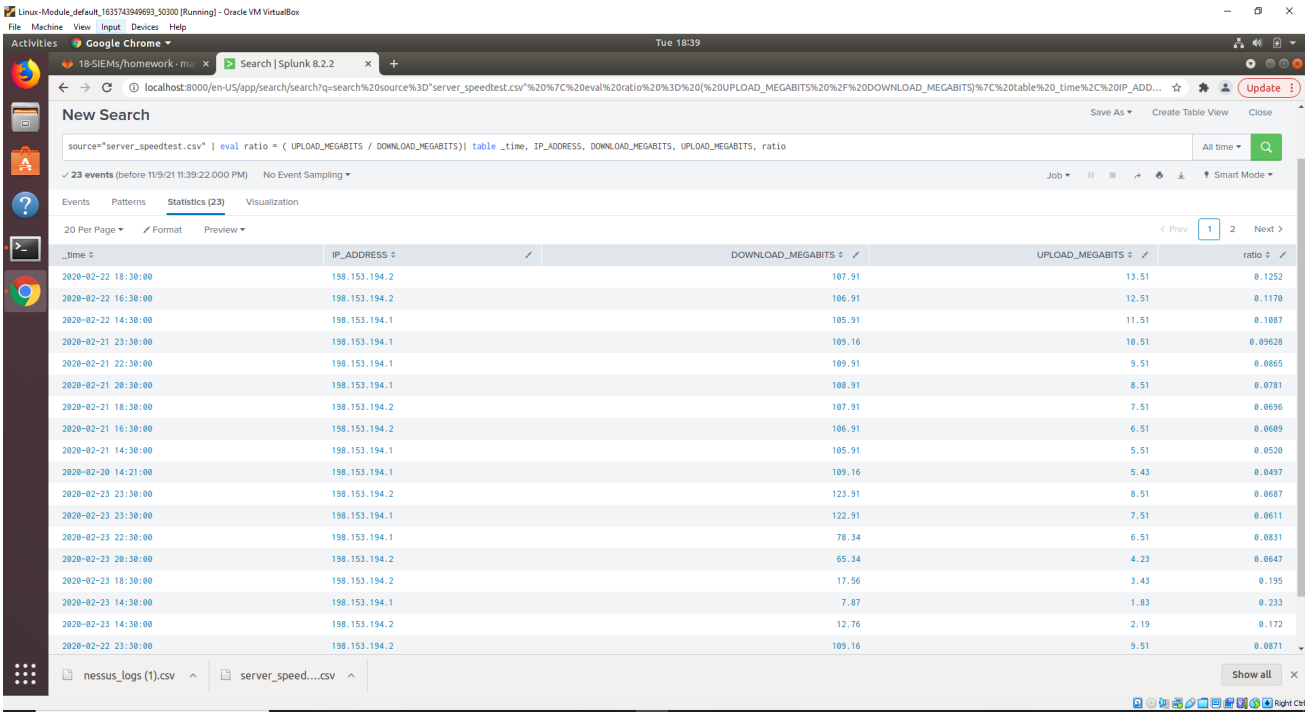
1.0 High-Level Summary

Vandalay Industries utilizes Splunk to handle their security monitoring needs. They have had a number of security risks directed at their systems for the past several months. Vandalay has ordered their SOC analysts to develop searches, custom reports, and alerts to secure their online environment from future attacks.

Need for Speed:

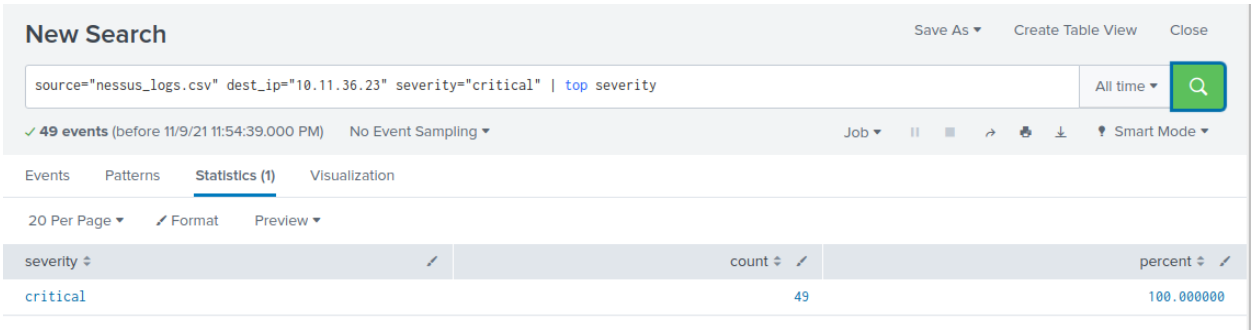


Based upon the report generated the attacks occurred on 2/23/2020 at 2:30 PM when the download/upload speeds dropped. Recovery occurred on 2/23/2020 at 8:30 PM, approximately six hours later.

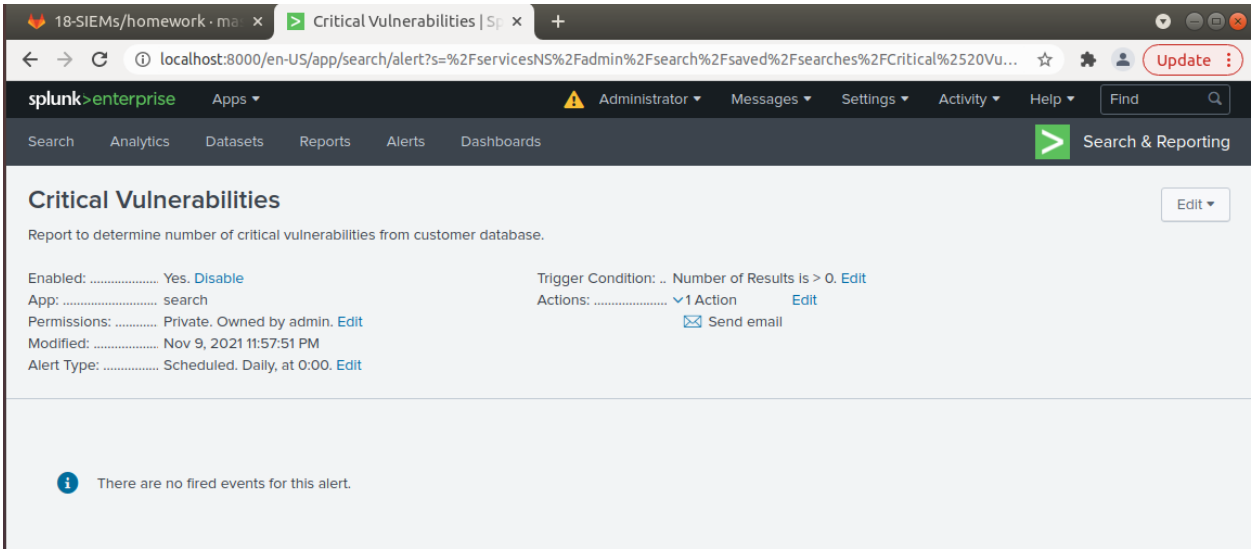


_time	IP_ADDRESS	DOWNLOAD_MEGABITS	UPLOAD_MEGABITS	ratio
2020-02-22 18:30:00	198.153.194.2	107.91	13.51	0.1252
2020-02-22 16:30:00	198.153.194.2	106.91	12.51	0.1170
2020-02-22 14:30:00	198.153.194.1	105.91	11.51	0.1087
2020-02-21 23:30:00	198.153.194.1	109.16	10.51	0.09628
2020-02-21 22:30:00	198.153.194.1	109.91	9.51	0.0865
2020-02-21 20:30:00	198.153.194.1	108.91	8.51	0.0781
2020-02-21 18:30:00	198.153.194.2	107.91	7.51	0.0696
2020-02-21 16:30:00	198.153.194.2	106.91	6.51	0.0609
2020-02-21 14:30:00	198.153.194.1	105.91	5.51	0.0520
2020-02-20 14:21:00	198.153.194.1	109.16	5.43	0.0497
2020-02-23 23:30:00	198.153.194.2	123.91	8.51	0.0687
2020-02-23 23:30:00	198.153.194.1	122.91	7.51	0.0611
2020-02-23 22:30:00	198.153.194.1	78.34	6.51	0.0831
2020-02-23 20:30:00	198.153.194.2	65.34	4.23	0.0647
2020-02-23 18:30:00	198.153.194.2	17.56	3.43	0.195
2020-02-23 14:30:00	198.153.194.1	7.87	1.83	0.233
2020-02-23 14:30:00	198.153.194.2	12.76	2.19	0.172
2020-02-22 23:30:00	198.153.194.2	109.16	9.51	0.0871

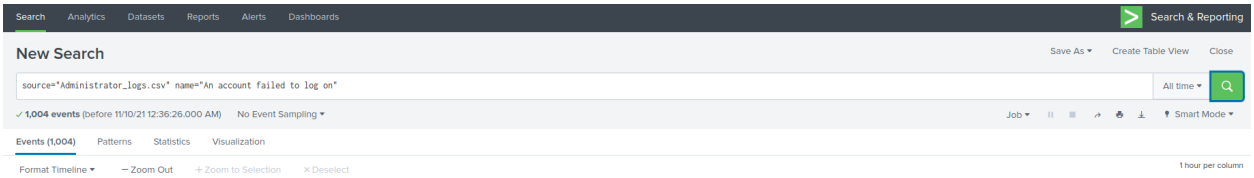
Are We Vulnerable:



Created report to view critical vulnerabilities from customer database and then created an alert to send an email to soc@vandalay.com if the trigger value is greater than 0.



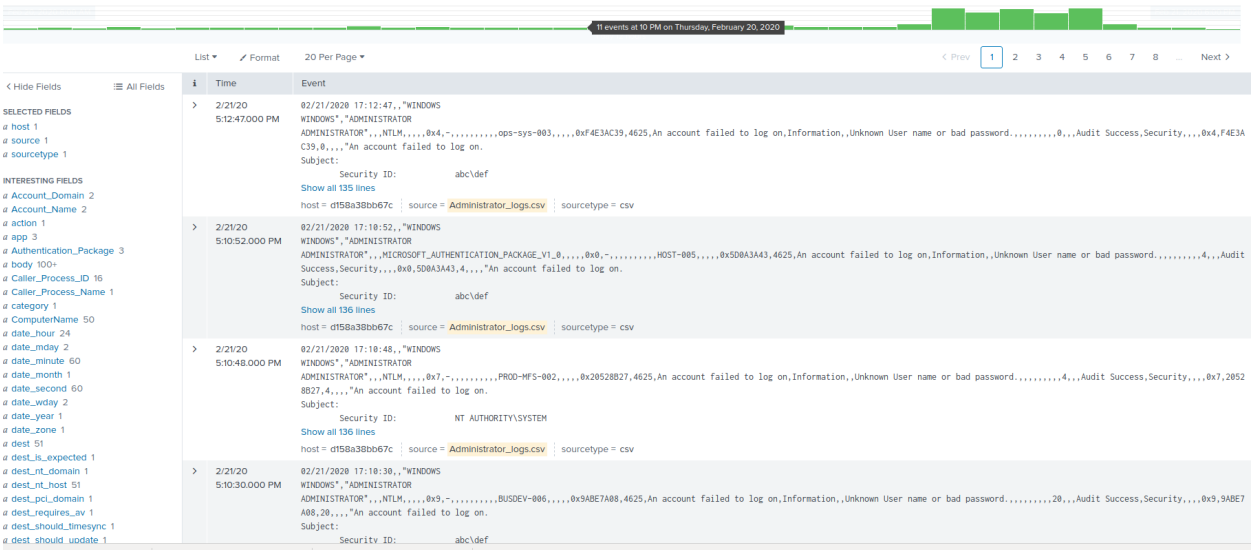
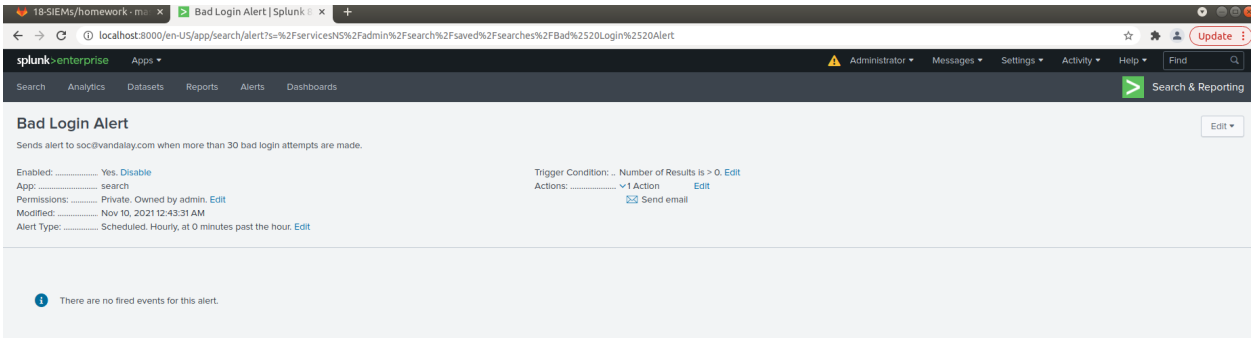
Drawing the (base)line:



The results show that the attack occurred on 2/21/2020 between 9:00 AM and 1:00 PM.

The bad login attempts average about 15 per hour during normal operations.

During attacks there are between 30 and 50 bad logins.



Created an alert to send an email to soc@vandalay.com when the trigger threshold of 30 to 50 bad login attempts is reached.