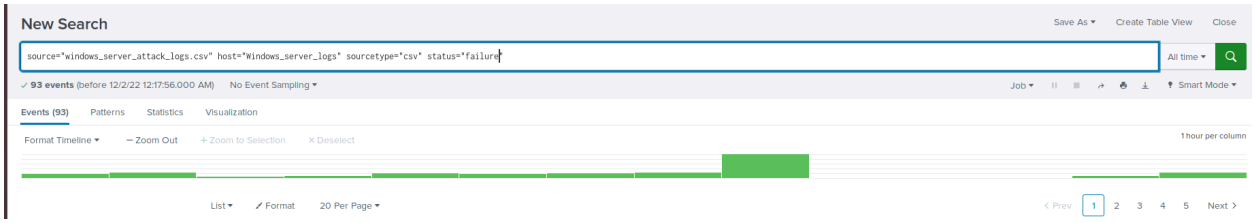
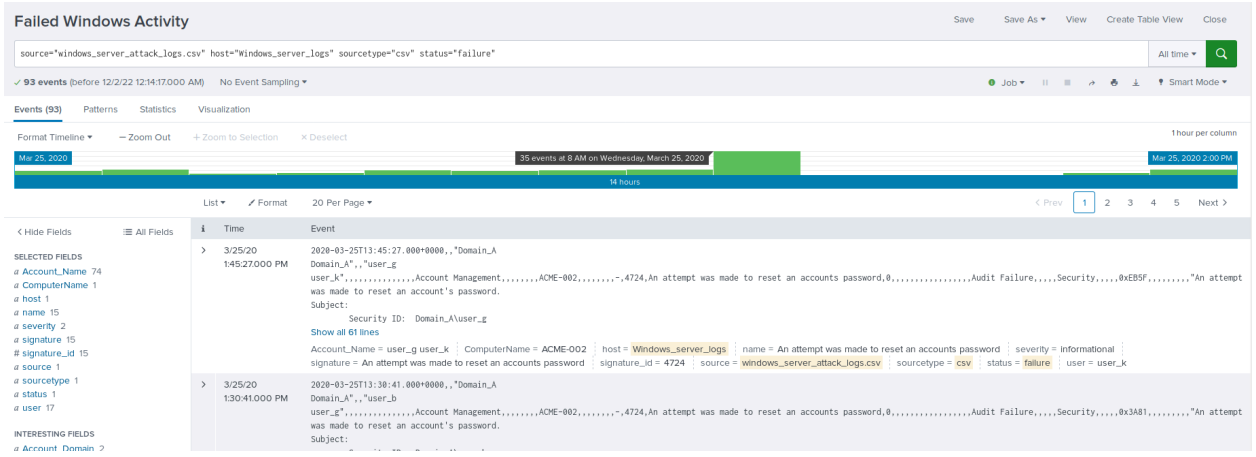
Splunk (Building a Security Monitoring Environment) Alerts, Dashboards, and Pie Charts

Alert 2.1

- Did you detect a suspicious volume of failed activity? **Yes**



- If so, what was the count of events in the hour(s) it occurred? **35**
- When did it occur? **3/25/20 0800**
- Would your alert be triggered for this activity? **Yes**
- After reviewing, would you change your threshold from what you previously selected? **No, threshold was set to 25 and only the attack breached the threshold.**



Alert 2.2

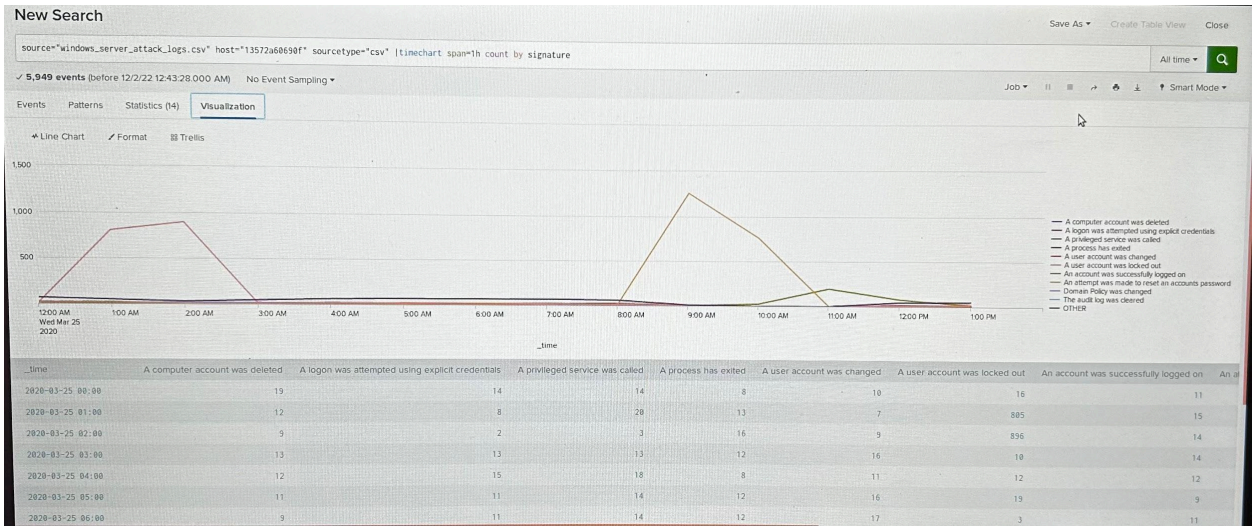
- Did you detect a suspicious volume of successful logins? **Yes**
- If so, what was the count of events in the hour(s) it occurred? **94 logins at 0200 and 70 logins at 0900**
- Who is the primary user logging in? **User_h**
- When did it occur? **3/25/20 0200 & 0900**
- Would your alert be triggered for this activity? **Yes**
- After reviewing, would you change your threshold from what you previously selected? **Yes from 50 to 60 (1000 set off an alert that appeared to be normal activity).**

Alert 2.3

- Did you detect a suspicious volume of deleted accounts? **Yes**

Dashboard Setup (for Windows logs)

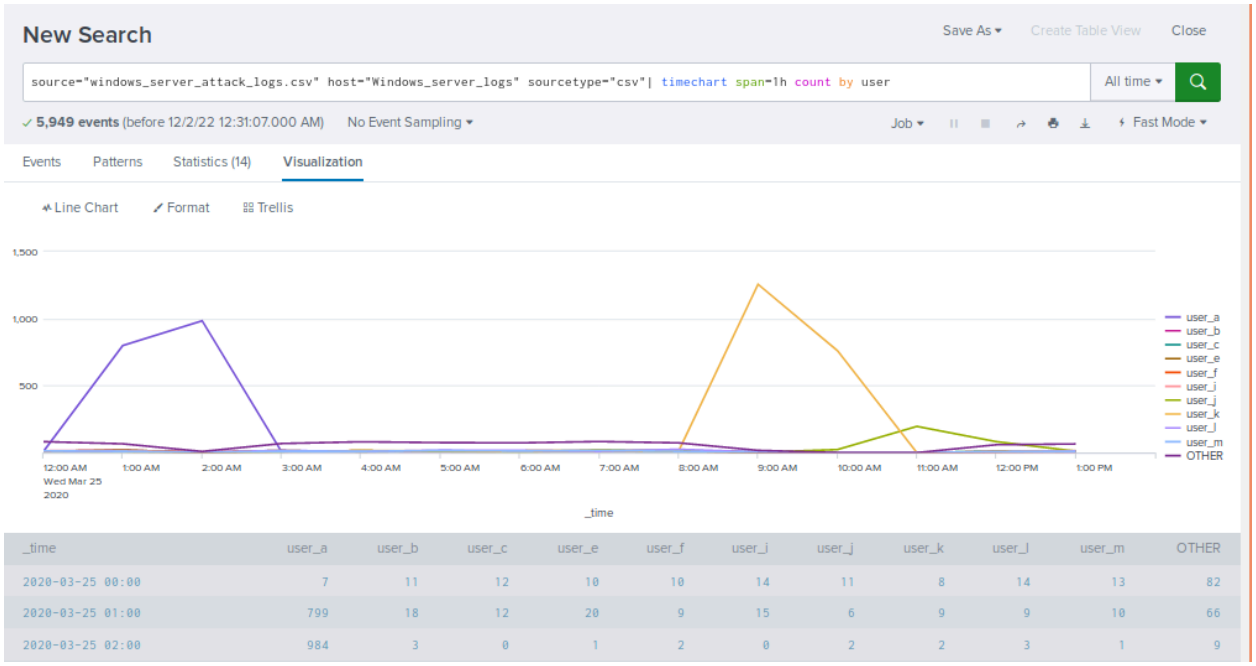
Dashboard Analysis for Time Chart of Signatures



_time	A computer account was deleted	A logon was attempted using explicit credentials	A privileged service was called	A process has exited	A user account was changed	A user account was locked out	An account was successfully logged on
2020-03-25 00:00	19	14	14	8	10	16	11
2020-03-25 01:00	12	8	28	13	7	805	15
2020-03-25 02:00	9	2	3	16	9	896	14
2020-03-25 03:00	13	13	13	12	16	10	14
2020-03-25 04:00	12	15	18	8	11	12	12
2020-03-25 05:00	11	11	14	12	16	19	9
2020-03-25 06:00	9	11	14	12	17	3	11

- Does anything stand out as suspicious? Yes, both sections called “A user account was locked out” and “An attempt was made to reset an accounts password” was significantly higher than the other sections that was provided.
- What signatures stand out? “A user account was locked out” and “An attempt was made to reset an accounts password”.
- What time did each signature’s suspicious activity begin and stop? For the “ A user account was locked out” signature began at 12am through 3am on wednesday, March 25th 2020. Also for the “An attempt was made to reset an accounts password” signature began at 8am through 11am on wednesday, March 25th 2020.
- What is the peak count of the different signatures? The peak count for the “A user account was locked out” signature was 896 and the “An attempt was made to reset an accounts password” signature peak was 1,258.

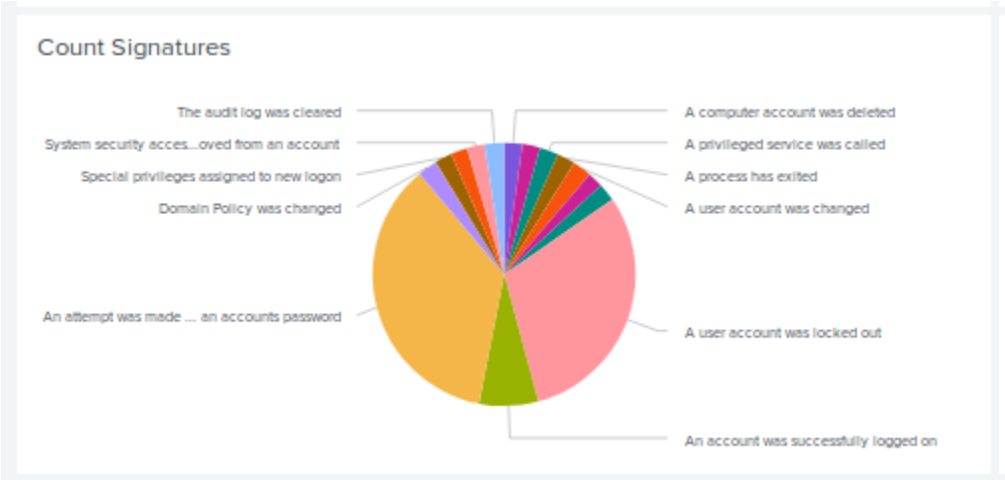
Dashboard Analysis for Users



_time	user_a	user_b	user_c	user_e	user_f	user_i	user_j	user_k	user_l	user_m	OTHER
2020-03-25 00:00	7	11	12	10	10	14	11	8	14	13	82
2020-03-25 01:00	799	18	12	20	9	15	6	9	9	10	66
2020-03-25 02:00	984	3	0	1	2	0	2	2	3	1	9

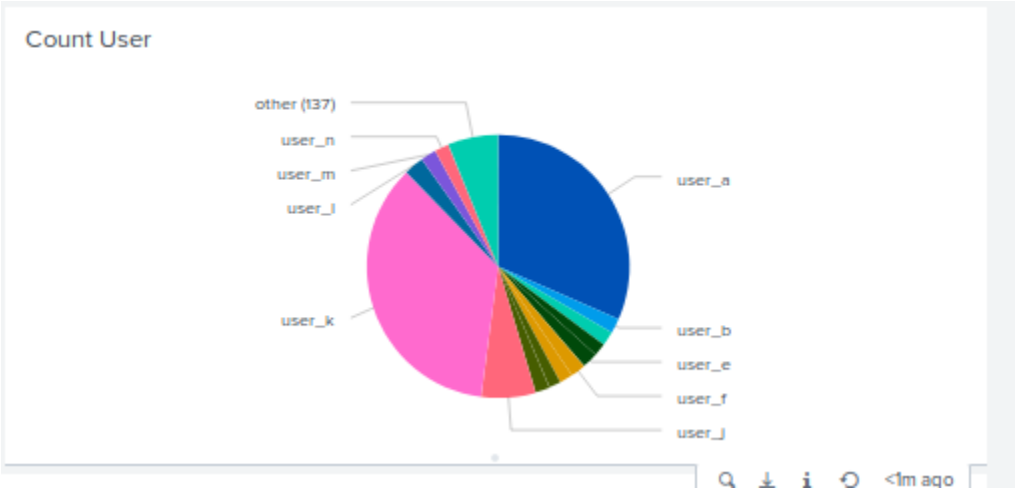
- Does anything stand out as suspicious?
    - **Yes, there is an abnormally large spike in user activity.**
- Which users stand out?
    - **user_a and user_k**
- What time did each user's suspicious activity begin and stop?
    - **user_a's activity became abnormal starting at 12:00 am and ending at 3:00 am**
    - **user_k's activity became abnormal at 8:00 am ending at 11:00 am**
- What is the peak count of the different users?
    - **user_a's peak activity is 984**
    - **user_k's peak activity is 1256**

Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts



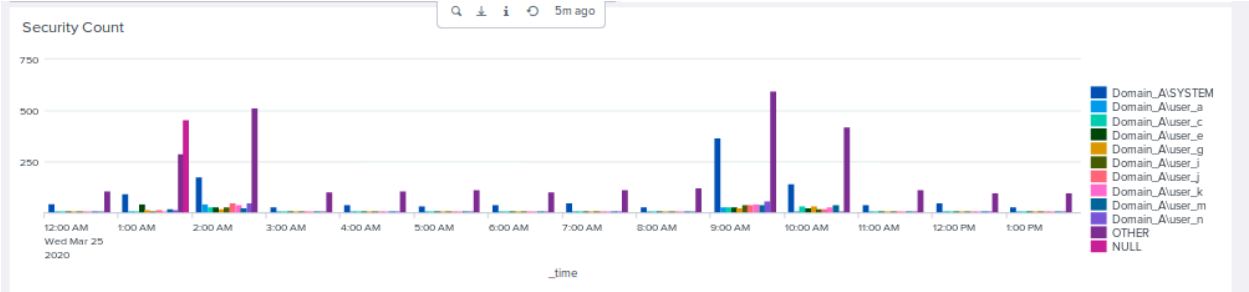
- Does anything stand out as suspicious?
    - **Yes, “An attempt was made to reset an accounts password” and “A user account was locked out” took up the vast majority of signatures**
- Do the results match your findings from the time chart for signatures?
    - **Yes**

Dashboard Analysis for Users with Bar, Graph, and Pie Charts



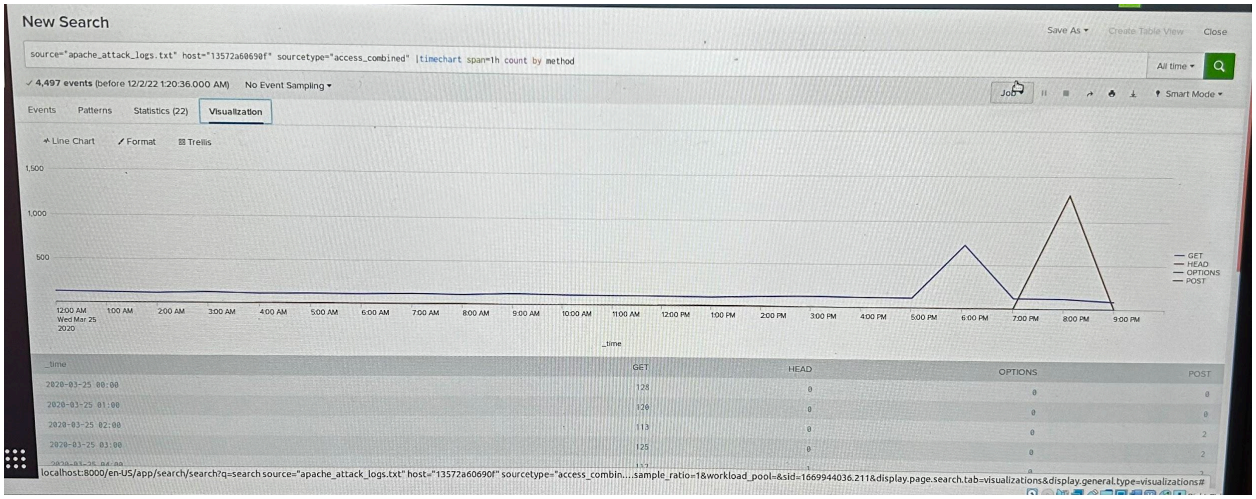
- Does anything stand out as suspicious?
    - **Yes, user_a and user_k’s activity takes up the vast majority of user activity**
- Do the results match your findings from the time chart for users?
    - **Yes**

Dashboard Analysis for Users with Statistical Charts



- What are the advantages and disadvantages of using this report, compared to the other user panels that you created?
    - **This report shows the security level of users accessing the site. This report shows that the majority of events came from a “NULL” or “OTHER” security_ID; indicating these users were not logged in**

Part 4: Analyze Apache Attack Logs

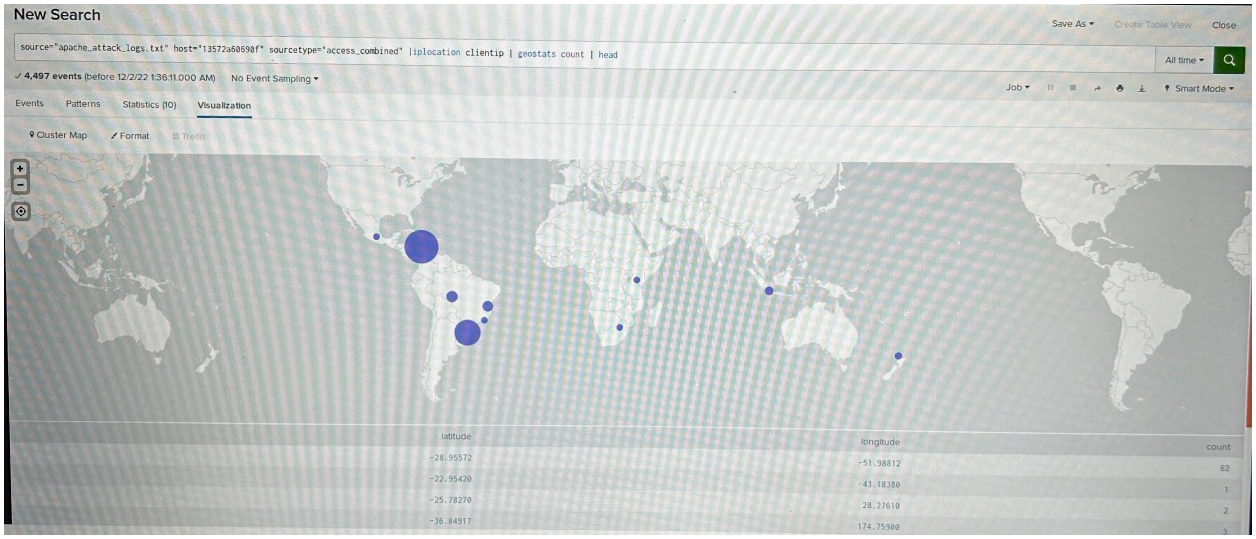


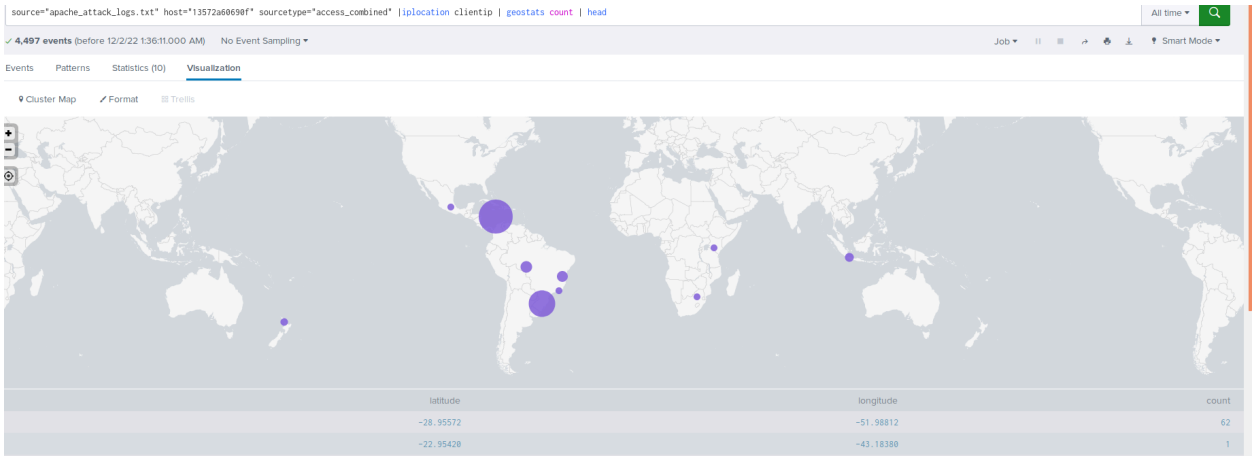
Dashboard Setup

Dashboard Analysis for Time Chart of HTTP Methods

- Does anything stand out as suspicious? Yes, the HTTP method “GET” and “POST” was used way more than the other ones.
- Which method seems to be used in the attack? The methods “GET” and “POST” was used in the attack.
- At what times did the attack start and stop? For the HTTP method “GET”, it started at 5pm and ended at 7pm. The other method “POST” it started at 7pm and ended at 9pm.
- What is the peak count of the top method during the attack? The peak count for the top method was “POST” and it was 1,296.

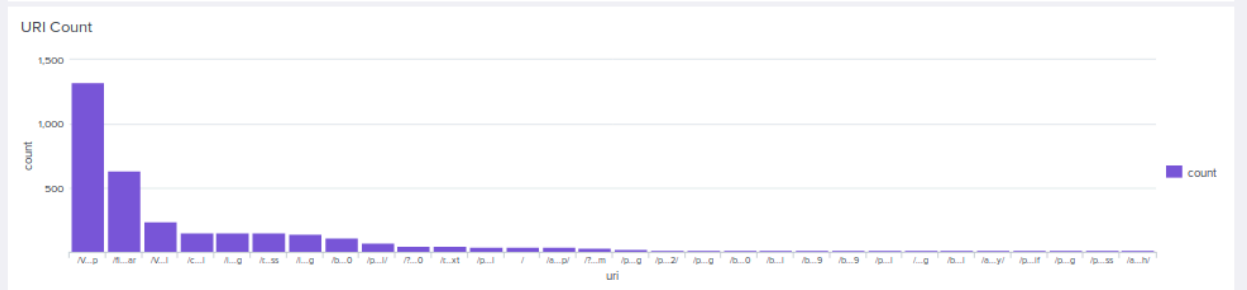
Dashboard Analysis for Cluster Map





- Does anything stand out as suspicious? Yes the in country Brazil and the area by the British Virgin Isalnds are located.
- Which new location (city, country) on the map has a high volume of activity?
    - **Hint**: Zoom in on the map. The locations that was tied with the high volume of activity is (Road Town, British Virgin Islands) and (San Salvador, El Salvador).
- What is the count of that city? They both had a total count of 34.

Dashboard Analysis for URI Data



- Does anything stand out as suspicious?
    - **Yes, the account login page has nearly five times the amount of hits as the homepage; indicating many failed login attempts**
- What URI is hit the most?
    - **Login page**
- Based on the URI being accessed, what could the attacker potentially be doing?
    - **Attempting to brute force an account based on the repeated number of URI requests for the login page**

Alerts 4.1

- Did you detect a suspicious volume of international activity? **Yes**
- If so, what was the count of events in the hour(s) it occurred? **864**
- Would your alert be triggered for this activity? **Yes**
- After reviewing, would you change the threshold you previously selected? **No, threshold was set to 6 and only the attack breached the Threshold.**

Alerts 4.2

- Did you detect any suspicious volume of HTTP POST activity? **Yes**
- If so, what was the count of events in the hour(s) it occurred? **1296**
- When did it occur? **3/25/20 2000**
- After reviewing, would you change the threshold that you previously selected? **No, threshold was set to 8 and only the attack breached the Threshold.**