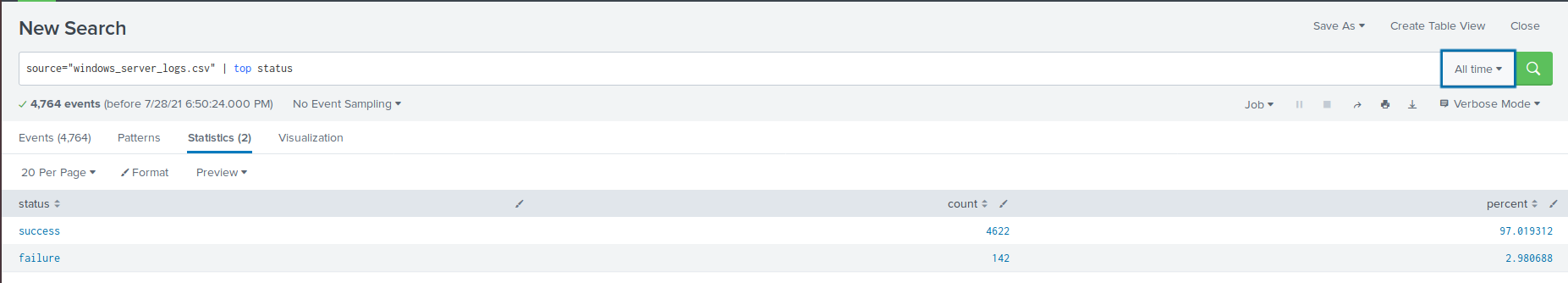
## **Solution Guide: Part 2 - Defend Your SOC**

### **Windows Server Logs**

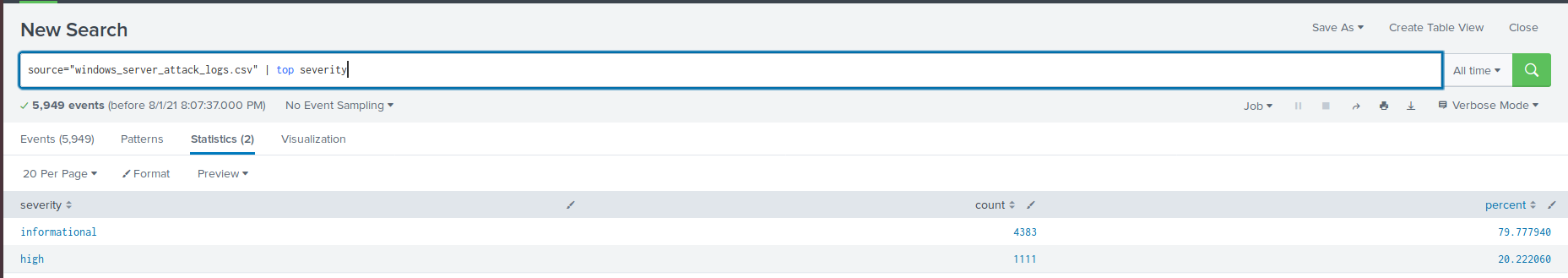
#### **Report Analysis for Severity**

1. Did you detect any suspicious changes in severity?
   1. Yes. The percentages changed from:  
       High: 7%

Informational: 93%

  
 to:  
 High: 20%

Informational: 80%



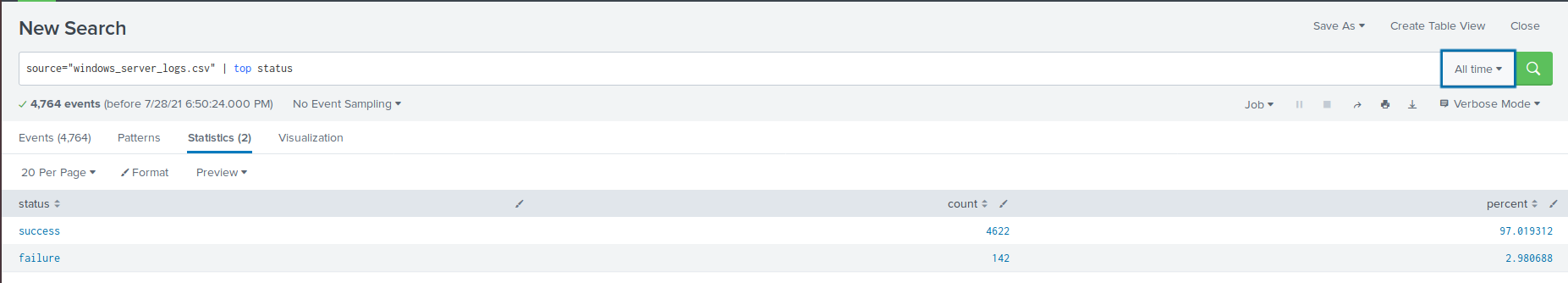
1. **This indicates an increase in the high severity cases.**

#### 

#### **Report Analysis for Failed Activities**

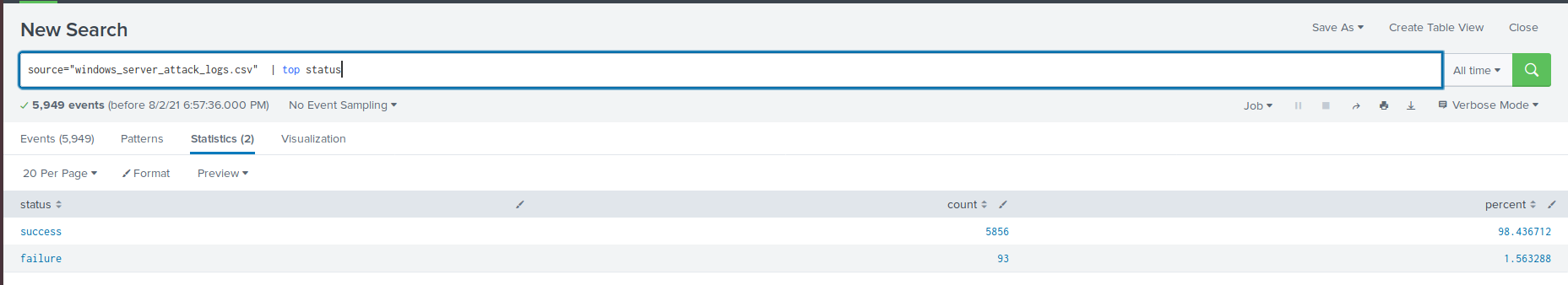
1. **Did you detect any suspicious changes in failed activities?**
   1. **Yes. The percentages changed from:**  
       success: 97%

failure: 3%



to:  
 success: 98%

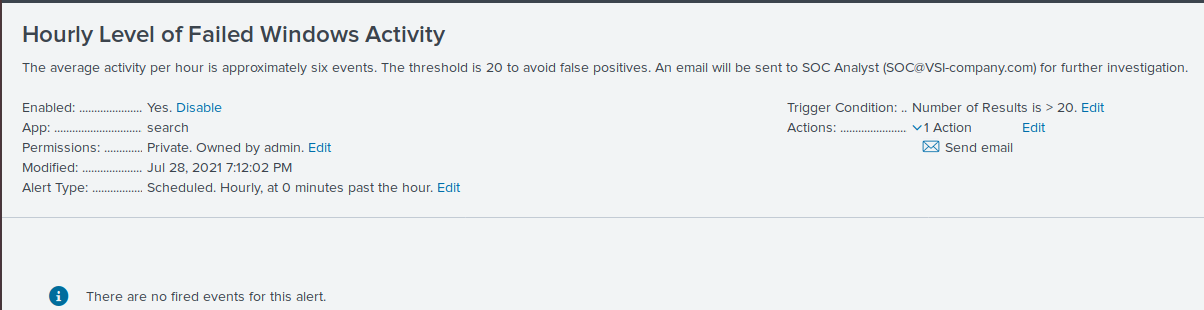
failure: 2%



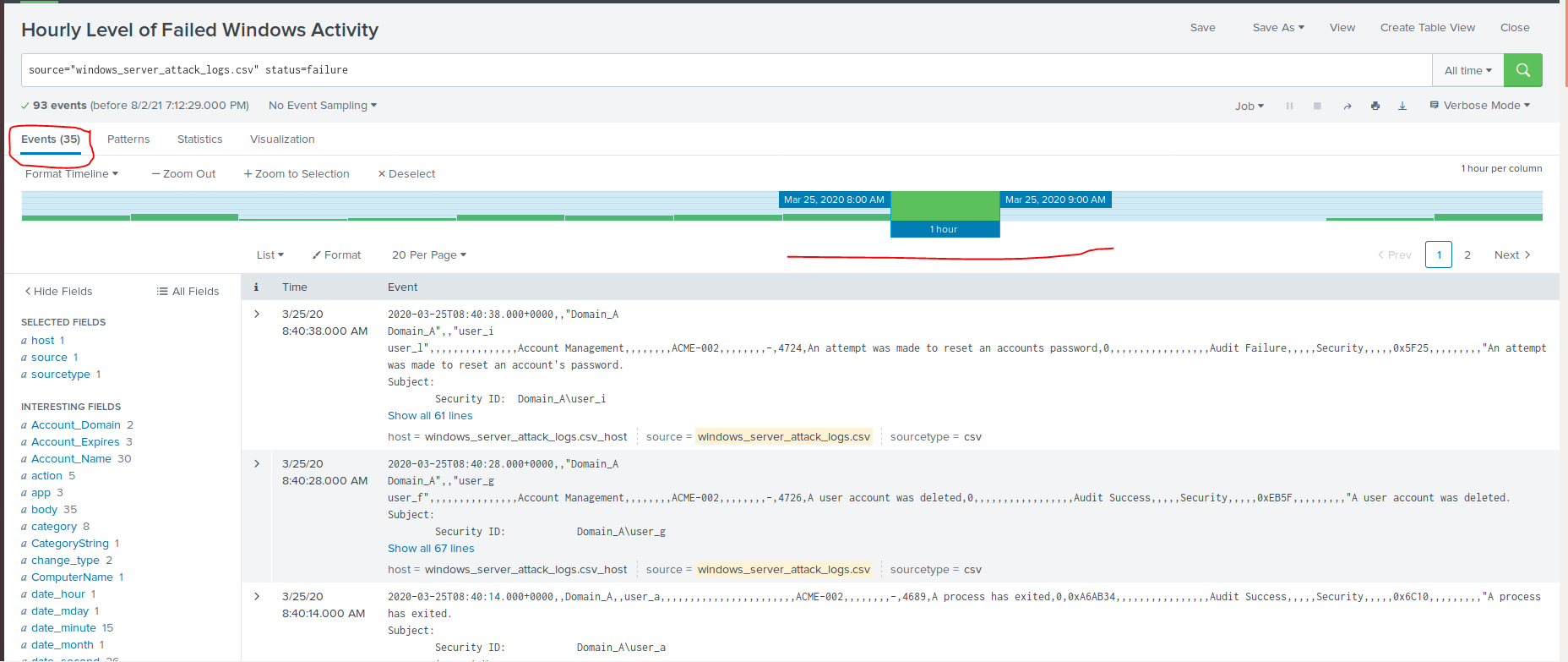
1. **This indicates that there is not a major change in the cumulative failure of events.**

#### 

#### **Alert Analysis for Failed Windows Activity**



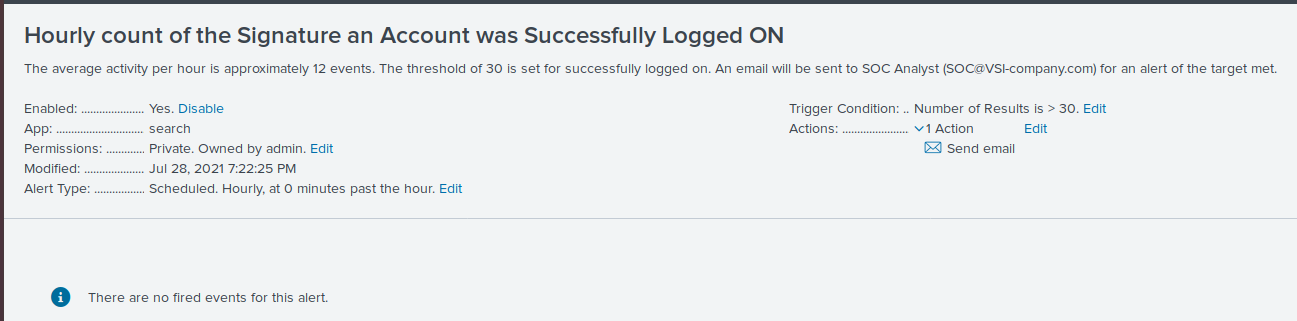
1. **There is some potential suspicious activity for failed activity between 8 a.m. and 9 a.m. on Weds, March 25th.**



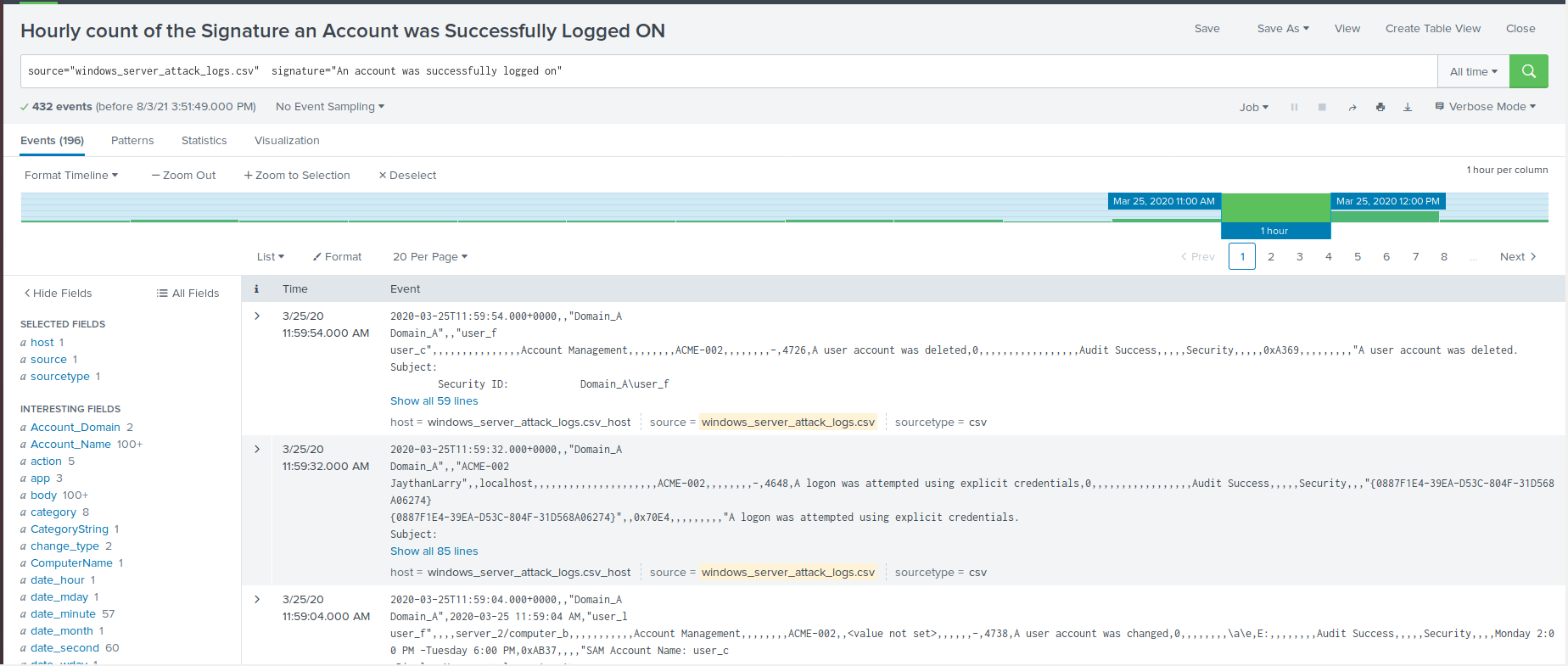
1. **The count of activity is 35 events during this hour, A privileged service was called, where the user account was deleted, Domain Policies were changed, A user account was created, an attempt was made to reset an accounts password, and a computer account was deleted.**

#### 

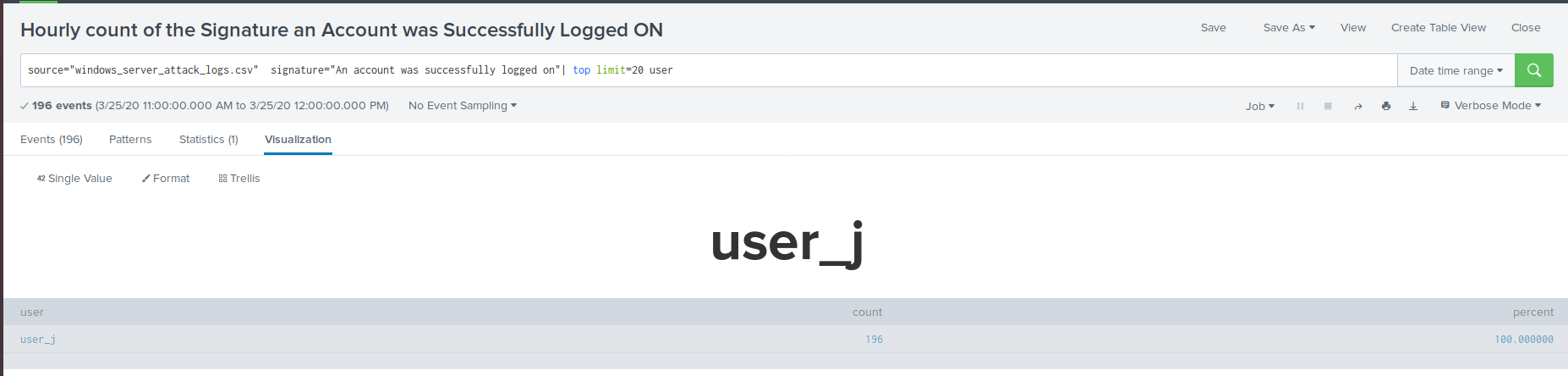
#### **Alert Analysis for Successful Logons**



1. **There is some potential suspicious activity for successful logons activity between 11 a.m and 12 p.m. on Weds, March 25th.**



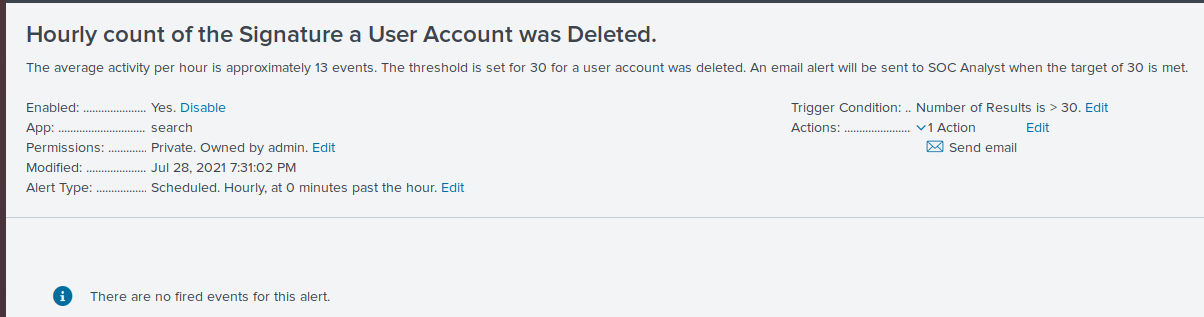
1. **The count of activity is 196 between 11 a.m. and 12 p.m.**
2. **The primary user logging in is user j.**



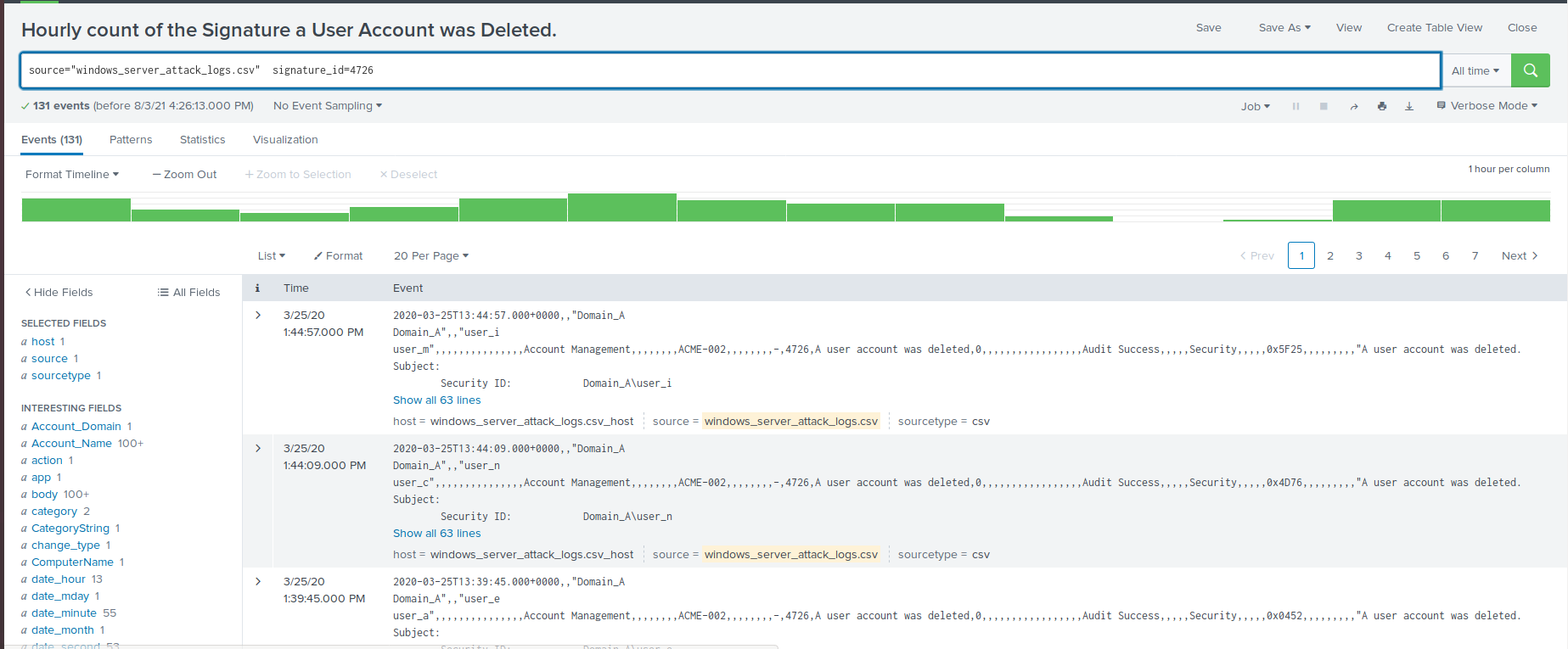
1. **Yes, it would have alerted the SOC Analyst of the suspicious logons.**
2. **No, it is set appropriately for the hourly settings, it would have also triggered an alert for the activity for the second hour from 12 p.m. to 1 p.m. on the same day.**

#### **Alert Analysis for Deleted Accounts**

Did you detect a suspicious volume of deleted accounts?



1. **There was no suspicious activity of deleted accounts.**

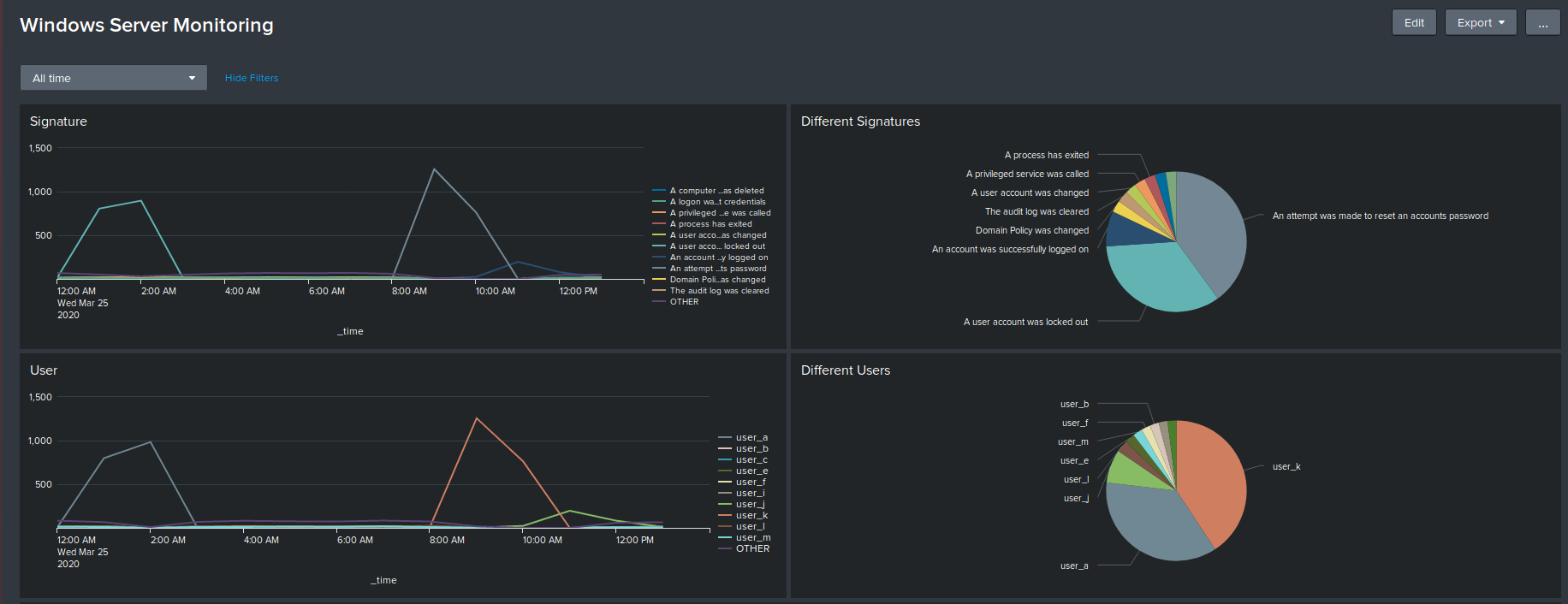


#### 

#### **Dashboard Analysis for Time Chart of Signatures**

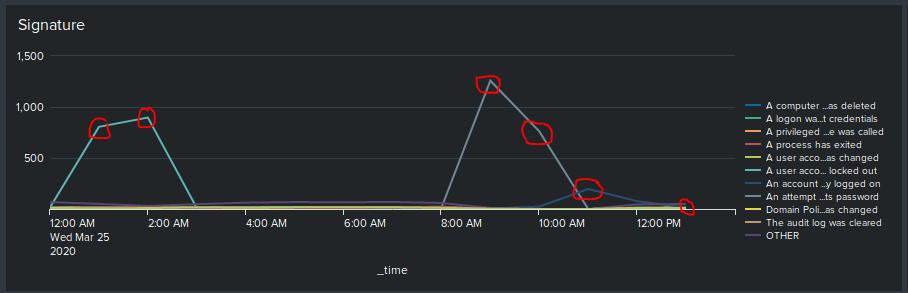
* Does anything stand out as suspicious? What signatures stand out?

1. **Yes, the signatures that have suspicious activity are: An attempt was made to reset a users password (39.955%), A user account was locked out (34.003%), and An account was successfully logged on (8.111%).**



* What time did it start and stop for each signature? What is the peak count of the different signatures?

1. **A user account was locked out: Started around 1 a.m. and ended at 3 a.m. on March 25th. The peak count was 896, and the total for the two hours was (805 + 896 = 1701).**
2. **An attempt was made to reset a users password: Started around 9 a.m. and ended at 11 a.m. on March 25th. The peak count was 1,258, and the total for the two hours was (1258 + 761 = 2019)**
3. **The account was successfully logged on: Started around 11 a.m. and ended at 1 p.m. on March 25th. The peak count was 196, and the total for the two hours was (196 + 77 = 273).**



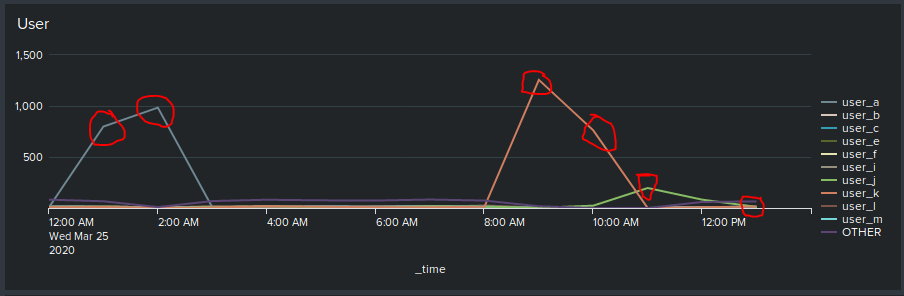
#### **Dashboard Analysis for Users**

* Does anything stand out as suspicious? Which users stand out?

1. **Yes, the users that have suspicious activity are users A, K, and J.**

* What time did it begin and stop for each user? What is the peak count of the different user?

1. **User A: Started around 1 a.m. and ended at 3 a.m. on March 25th. Peak count was 984, and the total for the two hours was (799 + 984 = 1783).**
2. **User K: Started around 9 a.m. and ended at 11 AM on March 25th. Peak count was 1,256, and the total for the two hours was (1256 + 761 = 2017).**
3. **User J: Started around 11 a.m. and ended at 1 p.m. on March 25th. Peak count was 196, and the total for the two hours was (196 + 82 = 278).**



#### **Dashboard Analysis for Signatures with Bar, Graph, Pie Charts**

1. **All Charts are showing the same information as above for the Signatures.**

#### **Dashboard Analysis for Users with Bar, Graph, Pie Charts**

1. **All Charts are showing the same information as above for the Users.**

#### **Dashboard Analysis for Users with Statistical Chart**

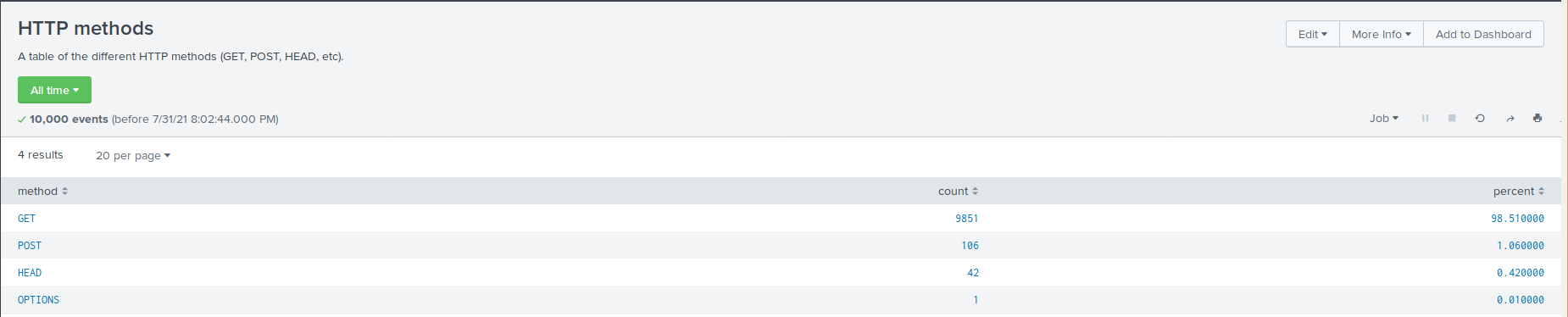
* What would be the advantage/disadvantage of using this report, compared to the other user panels you created?
* **There is only one advantage of the stats chart, as it will only give the total count of the users activity or the percentage of the activity. However, the disadvantage of the stats chart compared to a chart will show a cumulative perspective, while a time chart shows the suspicious activity over a more specific, and shorter time frame.**

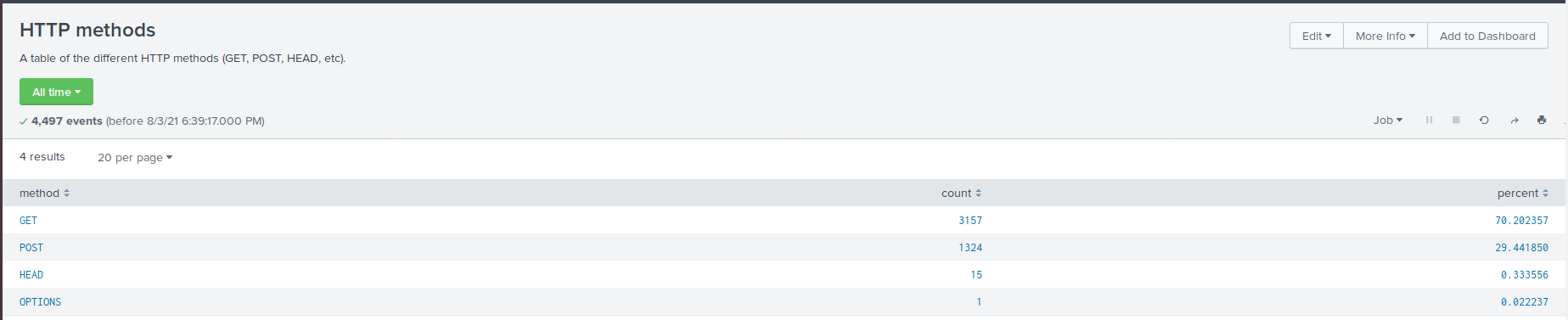
### **Apache WebServer Logs**

#### **Report Analysis for Methods**

1. Did you detect any suspicious changes in HTTP methods? If so, which one?

* **Yes, a suspicious change in the HTTP POST method was raised from 1% to 29%.**

****

****

1. What is that method used for?

* **POST is used to submit or update information to a web server.**

#### **Report Analysis for Referrer Domains**

1. Did you detect any suspicious changes in referrer domains?

* **There were no major suspicious referrers during the attack. Only minor changes to the first two domains by a couple of percentages.**

#### 

#### **Report Analysis for HTTP Response Codes**

1. Did you detect any suspicious changes in HTTP response codes?

* **There are several small changes, but the most prominent is the 404 response code, which increased from 2% to 15%. The 200 response code went down from 91% to 83%.**

****

****

#### 

#### **Alert Analysis for International Activity**

1. Did you detect any suspicious volume of international activity? If so, what was the count of the hour it occurred in?

* **There was activity in Ukraine between 8 p.m. and 9 p.m. on Weds, March 25th, and had a count of 935 events.**
* **Yes, as the threshold was set at 200, so this activity would be triggered as part of the alert.**
* **No, as it’s above the activity set threshold.**

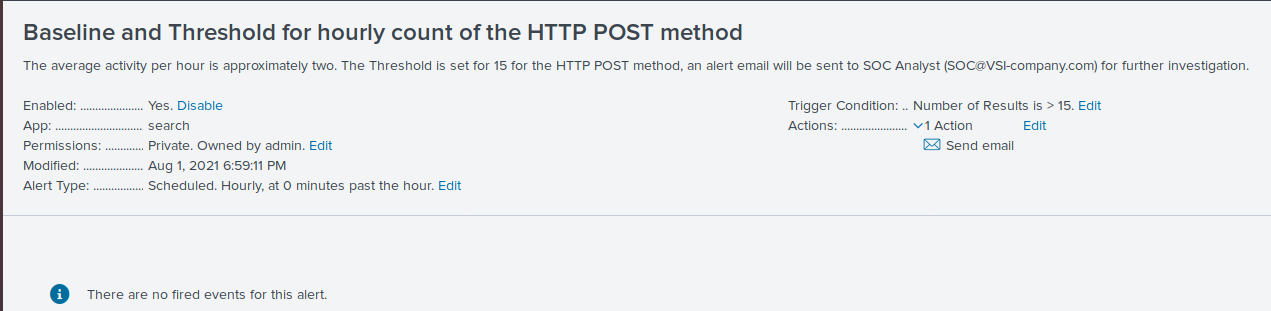
#### 

#### 

#### **Alert Analysis for HTTP POST Activity**

1. Did you detect any suspicious volume of HTTP POST activity? If so, what was the count of the hour it occurred in and when did it occur?

* **There was a spike in POST method activity between 8 p.m. and 9 p.m. on Weds, March 25th, and had a count of 1,296 events.**
* **No, the threshold set is at 15 counts, this would have been triggered.**

****

#### **Dashboard Analysis for Time Chart of HTTP Methods**

* Does anything stand out as suspicious?
* **Yes, there were suspicious activities of the POST and GET method.**
* What was the method that seems to be used in the attack? What time did it begin and end, and what was the peak count?
* **The POST method was used, starting at 8 p.m. and ending at 9 p.m. The peak count was 1,296.**
* **THE GET method was used, starting at 6 p.m. and ending at 7 p.m. The peak count was 729.**

#### **Dashboard Analysis for Cluster Map**

* Does anything stand out as suspicious? What new country, city on the map has a high volume of activity?
* **Yes, there is suspicious activity in Ukraine.**
* What is the count of that country, city?
* **When zoomed in, we can see the cities in Ukraine are:**
  + **Kiev: Count of 439**
  + **Kharkiv: Count of 433**
  + **Lvov: 5**

#### **Dashboard Analysis for URI Data**

* Does anything stand out as suspicious? What URI is being hit the most?
* **Yes, there is suspicious activity against the main VSI logon page: /VSI\_Account\_logon.php (count of 1323).**
* Based on the URI being accessed, what could the attacker potentially be doing?
* **The attacker may be trying to brute force the VSI logon page.**

© 2020 Trilogy Education Services, a 2U, Inc. brand. All Rights Reserved.