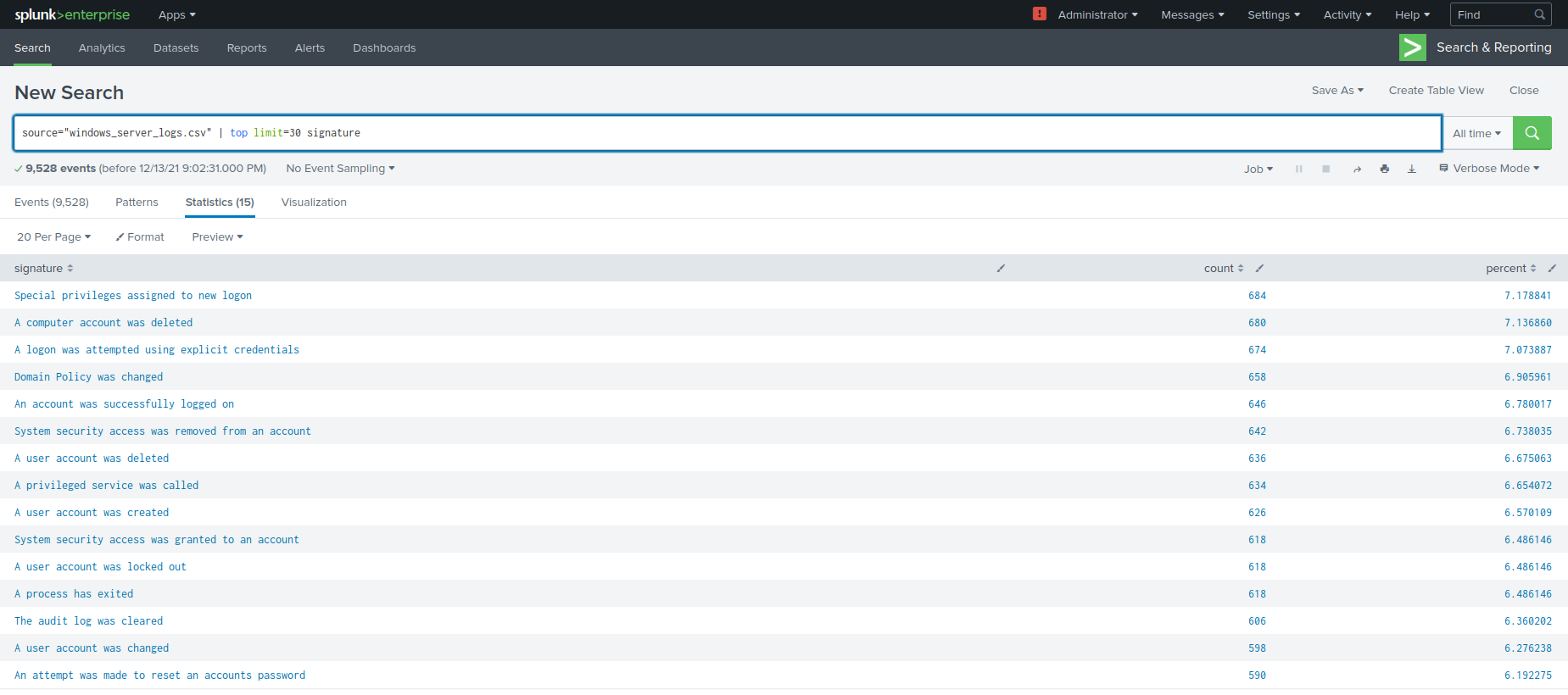
### Part 1: Windows Server Attack

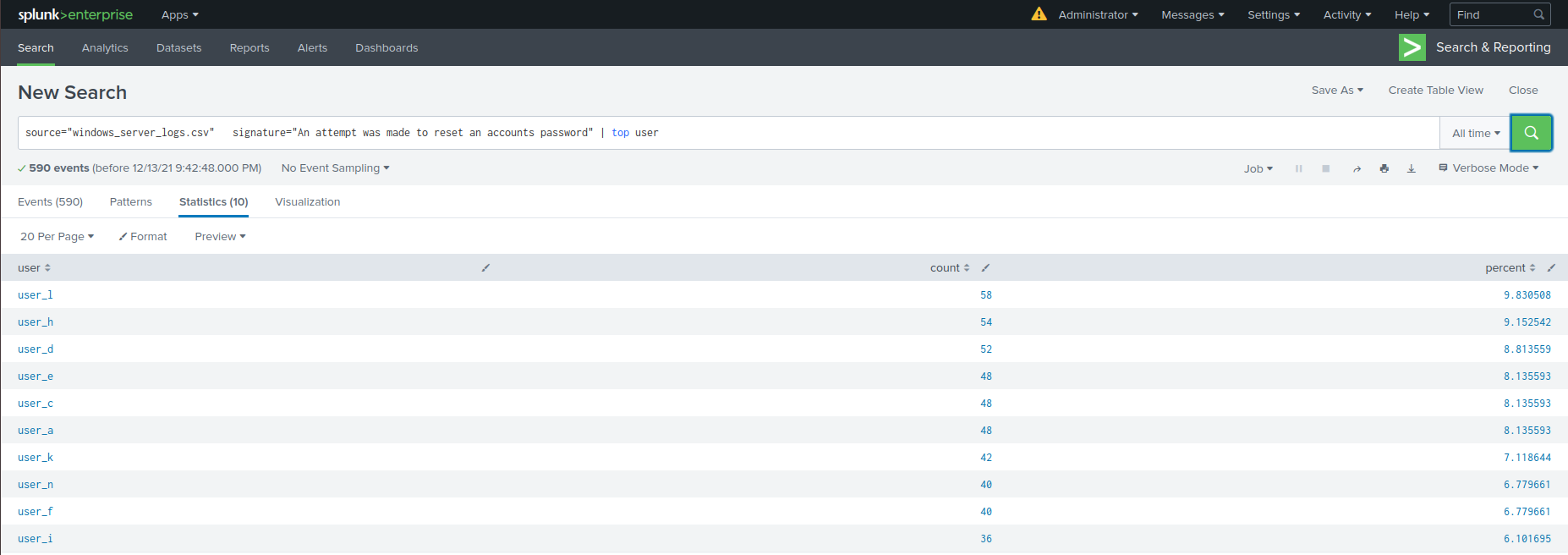
Note: This is a public-facing windows server that VSI employees access.

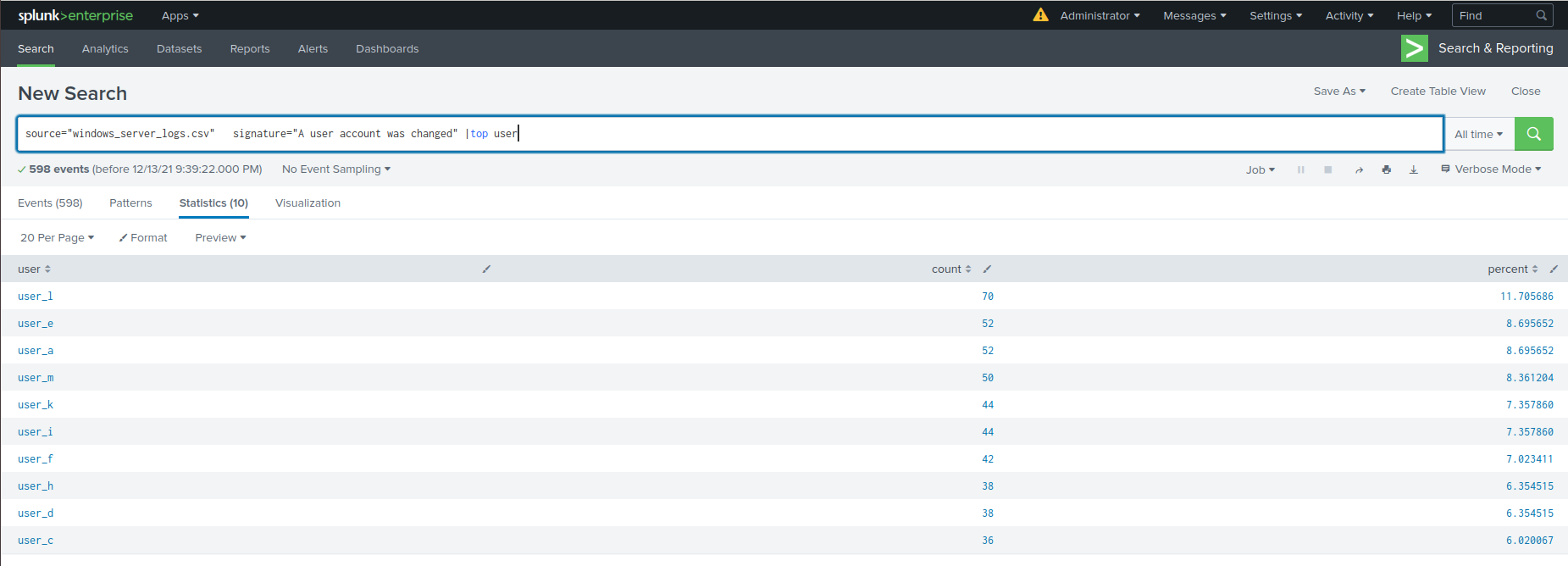
#### Question 1

- Several users were impacted during the attack on March 25th.  
I noticed many users accounts were locked out and attempts to reset the password on Domain\_A. For example:

"An attempt was made to reset an account's password.  
Subject:  
 Security ID: Domain\_A\user\_k”







-Based on the attack signatures, what mitigations would you recommend to protect each user account? Provide global mitigations that the whole company can use and individual mitigations that are specific to each user.

Global Permission policy that requires 13 failed attempts within one hour before locking up the user account, and sending alert to the SOC team to investigate immediately. Anytime a user is let go of the company, the Global permission policy must be updated immediately by removing the user account.  
All departments must follow the permission policy by having long passwords with special characters.  
All company users should be forced to update their user account every 3 months.

#### Question 2

- VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.

- What sort of mitigation could you use to protect against this?

1) Strong password policy

2) Multi-Factor Authentication (MFA)

3) Encrypt the folder where the system user is located

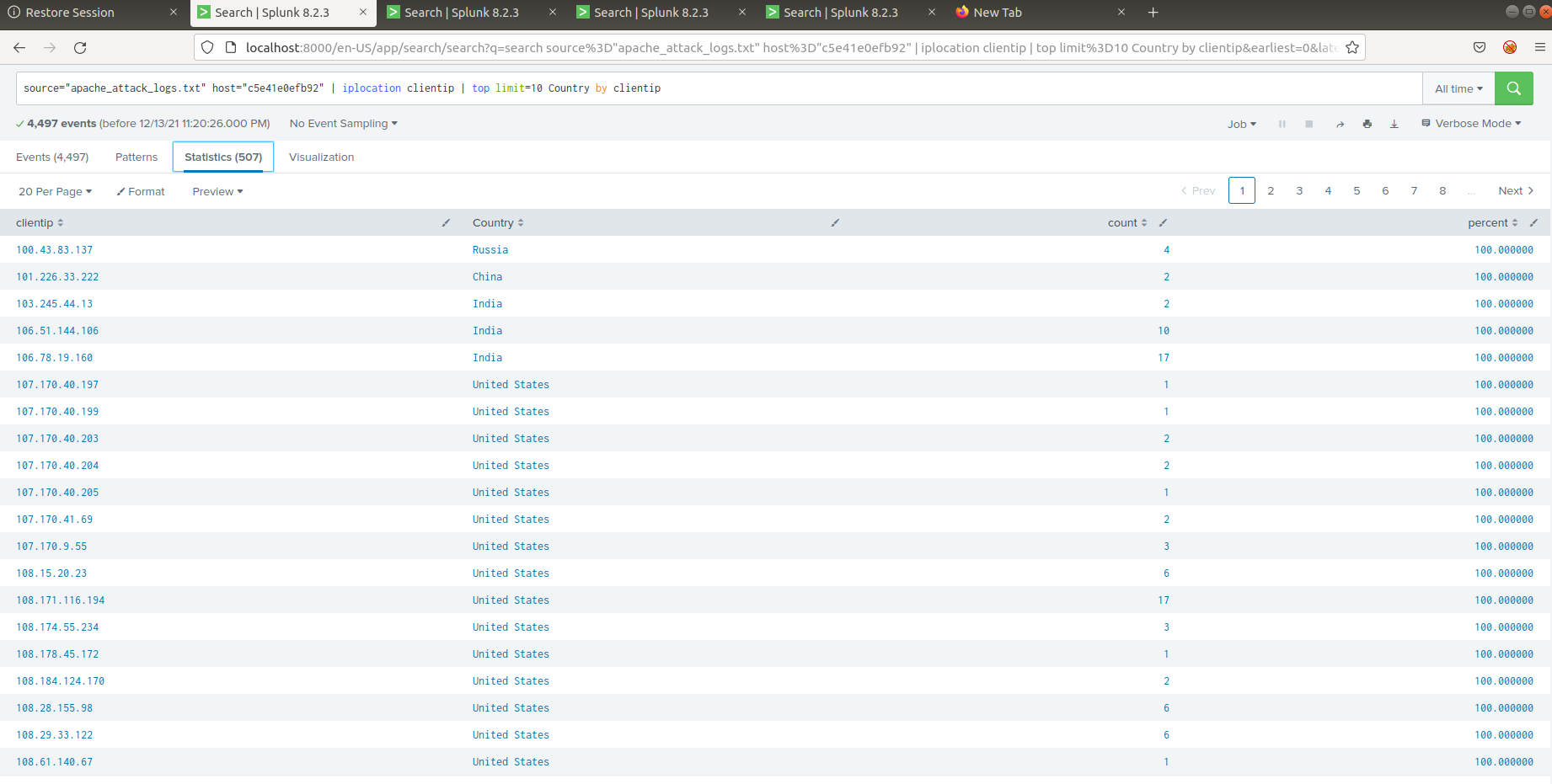
4) Set a rule in your Intrusion Prevention System to detect and prevent access after “Bad Logins”  
and send alert to the SOC team based on the threshold alert of attempts to do a brute force password.  
  
### Part 2: Apache Webserver Attack:

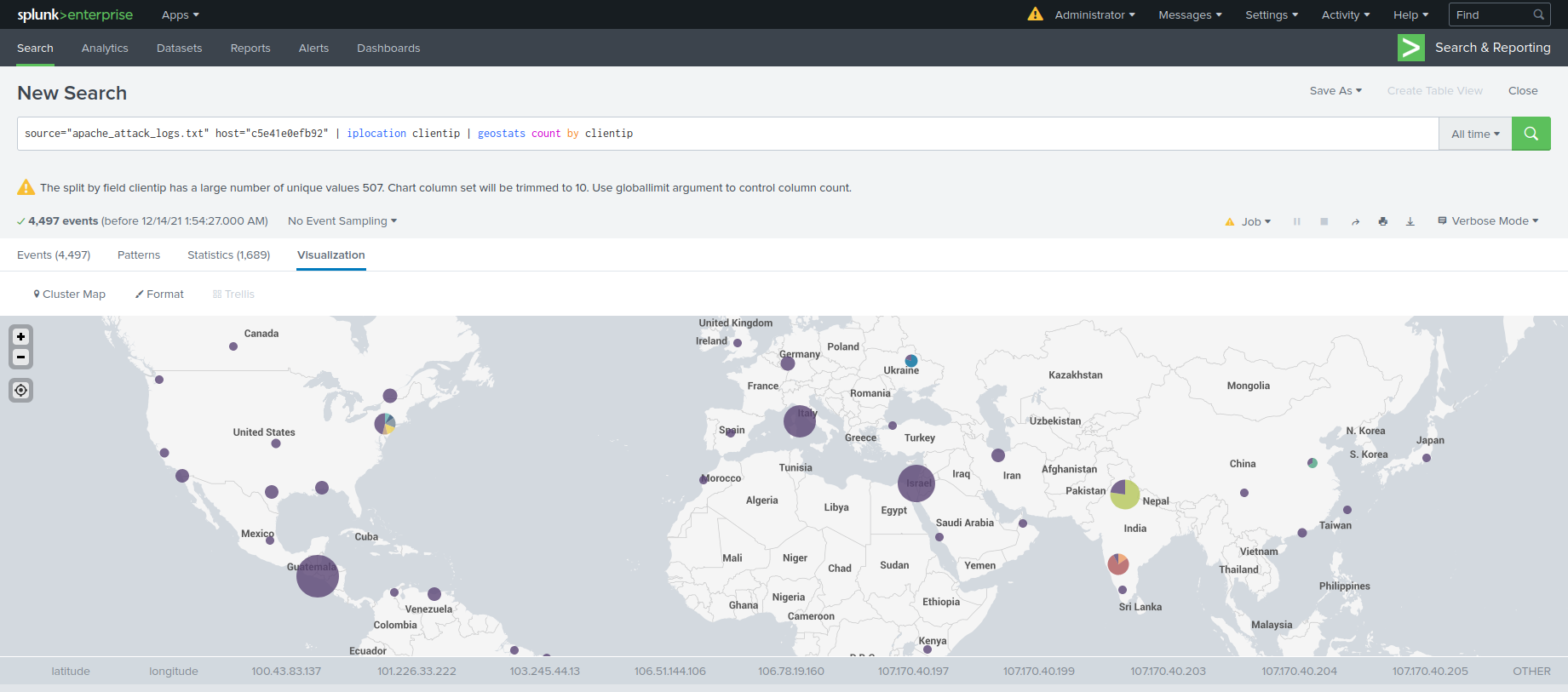
#### Question 1

- Based on the geographic map, recommend a firewall rule that the networking team should implement.

- Provide a "plain english" description of the rule.

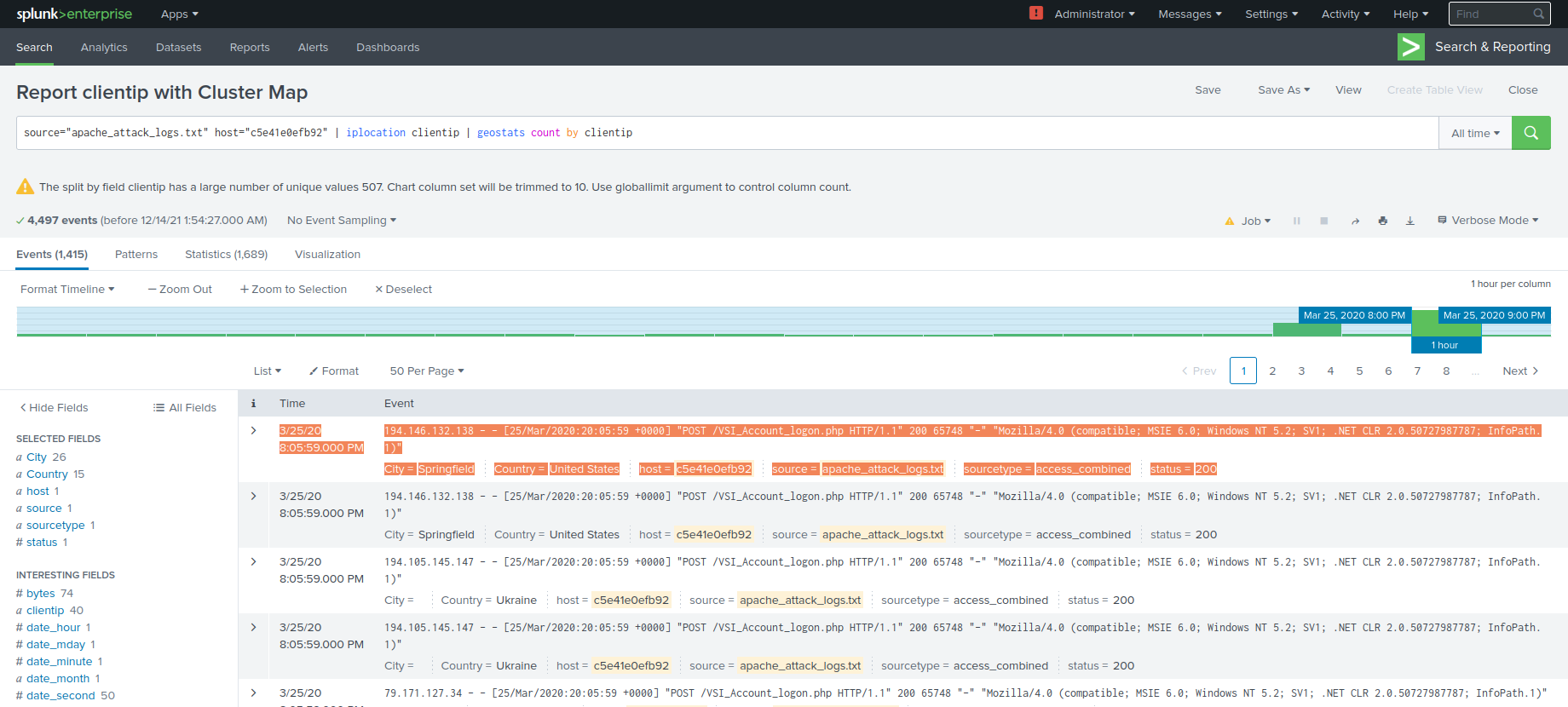
- For example: "Block all incoming HTTP traffic where the source IP comes from the city of Los Angeles."

- Provide a screen shot of the geographic map that justifies why you created this rule.   


  
  
#### Question 2

- VSI has insider information that JobeCorp will launch the same webserver attack but use a different IP each time in order to avoid being stopped by the rule you just created.

- What other rules can you create to protect VSI from attacks against your webserver?  
  
By creating a rule that requires a threshold that allows certain amount of connections to the web server during off hours, 10 connections only within five minutes. If it exceeds, set alarm and send an email to the SOC team.  
  
I added status to the search status: 200 illustrates that the connection was successful. It indicates the city from where the connection came from.

  
  
I tracked the top IP addresses:

