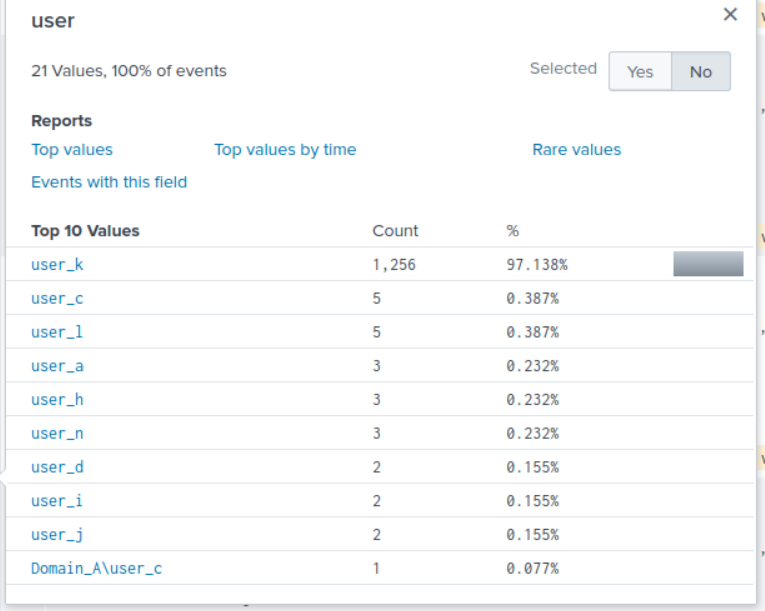
### **Windows Server Attack Project**

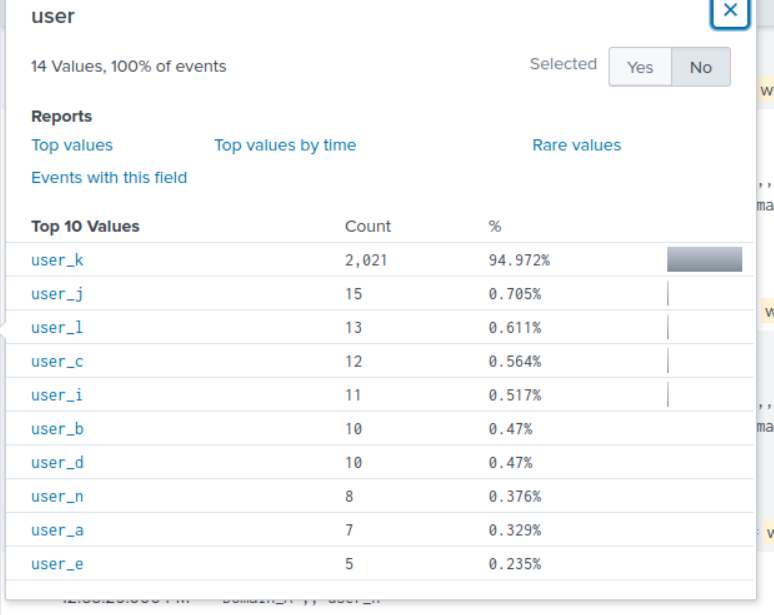
Note: This is a public-facing windows server that VSI employees access.

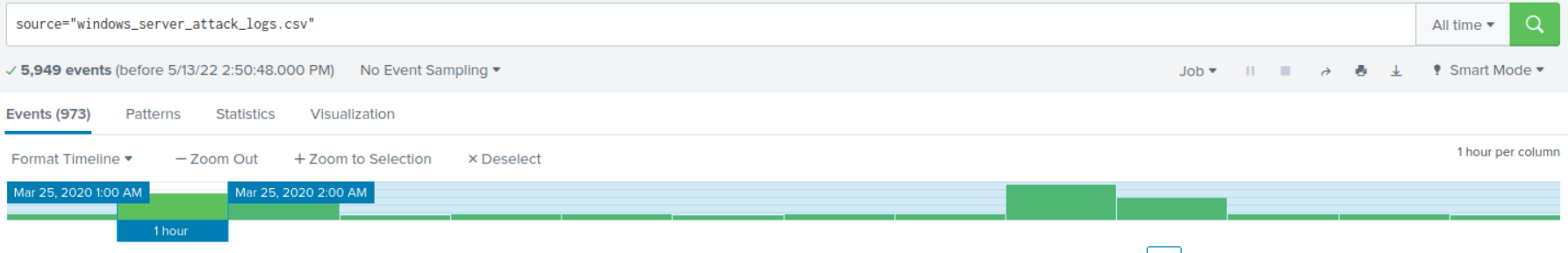
#### **Question 1**

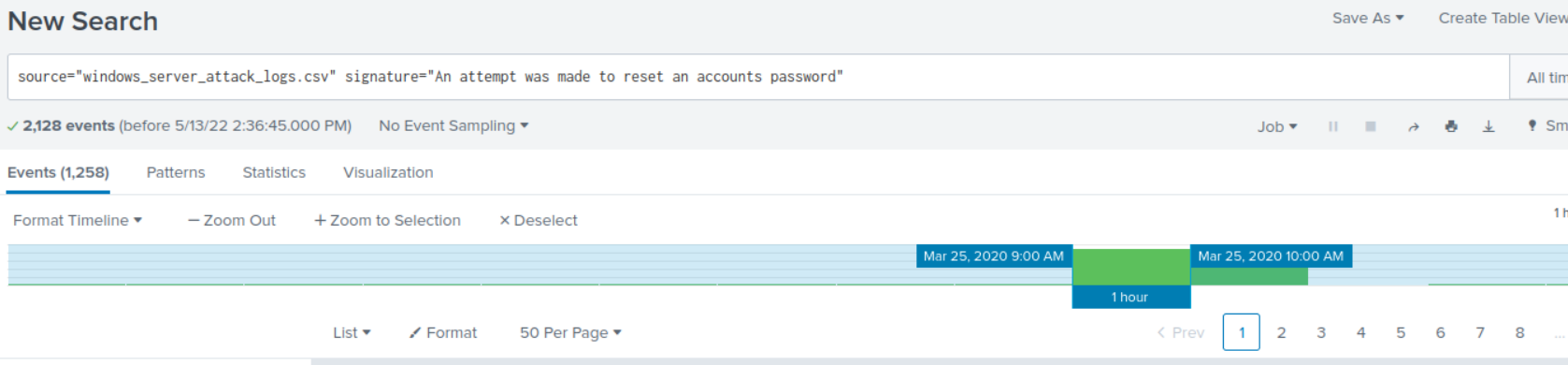
Several users were impacted during the attack on March 25th.

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.









On Wednesday March 25, 2020 the Windows server attack logs show that at 1:00 am - 973, 2:00 am - 1007, 9:00 am - 1,258, and 10:00 am there were 761 attempts made to reset account passwords. User K had the highest attempts.

The best global mitigation for a company is to add the following corrective actions in place: auto lock out after 5 attempts, delay the response between attempts, IP address lock-out, and brute force site scanners.

#### **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?

**The company can use IP address lock-out. If failed attempts from a given IP address exceed a maximum predefined number, that address can be locked out… though if the attacker is using a botnet, with many IP addresses for its bots, this approach will be inadequate.**

### **Part 2: Apache Webserver Attack:**

#### **Question 1**

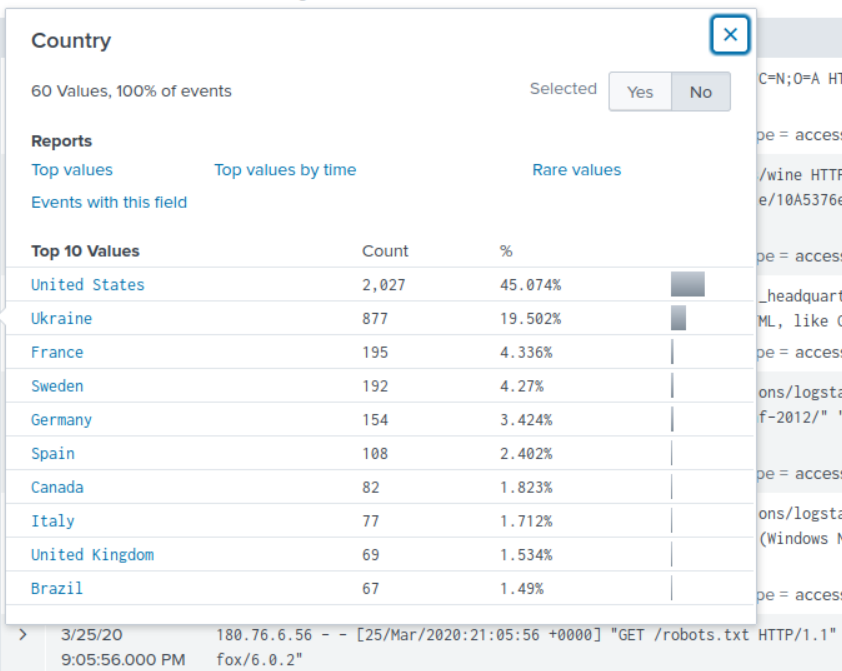
Based on the geographic map, recommend a firewall rule that the networking team should implement.

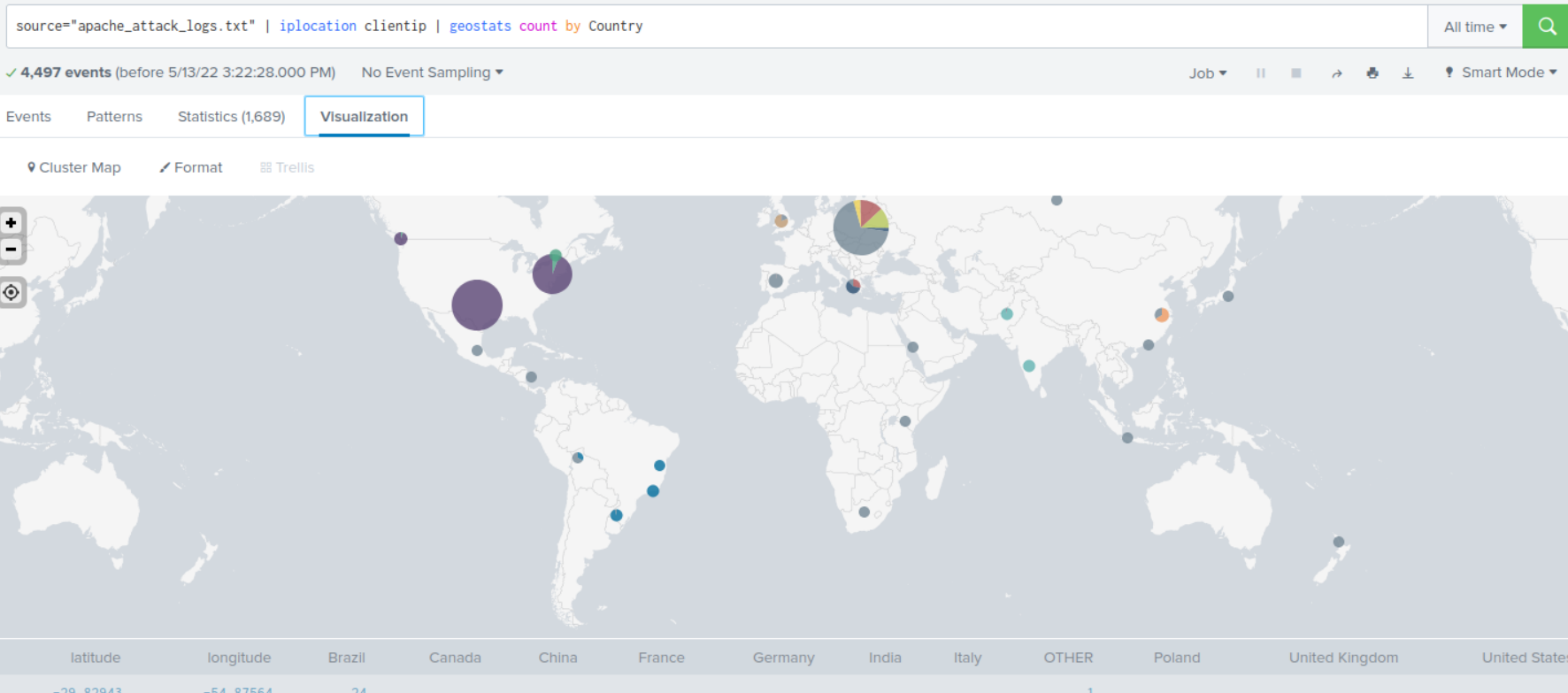
Provide a "plain english" description of the rule.

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

Provide a screenshot of the geographic map that justifies why you created this rule.

I recommend blocking all incoming HTTP traffic where the source IP comes from, which is Ukraine.





#### **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?  
Conceive of two more rules in "plain english".

Hint: Look for other fields that indicate the attacker.

**The two rules that I recommend: (1) Block or limit the user agent “Mozilla/4.0 because this user agent has the highest number count of 1,296 28%. (2) Block all incoming HTTP traffic in the amount of 65748.**

