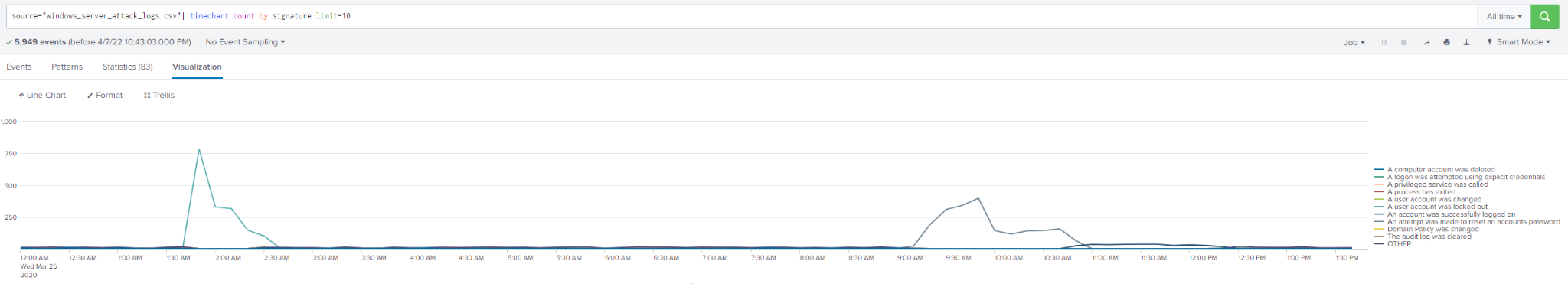
Unit 19 Homework:  
Protecting VSI from Future Attacks

Leo Katz  
4/6/2022

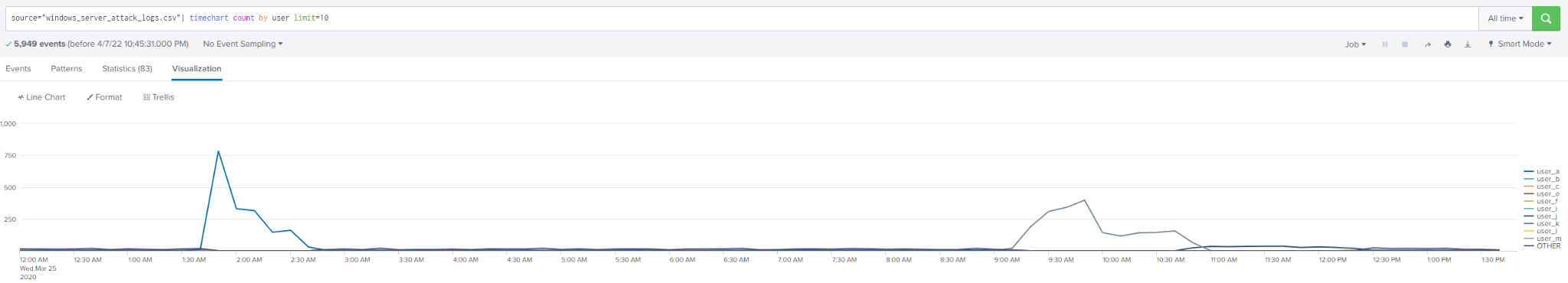
### Part 1: Windows Server Attack

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.



[Figure 1](https://drive.google.com/file/d/1idVoYkZKQx0jEjj-MBY2OkGCSiCHADuu/view?usp=sharing)



[Figure 2](https://drive.google.com/file/d/1b_mha6G4XyWMlVE7e66WRgP9KKgIbyP6/view?usp=sharing)

A strong general solution would be to add multi-factor authentication (MFA) to the VSI login portal. A captcha would also be helpful. Together, these controls would greatly mitigate the threat from JobeCorp.

Individual Solutions:

* User\_K: An attempt was made to reset the account password.
  + The best control for this user would be to set user-specific login alerts with a lower threshold in order to more closely monitor the situation.
* User\_A: A user account was locked out.
  + It appears that the attacker is attempting to brute force User\_A’s password. Therefore, User\_A should immediately change their password, and ensure that it is sufficiently strong and complex.
* User\_J: An account was successfully logged on.
  + Unfortunately, it appears that the User\_J account was compromised. This account should be immediately locked and then carefully inspected. If nothing suspicious appears under scrutiny, then the administrator should manually change the password and unlock the account–in that order.

Question 2:

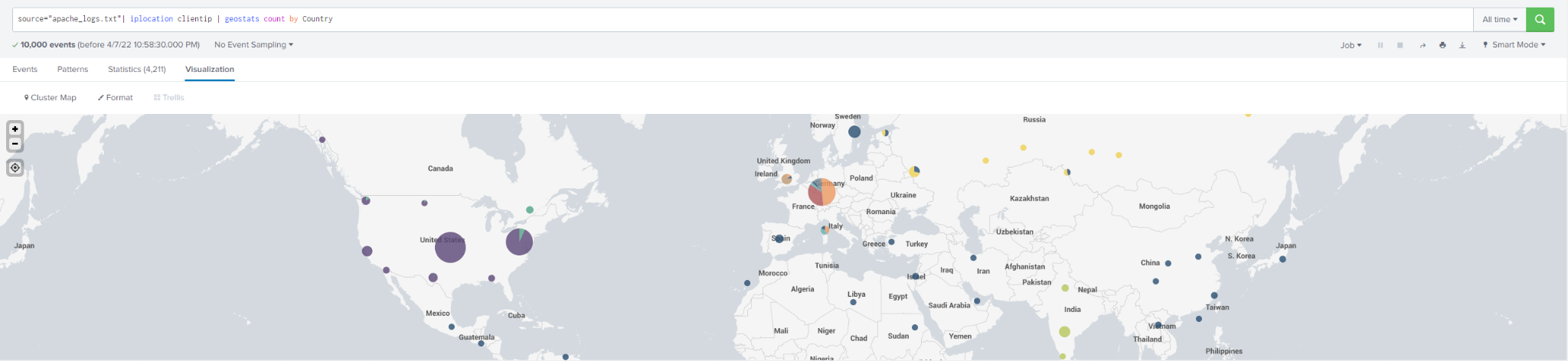
* VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.
* What sort of mitigation could you use to protect against this?

One of the most simple and effective controls against such a Denial of Service attack is to add a mandatory waiting period for each login attempt. Several seconds will be sufficient to drastically slow down automated DoS attempts, but not unduly inconvenience users. A captcha would also help protect accounts from being locked out.

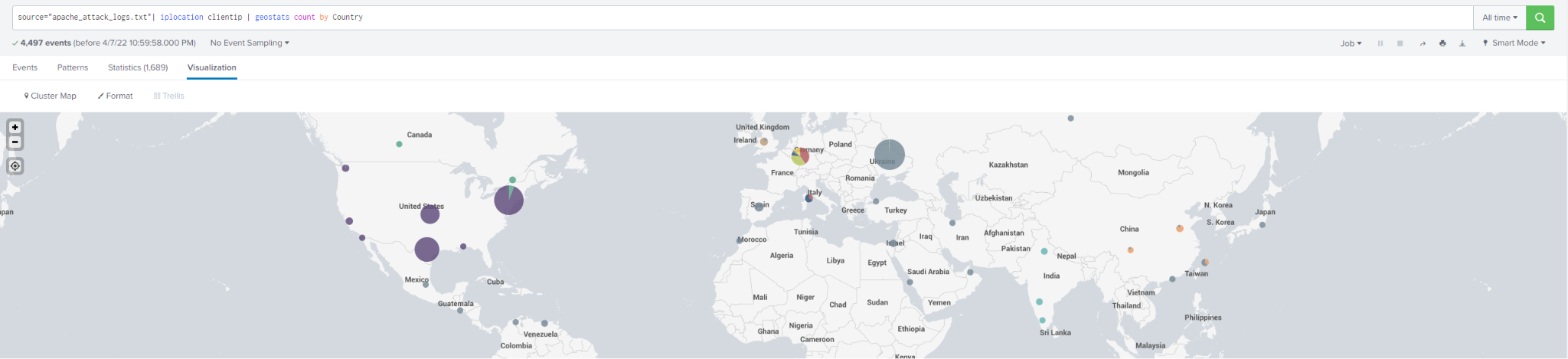
### Part 2: Apache Webserver Attack

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.



[Figure 3](https://drive.google.com/file/d/1dYH4y8PvMzMbOdBHvcE-1Ok79MLaeJkc/view?usp=sharing)



[Figure 4](https://drive.google.com/file/d/1p41UGRh5-GLAqRLzaPtrZf2PMgjHdWAh/view?usp=sharing)

The difference between normal activity in Figure 3 and the webserver attack in Figure 4 shows that most of the attacks are coming from Ukraine. And, importantly, there is no apparent legitimate traffic from Ukraine. Therefore, the networking team should implement a firewall rule to block all incoming HTTP traffic from 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.

Two other indicators of attack are the “bytes” field and the “user\_agent” field. The byte amount for attacks is consistently 65748 bytes, and the user agent for attacks is “Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)." When put into network rules, these two indicators might be used as follows:

* Block all incoming HTTP traffic where the user\_agent is “Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)."
* Block all incoming HTTP traffic where the bytes amount is equal to 65748.