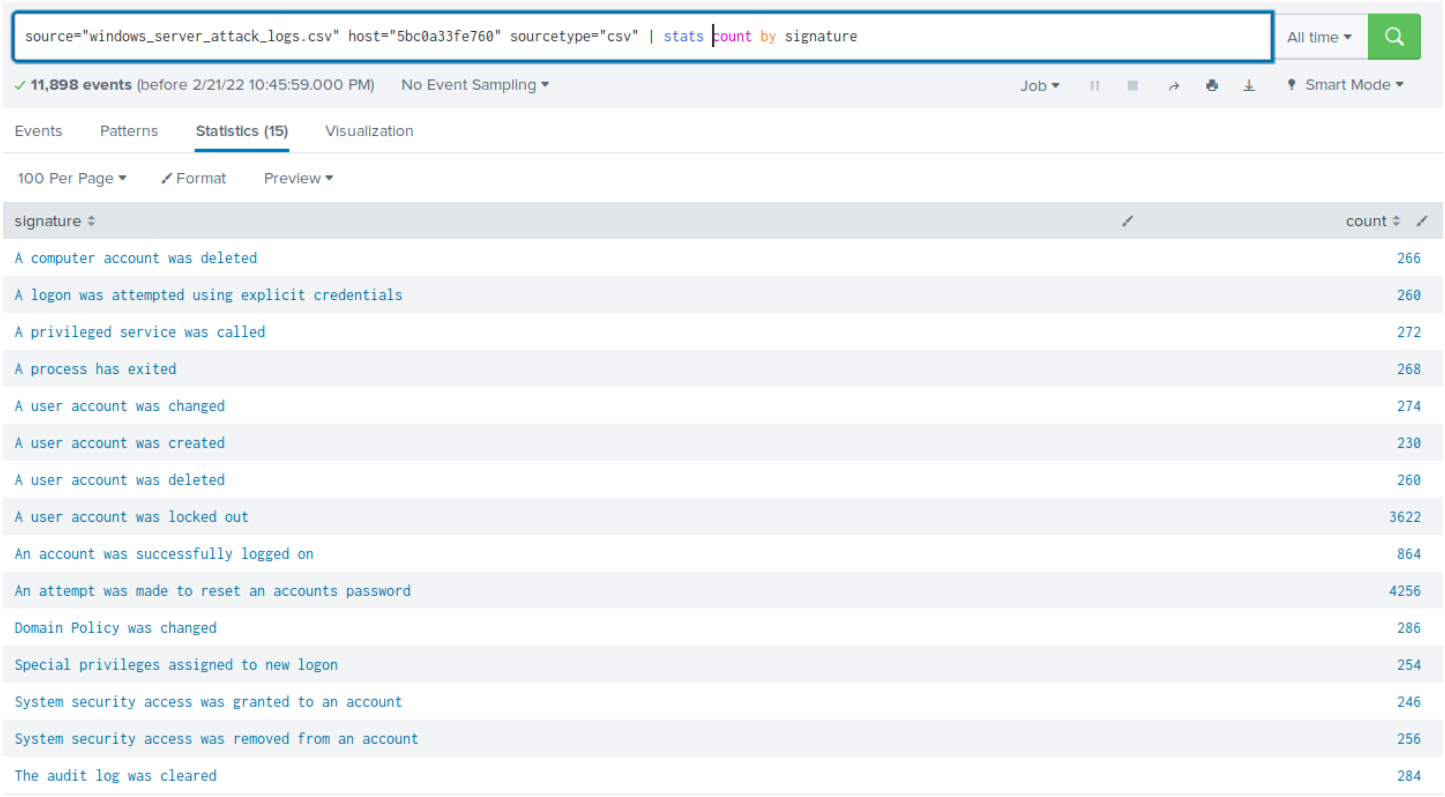
Part 1: Windows Server Attack

Question 1

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.

- Here are the attack signatures I used to make these recommendations:



signature	count
A computer account was deleted	266
A logon was attempted using explicit credentials	260
A privileged service was called	272
A process has exited	268
A user account was changed	274
A user account was created	230
A user account was deleted	260
A user account was locked out	3622
An account was successfully logged on	864
An attempt was made to reset an accounts password	4256
Domain Policy was changed	286
Special privileges assigned to new logon	254
System security access was granted to an account	246
System security access was removed from an account	256
The audit log was cleared	284

- The most alarming signatures counts are the following:
  - “A user account was locked out” – this indicates attackers trying to brute force the password for an account
  - “An attempt was made to reset an accounts password”
- Mitigation Recommendations:
  - Require users to set up MFA – multi-factor authentication. This will increase the overall security of user accounts.
  - Blacklist IPs that make an unreasonable number of password change requests.

- Only allow one password change request in a given period of time – one week for example.
- Lock out accounts for longer periods of time or perhaps even consider only unlocking accounts after the user has contacted support.
- If deciding on a period of time to keep accounts locked, then permanently lock accounts after two consecutive lockouts.

Question 2

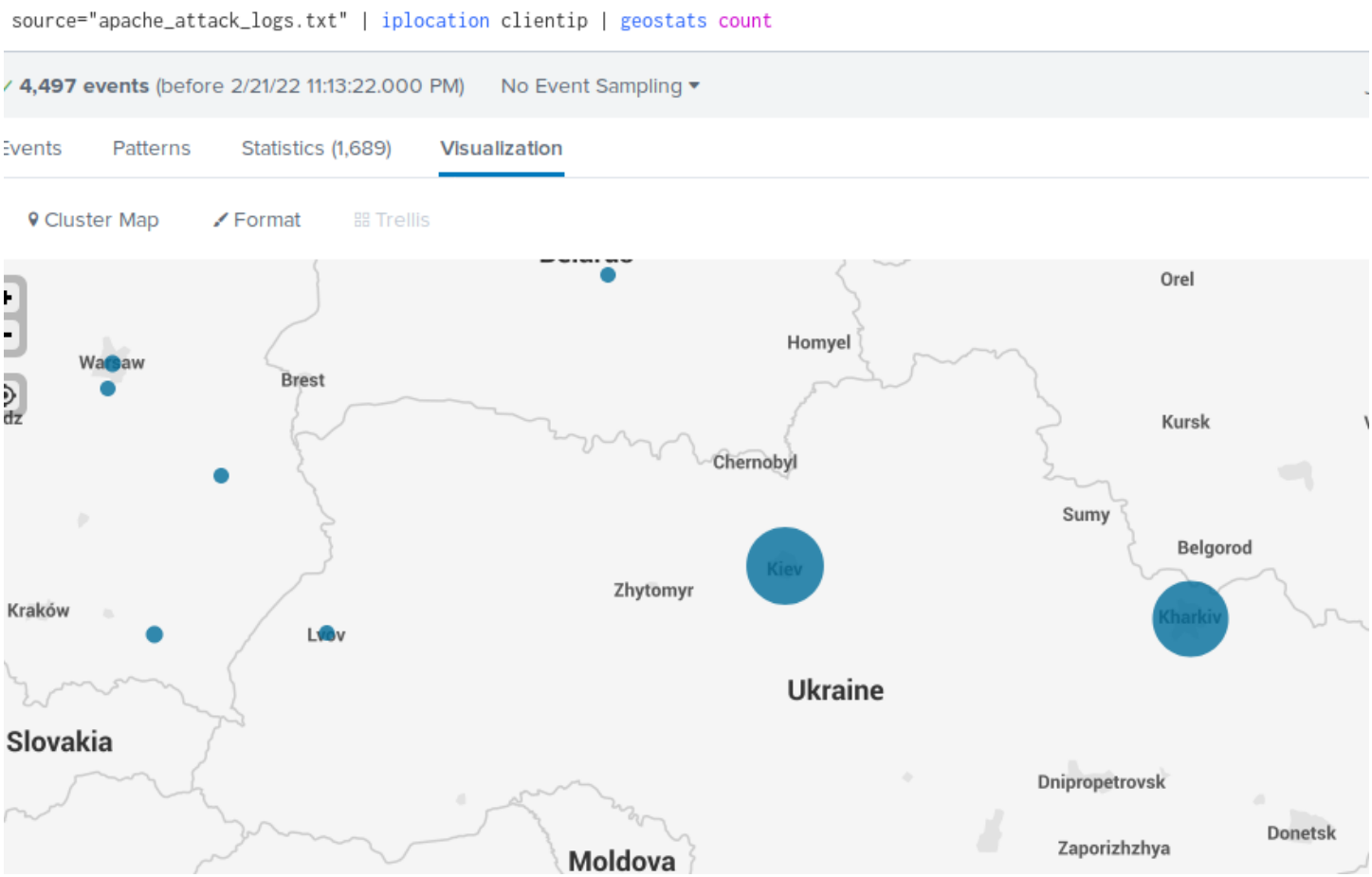
VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user. What sort of mitigation could you use to protect against this?

- Mitigation recommendations:
  - Most likely these bad logins were sent from a given IP or set of IPs. In this case you could blacklist any IP that has consecutive “bad login” requests.

Part 2: Apache Webserver Attack

Question 1

Here’s the map that I used for the following recommendations:

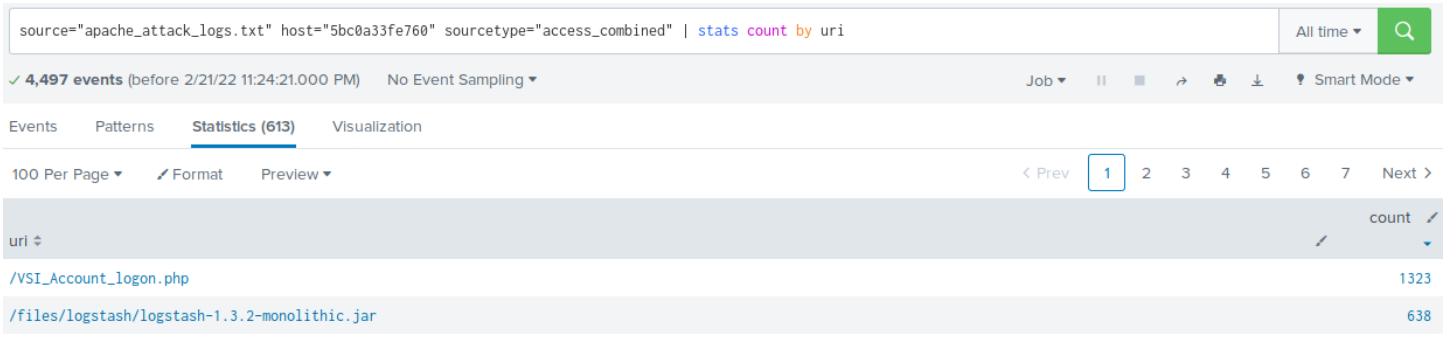


And here’s the counts for the above map that helped me decide Ukraine was the country to focus on:

I would use a rule that does the following: blocks all HTTP traffic that comes from the cities of Kiev and Kharkiv, Ukraine.

Question 2

Here's the data I used in order to make the firewall rule recommendations:



The "URL" and "user agent" fields contained the most common values during the time of the attack. So, we can generate firewall rules based on those values. Also, we'll need to create stateful firewall rules that are based on the number of consecutive POST requests.

- Blacklist IPs that have sent a given number of POST requests – the specific number will need to be decided based on testing in order to not filter legitimate traffic – and the URL or URL path is "/VSI_Account_logon.php".
- Blacklist IPs that have sent a given number of POST requests – the specific number will need to be decided based on testing in order to not filter legitimate traffic – and the user agent is the one listed at the top of the table in the second screen shot.