### 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.

- 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.

-I would have to say to limit the amount of bad logins an account can have before being locked out and the possibility of after so many bad logins in a certain time limit only a systems administrator can unlock the account or only let certain ip addresses log into it.

#### 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 mitigation would be to find out the ip addresses used by JobeCorp and block them or to only allow employee ip addresses to have access to login pages.

### Part 2: Apache Webserver Attack:

#### Question 1

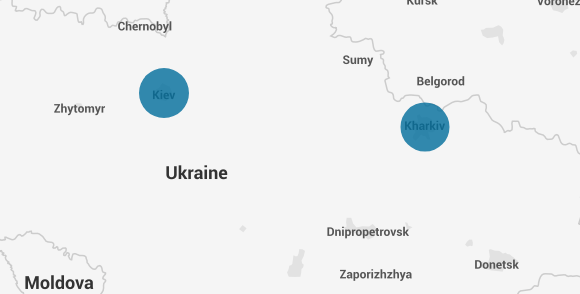
- Based on the geographic map, recommend a firewall rule that the networking team should implement.

- 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.

-A firewall rule would be to block non-employee IP addresses from the Ukraine specifically Kiev and Kharkiv, because those two cities had the largest increase in activity after the attack.



#### 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.

- A rule would be to block traffic from older versions of Mozilla. After the attack there was a huge influx from Mozilla 4.0 and Chef Client vs pre attack it was all on Mozilla 5.0. This tells me that they are using an older version of Mozilla so I would block all traffic from that version.