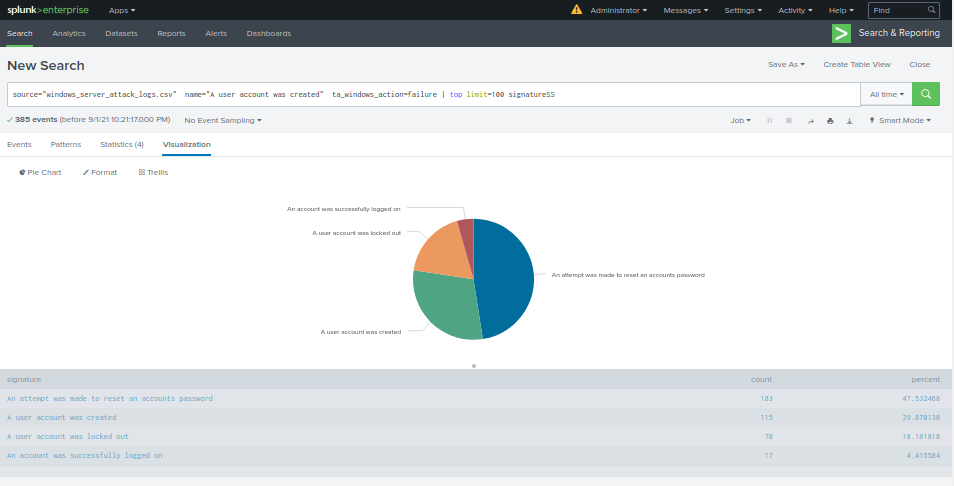
Part 1: Windows Server Attack

Note: This is a public-facing windows server that VSI employee’s access.

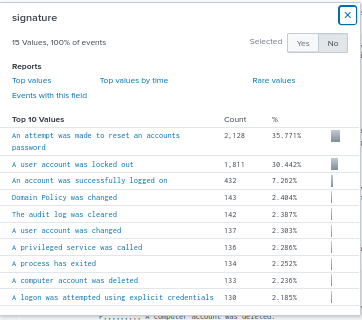
Question 1

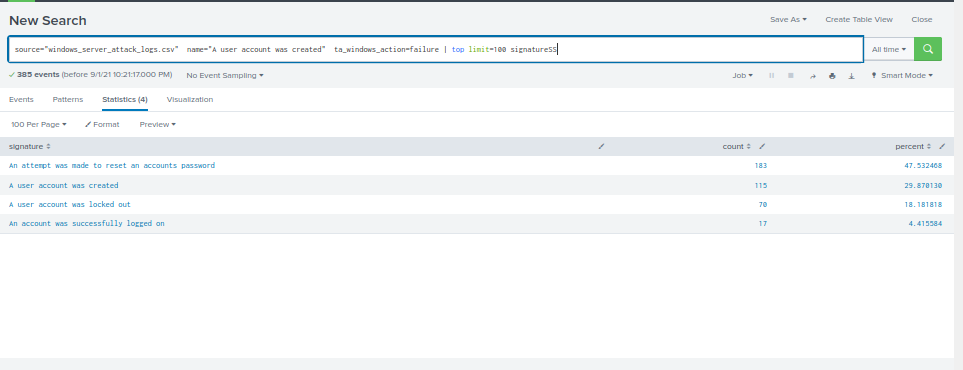
Several users were impacted during the attack on March 25th.



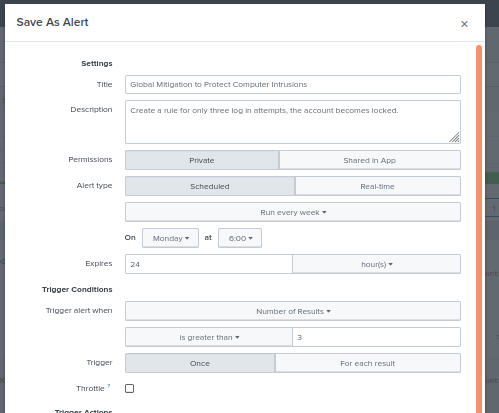
Based on the attack signatures, what mitigations would you recommend to protect each user account?

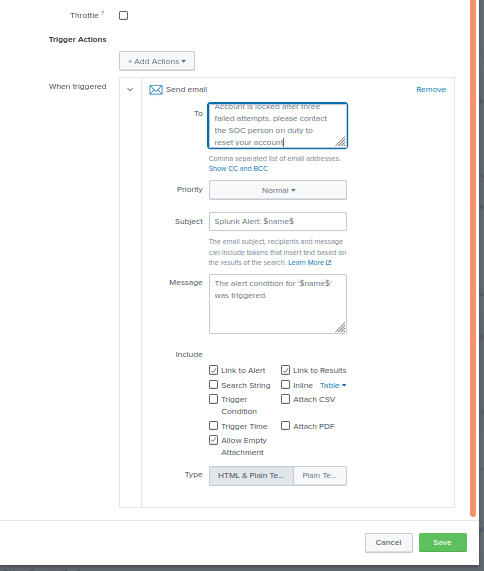
Set up a time alert to reset accounts so [SOC@email.com](mailto:SOC@email.com) is alerted after 3 resets within a 24-hour period and lock the account.





Provide global mitigations that the whole company can use and individual mitigations that are specific to each user.





**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?

I would use 3 failed login attempt lock-out for each user and create an alert. I would automate the user to change their credentials by email.

### Part 2: Apache Webserver Attack:

#### Question 1

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

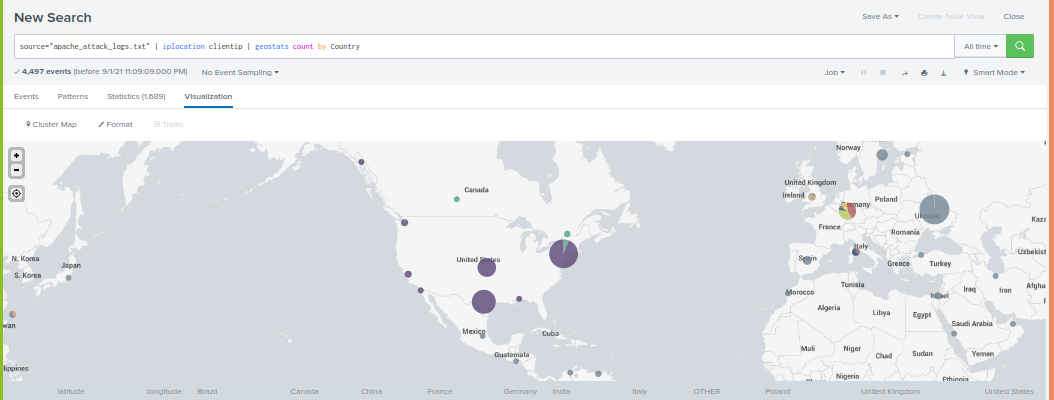
Block country IP addresses

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."

Most of the IP addresses are coming from Ukraine. Block incoming Ukraine traffic from entering the server.

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



Because most of the IP addresses are coming out of the Ukraine. So I would block all 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?

I would create a rule that will block packages of the size 65748.

Create a rule where if there are more than 3 login attempts the account will be locked out.

Create a rule where this user agent cannot be used.

