Unit 19 Project: Protecting VSI from Future Attacks

Scenario

In the previous class, you set up your SOC and monitored attacks from JobeCorp. Now, you will need to design mitigation strategies to protect VSI from future attacks.

You are tasked with using your findings from the Master of SOC activity to answer questions about mitigation strategies.

System Requirements

You will be using the Splunk app located in the Ubuntu VM.

Logs

Use the same log files you used during the Master of SOC activity:

- Windows Logs
- Windows Attack Logs
- Apache Webserver Logs
- Apache Webserver Attack Logs

Part 1: Windows Server Attack

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

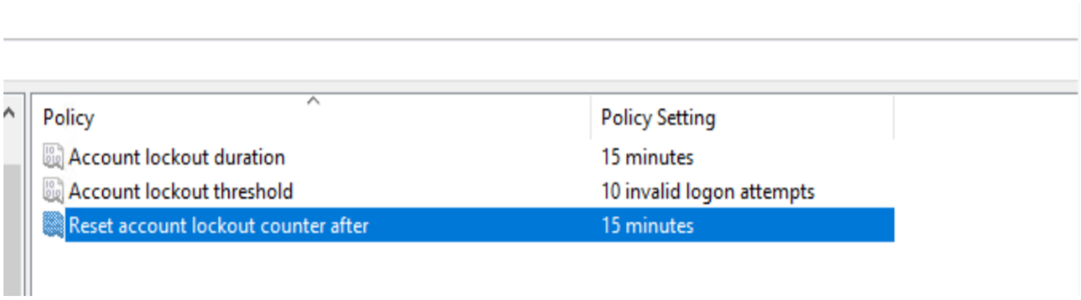
Question 1

- 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.

  -User accounts should be locked out after 5 incorrect attempts. This helps in reducing the vulnerability of several user accounts,

  -Users should only be allowed to attempt to reset their password once in any 15 hours period. During the 9:00 AM hour, 1,258 total attempts were made to reset a password. Limiting this number of times a user can reset their password would mitigate this vulnerability.

-Individual user accounts, users should be required to use some sort of multi-factor authentication



Policy	Policy Setting
Account lockout duration	15 minutes
Account lockout threshold	10 invalid logon attempts
Reset account lockout counter after	15 minutes

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?

  -Online Services Should Send Reset Links Or Send Code Over Phone Calls

  -Allow a set number of "bad logins", once the threshold is met, a text/email would be sent to the victim user, rather than locking them out from the get go.

Part 2: Apache Webserver Attack:

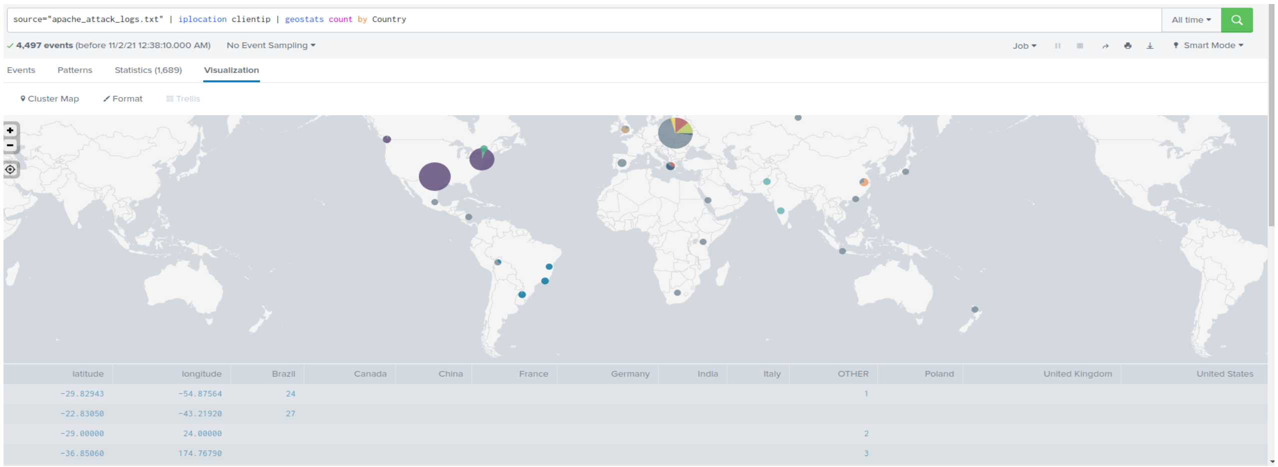
Question 1

- 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."

  -VSI's Apache Web Server was attacked on March 25, 2020 between the hours of 6:00 PM and 9:00 PM. Based on the data, it seems this attack originated in Kiev, Ukraine. To mitigate against future attacks from the same threat actor, the SOC team recommends the following firewall rule be implemented:

  -Block all incoming HTTP traffic where the source IP = 79.171.127.34 & IP= 194.105.145.147 comes from the country of Ukraine

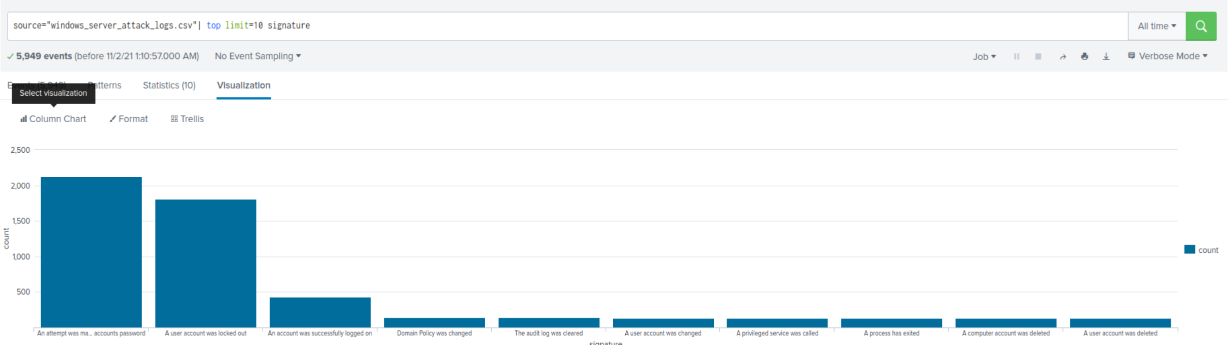
- Provide a screenshot of the geographic map that justifies why you created this rule.



```
source="apache_attack_logs.txt" | iplocation clientip | geostats count by Country
```

✓ 4,497 events (before 11/2/21 12:38:10.000 AM)

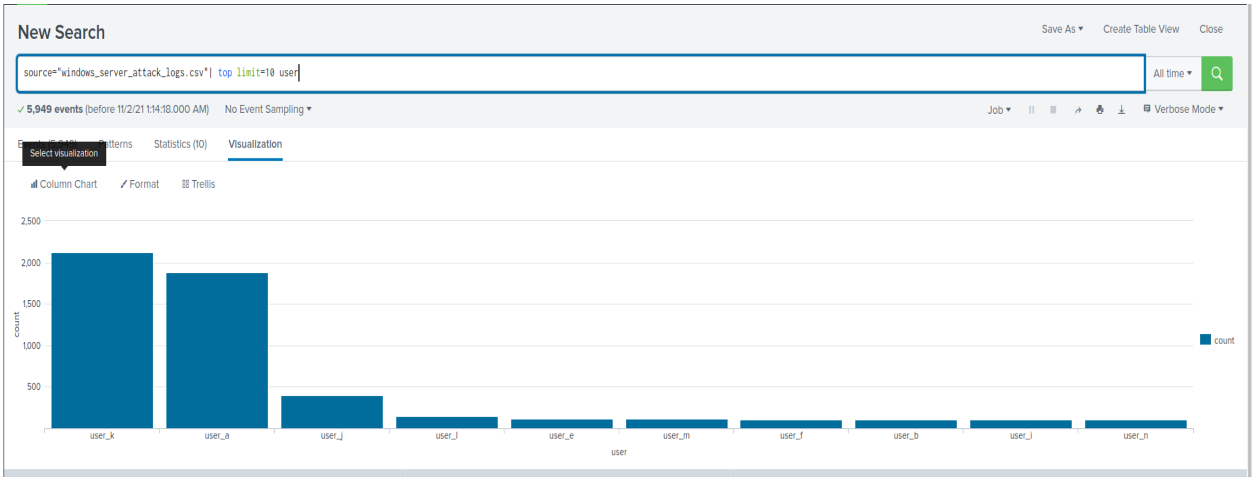
latitude	longitude	Brazil	Canada	China	France	Germany	India	Italy	OTHER	Poland	United Kingdom	United States
-29.82943	-54.87564	24							1			
-22.83050	-43.21920	27										
-29.00000	24.00000								2			
-36.85060	174.76790								3			



```
source="windows_server_attack_logs.csv"| top limit=10 signature
```

✓ 5,949 events (before 11/2/21 1:10:57.000 AM)

All time ▾
No Event Sampling ▾
Job ▾
Verbose Mode ▾
Select visualization
Patterns
Statistics (10)
Visualization
Column Chart
Format
Trellis
2,500
2,000
1,500
1,000
500
count
An attempt was ma... accounts password
A user account was locked out
An account was successfully logged on
Domain Policy was changed
The audit log was cleared
A user account was changed
A privileged service was called
A process has exited
A computer account was deleted
A user account was deleted
signature
count



New Search

```
source="windows_server_attack_logs.csv"| top limit=10 user
```

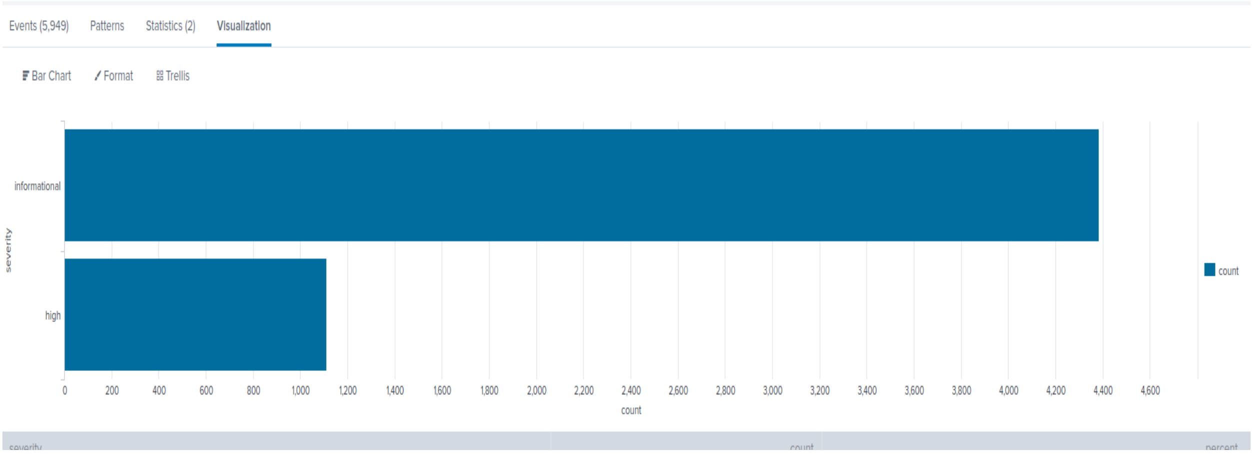
✓ 5,949 events (before 11/2/21 1:14:18.000 AM)

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.

1-limited on concurrent requests or total requests over a given duration (50 requests per minute) can be an excellent way to reject traffic and maintain service stability
2-Block any IP address which generates three or more consecutive POST requests to the login page (“/VSI_Account_logon.php”). This would prevent any brute-force attacks on the login page, regardless of source IP.
3-Block any IP address which generates three or more consecutive POST requests identified by the user agent string “Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)”.


Events (5,949)
Patterns
Statistics (2)
Visualization
Bar Chart
Format
Trellis
severity
informational
high
0
200
400
600
800
1,000
1,200
1,400
1,600
1,800
2,000
2,200
2,400
2,600
2,800
3,000
3,200
3,400
3,600
3,800
4,000
4,200
4,400
4,600
count
count
severity
count
percent