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.

  A good solution would be to block all foreign IP addresses or only allow knows IP addresses.

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?

  Allow a set number of “bad logins”, once the threshold is met, a text/mail 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."

      Block all incoming traffic from Ukraine

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

Country

58 Values, 100% of events

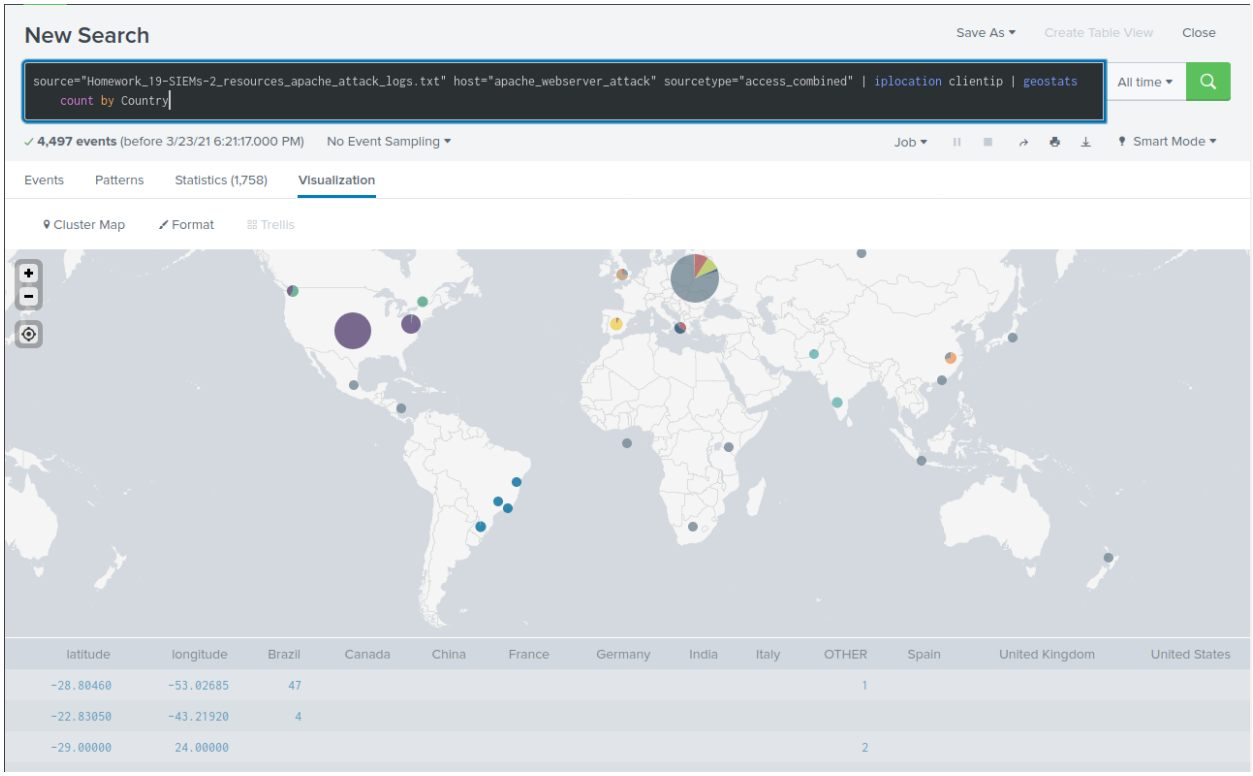
Selected Yes No

Reports

Top values | Top values by time | Rare values

Events with this field

Top 10 Values	Count	%
United States	1,592	35.401%
Ukraine	1,309	29.108%
France	196	4.358%
Sweden	192	4.27%
Germany	154	3.424%
Spain	108	2.402%
Canada	84	1.868%
Italy	77	1.712%
United Kingdom	69	1.534%
Brazil	66	1.468%



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 two more rules in "plain English".
    - Hint: Look for other fields that indicate the attacker.

      Block all incoming traffic with a byte count of 65748

      Limit number of HTTP Get request

      Block Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1) user agent request

bytes

>100 Values, 100% of events

Selected: Yes | No

Reports

Average over time | Maximum value over time | Minimum value over time

Top values | Top values by time | Rare values

Events with this field

Avg: 218969.75306678782 **Min:** 35 **Max:** 69192717 **Std Dev:** 2954456.3728965824

Top 10 Values	Count	%
65748	1,322	29.397%
324	638	14.187%
3638	232	5.159%
4877	151	3.358%
6146	150	3.336%
1015	149	3.313%
52315	144	3.202%
14872	114	2.535%
-	95	2.112%
12292	71	1.579%

method

4 Values, 100% of events

Selected: Yes | No

Reports

Top values | Top values by time | Rare values

Events with this field

Values	Count	%
GET	3,157	70.202%
POST	1,324	29.442%
HEAD	15	0.334%
OPTIONS	1	0.022%

useragent

>100 Values, 99.978% of events

Selected Yes No

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)	1,296	28.826%
Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)	638	14.19%