Unit 19 Homework: 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

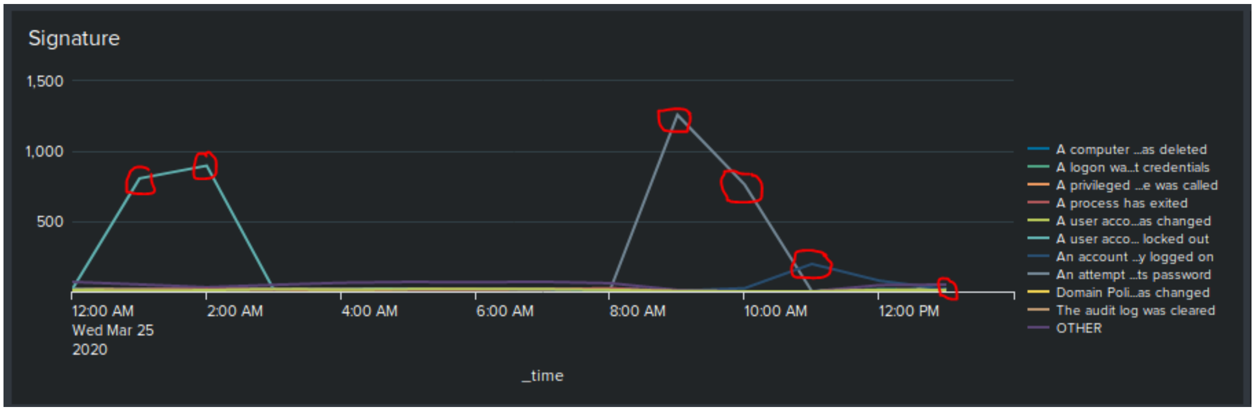
Part 1: Windows Server Attack

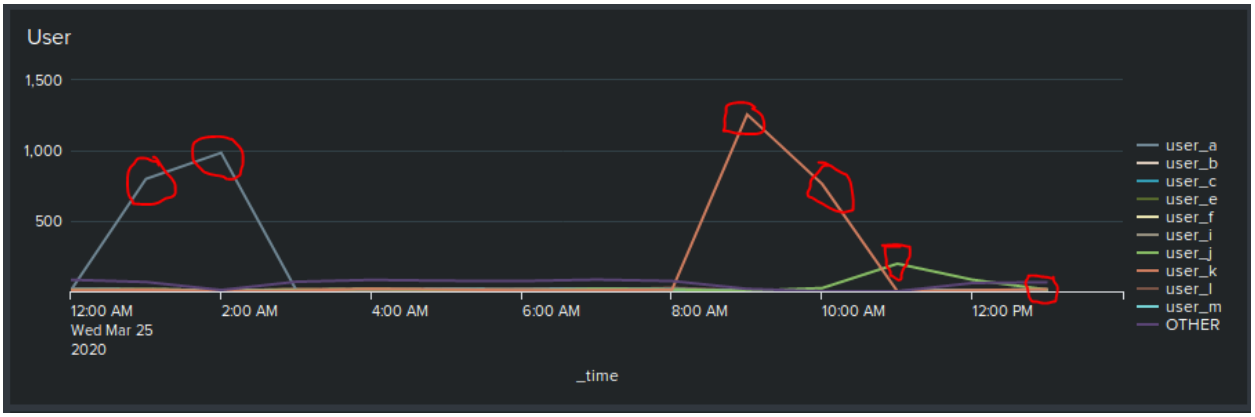
Note: This is a public-facing windows server that VSI employees access.

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.
    - **Global Solution:**
    - **The best global mitigation would probably be to add multi-factor authentication to the companies systems. This would greatly reduce the number of successes of a threat actor to access user accounts.**
    - **Individual Solution:**
        - **User_K: An attempt was made to reset an account password.**
        - **The logs for this user do not show any evidence that the attacker was ever able to successfully log into or reset the password for user_k, however, there were several attempts to reset the password.**

- The best mitigation for this user would be to set up user-specific alerts with lower values in order to more closely analyze and watch for the users password getting changed again.
- User_A: A user account was locked out.
- User_A should change their password immediately to something completely different and ensure that the complexity is high. This is because the attacker is trying to brute force their way to the users password in order to steal the account.
- User_J: An account was successfully logged on.
- This log shows that the attacker was able to successfully obtain the users password.
- The best thing to do in this scenario is to manually change the password for User_J.
- You could also apply the same mitigation we used for User_K and apply user-specific alerts to watch the users activity more closely.
- All other users had accounts either created or changed.





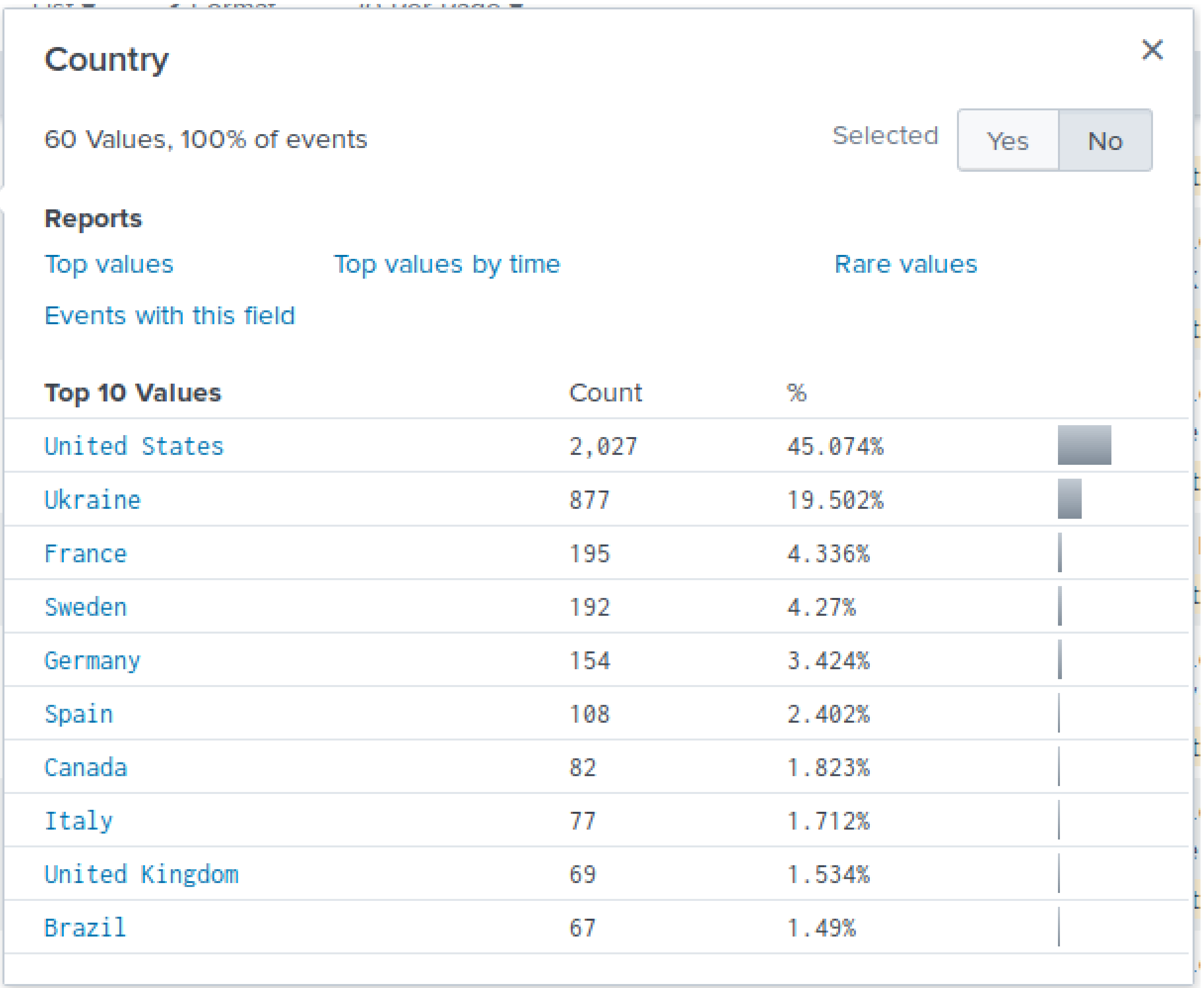
Question 2

- 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?
  - **The easiest solution would be to set up a group policy for the company that would automatically unlock users accounts after a specific amount of time.**
  - **As soon as the company finds out about this insider attack, the employees should also be notified immediately to be more vigilant and careful about who they accept information from.**

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.
    - **Most of the incoming attacks were coming from Ukraine, therefore we should set up a firewall rule to block HTTP traffic from Ukraine.**
    - **Firewall Rule Description - "Block all incoming HTTP traffic where the source IP comes from the country of Ukraine"**



Country

60 Values, 100% of events

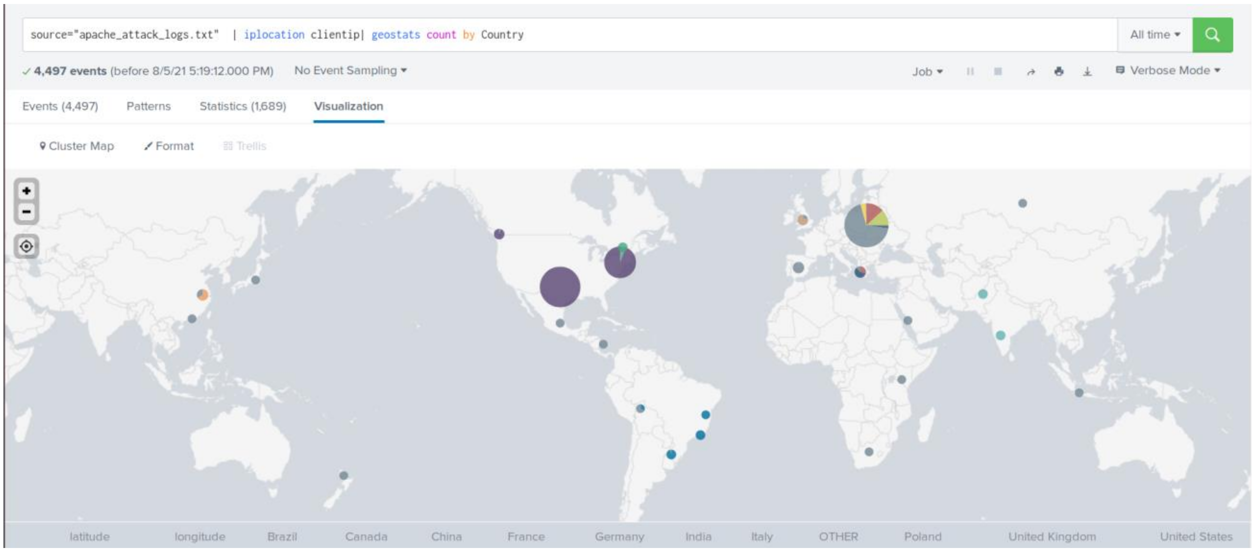
Selected Yes [✓ No]

Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
United States	2,027	45.074%
Ukraine	877	19.502%
France	195	4.336%
Sweden	192	4.27%
Germany	154	3.424%
Spain	108	2.402%
Canada	82	1.823%
Italy	77	1.712%
United Kingdom	69	1.534%
Brazil	67	1.49%



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

✓ 4,497 events (before 8/5/21 5:19:12.000 PM)

- **The screenshot above shows Ukraine's incoming HTTP Traffic**

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.
  - **You can create two others rules based off of 'user_agent' and 'bytes'. The recurring user agent is "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)." and the recurring byte amount is 65748.**
  - **Both rule descriptions would be as follows**
    - **"Block all incoming HTTP traffic where the useragent is "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)."**
    - **"Block all incoming HTTP traffic where the bytes amount is 65748."**