Unit 19 SIEM Assignment

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.

Logs

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

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

- For user a: This user was a victim of a lockout attack, with the highest lockout number at 896. Some mitigation strategies for this user include input sanitation/validation, 2-factor authentication, and an account lockout policy that includes a captcha, a timed account reset of an hour, and a limit for failed log in attempts.
- For user k: This user was a victim of a password reset attack. Some mitigation strategies include limiting the amount of times a user can request a password reset to 3 resets per day, and a reset email that notifies the user they made a

password reset request, to prevent unauthorized requests. When resetting the password, include security questions before approving the request, to add an extra layer of security.

- For user j: This user is a victim of a successful login attack, with potential attempt to crash the server. One mitigation strategy includes capping and sending an alert when successful login of a user surpasses the normal threshold in a one hour span. Another strategy would be to notify the user if they are logged from an unknown device. Also to protect User_J, we should also change their password ASAP since the attacker was able to successfully login to the account.
- Provide global mitigations that the whole company can use and individual mitigations that are specific to each user.
- I would make sure that each user receives a unique temporary password when trying to reset their account password. Before the password can be reset, an email notifying the user that they requested a password reset will be sent.
- As a company, I would ensure there is input sanitization and validation.
- Limit number of failed login attempts and the logins to specific IPs in range.
- Consider having an internally accessible login page url.

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?

- Change the account lockout threshold to either 0 so the account doesn't lock out, or a higher number than currently set.
- Consider adding a captcha to the login page
- Giving the user 3-5 min between lockouts
- Close TCP and UDP to unauthorized networks and further add a threshold to prevent unwanted users.

Part 2: Apache Webserver Attack:

Question 1

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

- "Block all incoming HTTP traffic where the source IP comes from Ukraine."

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

Country

58 Values, 100% of events

Selected Yes No

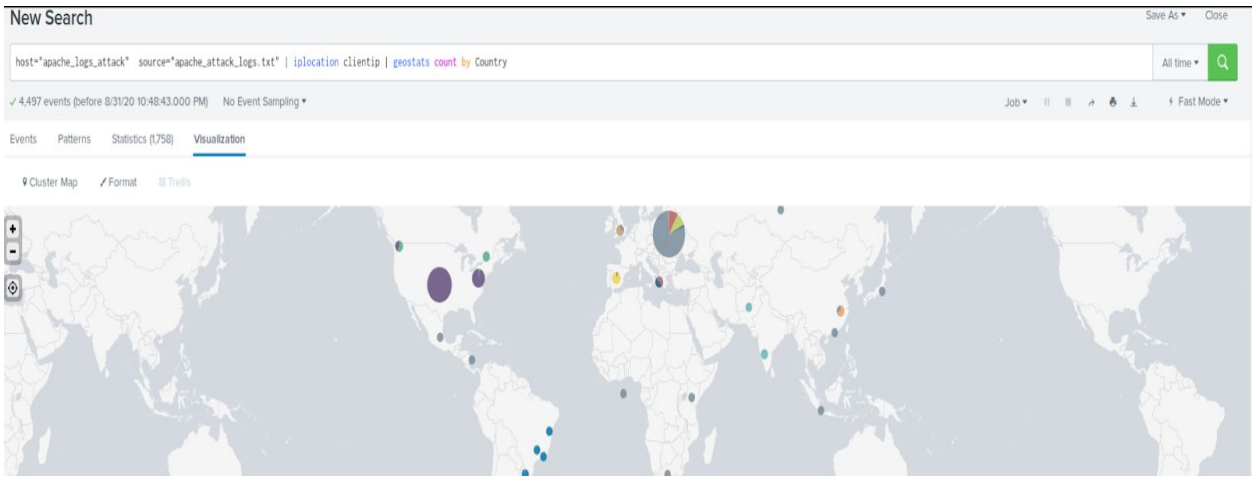
Reports

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%

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



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?

- "Block a number of HTTP POST requests when they surpass threshold."
- **"Limit number of HTTP GET requests based on our baseline to make sure our server doesn't go down."
- "Block Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1) User Agent request when it surpasses baseline."