## 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](resources/windows\_server\_logs.csv)

- [Windows Attack Logs](resources/windows\_server\_attack\_logs.csv)

- [Apache Webserver Logs](resources/apache\_logs.txt )

- [Apache Webserver Attack Logs](resources/apache\_attack\_logs.txt )

---

### 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. Can just add the certain users account to allow users rights based on their IP addresses.

K: An attempt was made to reset an accounts password. Don’t see any info from log that it was automated. There was a reset password. There could be an alert for a report on password resets. Maybe those off hours or on suspicious days/times.

J: successful. It looks like the attacker had the password. An alert could be setup for bot login attempts.

A: locked out. It looks like the attacker may have tried to force their way in with wrong password. User A could try changing their user or password to alphanumeric.

#### 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? Once outside IP’s/hosts/etc are discovered from login in attempts could blacklist those IP’s or hosts. Also can create an alert based on failed logins to run hourly

### Part 2: Apache Webserver Attack:

#### Question 1

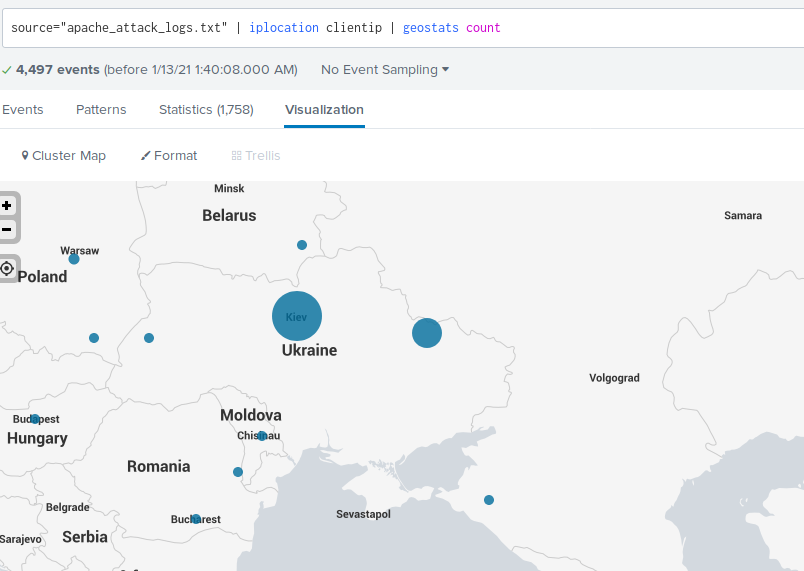
- Based on the geographic map, recommend a firewall rule that the networking team should implement.

- 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.

You could add some criteria to a firewall to block attempted logins from a specific location based on where the attacks are coming from.



#### 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 add an alert to block user/user agents and could set an alert with a threshold for downloading of X bytes.

