

[Part 1: Windows Server Attack](#)

[Question 1](#)

[Question 2](#)

[Part 2: Apache Webserver Attack](#)

[Question 1](#)

[Question 2](#)

Part 1: Windows Server Attack

Question 1

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.

- Here are the attack signatures I used to make these recommendations:

source="windows_server_attack_logs.csv" host="5bc0a33fe760" sourcetype="csv" stats count by signature		All time	🔍
✓ 11,898 events (before 2/21/22 10:45:59.000 PM) No Event Sampling ▼		Job ▼	⏏
Events	Patterns	Statistics (15)	Visualization
100 Per Page ▼	Format	Preview ▼	
signature ↕		count ↕	
A computer account was deleted		266	
A logon was attempted using explicit credentials		260	
A privileged service was called		272	
A process has exited		268	
A user account was changed		274	
A user account was created		230	
A user account was deleted		260	
A user account was locked out		3622	
An account was successfully logged on		864	
An attempt was made to reset an accounts password		4256	
Domain Policy was changed		286	
Special privileges assigned to new logon		254	
System security access was granted to an account		246	
System security access was removed from an account		256	
The audit log was cleared		284	

- The most alarming signatures counts are the following:
 - “A user account was locked out” – this indicates attackers trying to brute force the password for an account
 - “An attempt was made to reset an accounts password”
- Mitigation Recommendations:
 - Require users to set up MFA – multi-factor authentication. This will increase the overall security of user accounts.
 - Blacklist IPs that make an unreasonable number of password change requests.

- Only allow one password change request in a given period of time – one week for example.
- Lock out accounts for longer periods of time or perhaps even consider only unlocking accounts after the user has contacted support.
- If deciding on a period of time to keep accounts locked, then permanently lock accounts after two consecutive lockouts.

Question 2

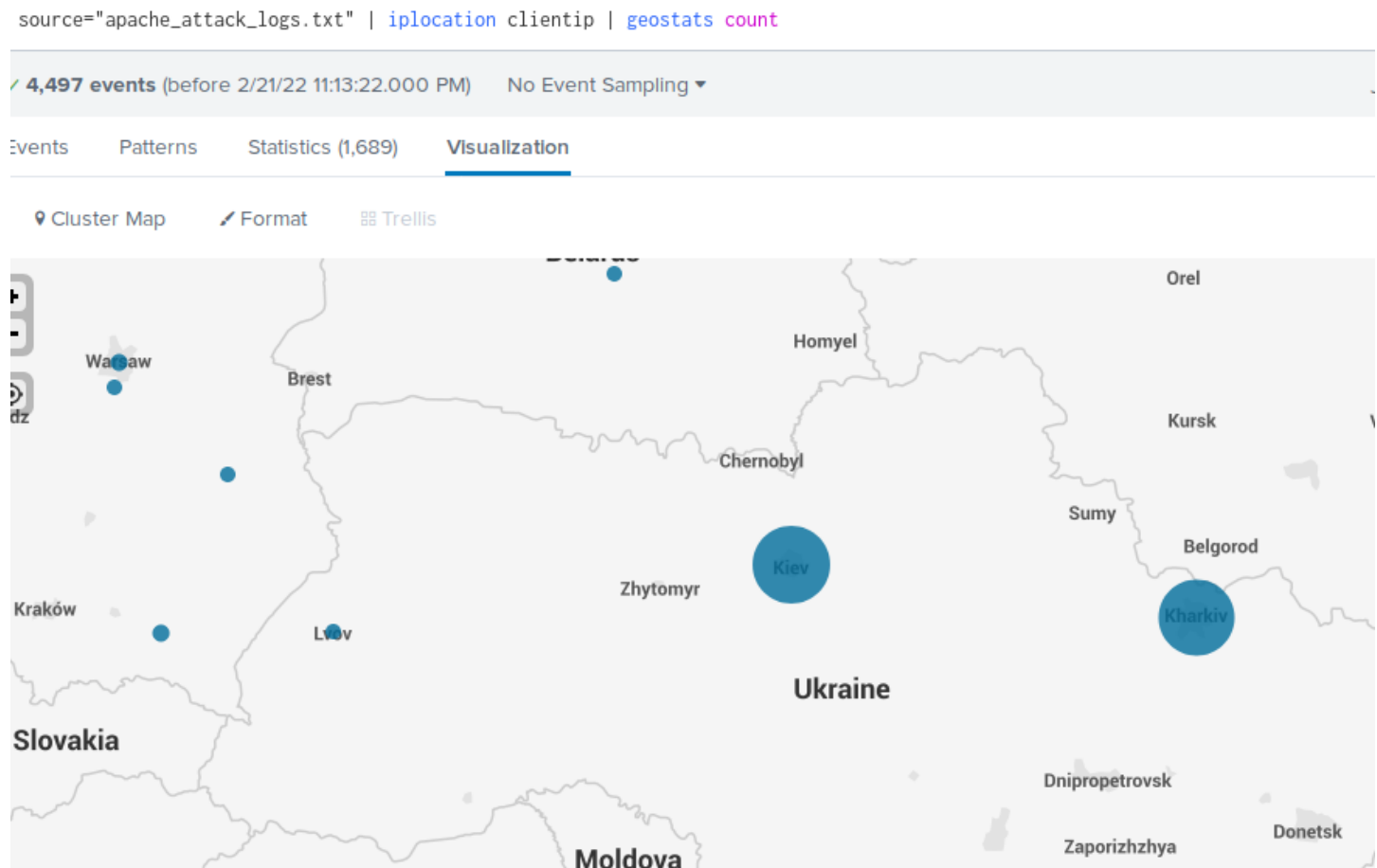
VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user. What sort of mitigation could you use to protect against this?

- Mitigation recommendations:
 - Most likely these bad logins were sent from a given IP or set of IPs. In this case you could blacklist any IP that has consecutive "bad login" requests.

Part 2: Apache Webserver Attack

Question 1

Here's the map that I used for the following recommendations:



And here's the counts for the above map that helped me decide Ukraine was the country to focus on:

source="apache_attack_logs.txt" iplocation clientip stats count by Country		All time	
✓ 4,497 events (before 2/21/22 11:18:38.000 PM) No Event Sampling		Job ▾ ▢ ↗ 📄 ⬇ ⚡ Fast Mode ▾	
Events	Patterns	Statistics (60)	Visualization
100 Per Page ▾ ↗ Format Preview ▾			
Country ↕			count ▾ ↗
United States			2027
Ukraine			877
France			195

I would use a rule that does the following: blocks all HTTP traffic that comes from the cities of Kiev and Kharkiv, Ukraine.

Question 2

Here's the data I used in order to make the firewall rule recommendations:

source="apache_attack_logs.txt" host="5bc0a33fe760" sourcetype="access_combined" stats count by uri		All time	
✓ 4,497 events (before 2/21/22 11:24:21.000 PM) No Event Sampling		Job ▾ ▢ ↗ 📄 ⬇ ⚡ Smart Mode ▾	
Events	Patterns	Statistics (613)	Visualization
100 Per Page ▾ ↗ Format Preview ▾		< Prev 1 2 3 4 5 6 7 Next >	
uri ↕			count ▾ ↗
/VSI_Account_logon.php			1323
/files/logstash/logstash-1.3.2-monolithic.jar			638

source="apache_attack_logs.txt" host="5bc0a33fe760" sourcetype="access_combined" stats count by useragent		All time	
✓ 4,497 events (before 2/21/22 11:27:38.000 PM) No Event Sampling		Job ▾ ▢ ↗ 📄 ⬇ ⚡ Smart Mode ▾	
Events	Patterns	Statistics (209)	Visualization
100 Per Page ▾ ↗ Format Preview ▾		< Prev 1 2 3 Next >	
useragent ↕			count ▾ ↗
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)			1296
Chef Client/10.18.2 (ruby-1.9.3-p327; ohai-6.16.0; x86_64-linux; +http://opscode.com)			638
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/32.0.1700.107 Safari/537.36			291

The "URL" and "user agent" fields contained the most common values during the time of the attack. So, we can generate firewall rules based on those values. Also, we'll need to create stateful firewall rules that are based on the number of consecutive POST requests.

- Blacklist IPs that have sent a given number of POST requests – the specific number will need to be decided based on testing in order to not filter legitimate traffic – and the URL or URL path is "/VSI_Account_logon.php".
- Blacklist IPs that have sent a given number of POST requests – the specific number will need to be decided based on testing in order to not filter legitimate traffic – and the user agent is the one listed at the top of the table in the second screen shot.