Report Analysis for Severity:

* Yes, I did detect some suspicious changes in severity. The percentages changed from (about)
  + High: 6% to 20%
  + Informational: 93% to 80%

Report Analysis for Failed Activities:

* No, I did not detect suspicious changes in failed activities. The percentages stayed close and went from (about)
  + Success: 97% to 98%
  + Failed: 3% to 1.55%

Alert Analysis for Failed Windows Security:

* On Wednesday 3/25/2020 at about 8 AM, there were 35 events that were logged - far more than any other time on that day.
* My alert would have been triggered (my alert was set to be triggered if the count was over 22).
* I would not change this after reviewing the data.

Alert Analysis for Successful Logins:

* On Wednesday 3/25/2020 at about 11 AM and then again at about 12 PM, there were an abnormally high number of successful logins.
* At 11 AM, the count of successful logins was 196. At 12 PM, the count of successful logins was 77.
* The primary user logging on was user \_j with a count of 196 and 302.
* My alert would have been triggered because it was set to Results > 30.
* After reviewing the data, I would increase the triggered value from 30 to 60.

Alert Analysis for Deleted Accounts

* The only odd thing that I found was that there were consistently accounts deleted from 12 AM to 9 AM, and then none deleted at 10 AM, before going back up in number of accounts deleted.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dashboard Analysis for Time Chart of Signatures:

* The following Signatures had suspicious activity:
  + A user account was locked out: 3/25/2020 approximate time frame 1 AM - 3 AM; peak count 896.
  + An attempt was made to reset a user’s password: 3/25/2020 approximate time frame 9 AM - 11 AM; peak count 1258.
  + An account was successfully logged on: 3/25/2020 approximate time frame 11 AM - 1 PM; peak count 196.

Dashboard Analysis for Users

* Yes. users \_a and \_k have extremely suspicious behavior and user \_j has slightly suspicious activity.
  + User \_a: 3/25/2020 approximate time frame 1 AM - 3 AM; peak count 985.
  + User \_j: 3/25/2020 approximate time frame 11 AM - 1 PM; peak count 196.
  + User \_k: 3/25/2020 approximate time frame 9 AM to 11 AM; peak count 1256.

Dashboard Analysis for Signatures with Bar, Graph, Pie Charts:

* The pie chart does match with the 1hr Count by Signature Table; no new suspicions.

Dashboard Analysis for Users with Bar, Graph, Pie Charts:

* The pie chart does match with the 1hr Count by User Table; no new suspicions.

Dashboard Analysis for Users with the Statistical Chart:

* Statistical charts may be harder for some people to understand due to it being harder to visualize numbers whereas the visualizations provide colored and shaped comparisons, allowing anomalies to stand out more.
* Statistical charts can be more useful, though, when one wants to look at full data sets as opposed to time framed data sets.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Report Analysis for Methods:

* The HTTPS POST method showed suspicious change; the percentage went from about 1% to about 29%.
* The POST method is used to send data to a server to create or update a resource.

Report Analysis for Referrer Domains:

* It does not appear that there were any significant changes in the data that would raise suspicion.

Report Analysis for HTTP Response Codes:

* The most prominent change in the data is the 404 Response Code, which went from about 2% to slightly over 15%.

Alert Analysis for International Activity:

* Yes. On 3/25/2020 at about 8 PM, there was a surge of counts equalling 935.
* My alert would have been triggered by this event as my alert was set for counts over 120.
* I would not change my alert threshold.

Alert Analysis for HTTP POST Activity:

* Yes. On 3/25/2020 at about 8 PM there was a count of 1296.
* I would not change my alert threshold.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dashboard Analysis for Time Chart of HTTP Methods:

* This chart showed suspicious activity in the following:
  + POST Method: 3/25/2020 from about 8 PM - 9 PM with a peak count of 1296.
  + GET Method: 3/25/2020 from about 6 PM to 7 PM with a peak count of 729.

Dashboard Analysis for Cluster Map:

* Ukraine has the largest volume of activity; Kiev has a count of 439 and Kharkiv has a count of 433.

Dashboard Analysis for URI Data:

* Yes, the count for /VSI\_Account\_logon.php has a suspiciously high number of counts.
* Based on the URI being accessed and the immense number of attempts, the attacker(s) may be trying to use a Brute Force Attack utilizing the VSI logon page.

### **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.
  + User \_A (A user account was locked out): recommended mitigation includes creating a complex password that contains at least one number, at least one special character, and at least 10 letters. The attacker(s) is utilizing Brute Force to attempt a way into User \_A’s account, and creating a more complex password makes that extremely more time consuming and difficult which in turn may dissuade the attacker(s) from continuing attempts.
  + User \_J (An account was successfully logged on): recommended mitigation includes the same password change and guidelines as outlined for User \_A, because the attacker(s) successfully achieved User\_J’s password.
  + User \_K (An attempt was made to reset an account password): recommended mitigation includes implementing multi-factor authentication when a user requests a password reset; utilize CAPTCHAs (completely automated public turing test to tell computers and humans apart). “Essentially, CAPTCHAs are challenges that are difficult for automated computer programs to perform but are easy for humans, such as spotting patterns or clicking in a specific area on a webpage” (https://www.itsasap.com/blog/how-to-prevent-brute-force-attacks).
  + GLOBAL MITIGATION STRATEGIES: include implementing multi-factor authentication company-wide in order to increase the difficulty level and work required for an attacker(s) to gain access into a user account. In addition, a company-wide alert can be made to monitor IP addresses and limit login attempts “to users coming from a specified IP address or range… set up alerts whenever you encounter login attempts from anomalous IP addresses and make sure to block them” (https://www.itsasap.com/blog/how-to-prevent-brute-force-attacks).

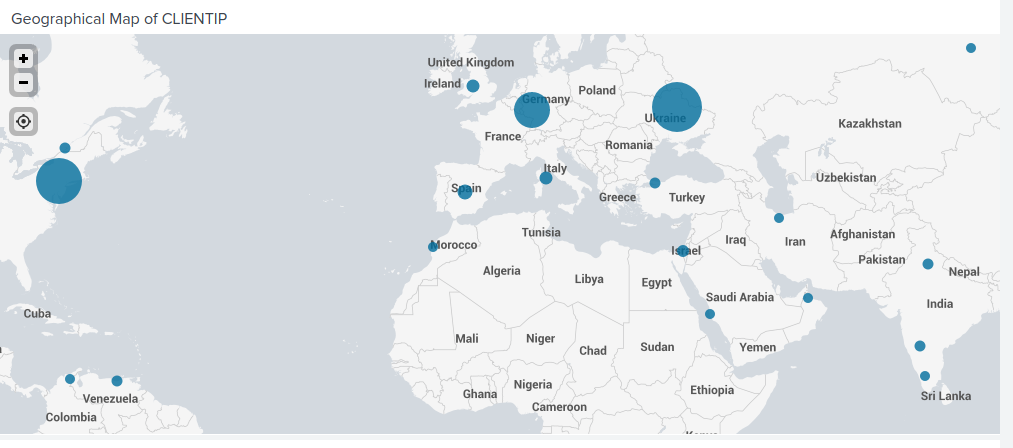
#### **Question 2**

* 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 mitigation strategies from Part 1 would assist in protecting against this attack by JobeCorp; in addition, monitoring server logs as well as locking accounts with longer wait times after each unsuccessful login would prevent ease of attacks. It should be noted that one of the most successful ways to prevent attacks is education; creating succinct, informational mandatory trainings for employees on what different cyber attacks look like as well as explaining why certain requirements are in place (ie password length and character requirements, multi-factor authentication, etc) may help with the prevention of attacks.

### **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; Provide a screenshot of the geographic map that justifies why you created this rule.
  + Block all incoming HTTP traffic where the source IP comes from the country of Ukraine.
  + Outside of the United States, a huge number of source IP addresses can be found originating in the Ukraine; unless VSI has a large number of employees in that country, which at this point they do not, then the chance of these being related to attacks are high and therefore should be blocked out of precaution and prevention.



#### **Question 2**

* VSI has insider information that JobeCorp will launch the same web server 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?
  + Because the HTTP POST Method usage jumped from about 1% to about 29% during the attack on 3/25/22, the following rule can be implemented: block IP addresses which provide 5 or more HTTP POST requests to the VSI login page in a 60 second time frame or, similarly, create an alert when the POST method is above 5%. This will allow us to investigate and stop current attacks from continuing.
  + The following useragent identification was found multiple times during the attack:
    - Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; INFOPATH.1)
    - This useragent identification should be blocked.

Resources:

Descalso, Alessandra. “How to Prevent Brute Force Attacks in 8 Easy Steps [Updated].” *Intelligent Technical Solutions*, 11 Jan. 2022, https://www.itsasap.com/blog/how-to-prevent-brute-force-attacks.

GITHUB Student Activities/Student Guide