## **Activity File: Part 1 - Master of the SOC**

* Each group is playing the role of an SOC analyst at a small company called Virtual Space Industries (VSI), which designs virtual reality programs for businesses.
* VSI has heard rumors that a competitor, JobeCorp, may be launching cyberattacks to disrupt VSI's business.
* As SOC analysts, you are tasked with using Splunk to monitor against potential attacks on your systems and applications.
* Your Networking team has provided you with past logs to help you develop baselines and create reports, alerts, and dashboards.

You've been provided the following logs:

* Windows Server Logs  
  + This server contains intellectual property of VSI's next-generation virtual reality programs.
* Apache Server Logs  
  + This server is used for VSI's main public-facing website vsi-company.com.

### **Windows Server Logs Instructions and Deliverables**

1. Load the logs into your Splunk environment.  
   * Select all default options provided.
   * **Important:** For the time range, select **All Time**.
2. Analyze the logs and the available fields.
3. Design the following deliverables to protect VSI from potential attacks by JobeCorp.  
   * **Reports**: Design the following reports to assist VSI with quickly identifying specific information.  
     1. A report with a table of signatures and associated SignatureID.  
        + This will allow VSI to easily view reports that show the ID number with a specific signature of the Windows activity.  
            
           **Hint:** Research how to remove the duplicate values in your SPL search.
     2. A report that provides the count and percent of the severity.  
        + This will allow VSI to quickly know the severity levels of the Windows logs being viewed.
     3. A report that provides a comparison between the success and failure of Windows activities.  
        + This will show VSI if there is a suspicious level of failed activities on their server.  
            
           **Hint:** Check the status field for this information.
   * **Alerts**: Design the following alerts to notify VSI of suspicious activity:  
     1. Determine a baseline and threshold for hourly level of failed Windows activity.  
        + Create an alert to trigger when the threshold has been reached.
        + The alert should trigger an email to SOC@VSI-company.com.
     2. Determine a baseline and threshold for hourly count of the signature: **an account was successfully logged on**.  
        + Create an alert to trigger when the threshold has been reached.
        + The alert should trigger an email to SOC@VSI-company.com.
     3. Determine a baseline and threshold for hourly count of the signature: **a user account was deleted**.  
        + Design the alert based on the corresponding SignatureID, as the signature name sometimes changes when the Windows system updates.
        + Create an alert to trigger when the threshold has been reached.
        + The alert should trigger an email to SOC@VSI-company.com.
   * **Visualizations and Dashboards**: Design the following visualizations and add them to a dashboard called Windows Server Monitoring:  
     1. A line chart that displays the different signature field values over time.  
        + **Hint:** Add the following after your search: timechart span=1h count by signature
     2. A line chart that displays the different user field values over time.
     3. A bar, column, or pie chart that illustrates the count of different signatures.
     4. A bar, column, or pie chart that illustrates the count of different users.
     5. A statistical chart that illustrates the count of different users.
     6. One single value visualization of your choice: radial gauge, marker gauge, etc.
4. On your dashboard, add the ability to change the time range for all your visualizations.  
   * Be sure to title all your panels appropriately.
   * Align your dashboard panels as you see fit.

### **Apache Web Server Instructions and Deliverables**

1. Load the logs into your Splunk environment.  
   * Select all default options provided.
   * **Important:** For the time range, select **All Time**.
2. Analyze the logs and the available fields.
3. Design the following deliverables to protect VSI from potential attacks by JobeCorp:  
   * **Reports**: Design the following reports to assist VSI with quickly identifying specific information:  
     1. A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc).  
        + This will provide insight into the type of HTTP activity being requested against their web server.
     2. A report that shows the top 10 domains that referred to VSI's website.  
        + This will assist VSI with identifying suspicious referrers.
     3. A report that shows the count of the HTTP response codes.  
        + This will provide insight into any suspicious levels of HTTP responses.
   * **Alerts**: Design the following alerts:  
     1. Determine a baseline and threshold for hourly activity from a country other than the United States.  
        + Create an alert to trigger when the threshold has been reached.
        + The alert should trigger an email to SOC@VSI-company.com.
     2. Determine an appropriate baseline and threshold for hourly count of the HTTP POST method.  
        + Create an alert to trigger when the threshold has been reached.
        + The alert should trigger an email to SOC@VSI-company.com.
   * **Visualizations and Dashboards**: Design the following visualizations and add them to a dashboard called Apache WebServer Monitoring.  
     1. A line chart that displays the different HTTP methods field over time.  
        + **Hint:** Add the following after your search: timechart span=1h count by method.
     2. A geographical map showing the location based on the clientip field.
     3. A bar, column, or pie chart that displays the number of different URIs.
     4. A bar, column, or pie chart that displays the counts of the top 10 countries.
     5. A statistical chart that illustrates the count of different user agents.
     6. One single value visualization of your choice: radial gauge, marker gauge, etc.
4. On your dashboard, add the ability to change the time range for all your visualizations:  
   * Be sure to title all your panels appropriately.
   * Align your dashboard panels as you see fit.