Splunk 1: Protecting VSI (Baselines, Alerts, Dashboards, and Queries)

Scenario

Virtual Space Industries (VSI) is a company which designs virtual reality programs for business. 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 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.

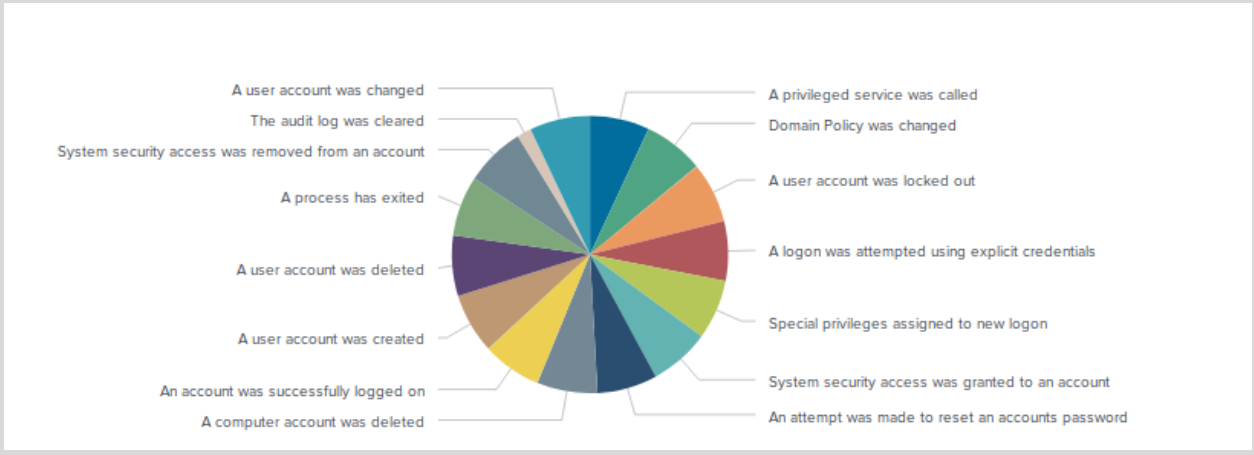
You've been provided the following logs:

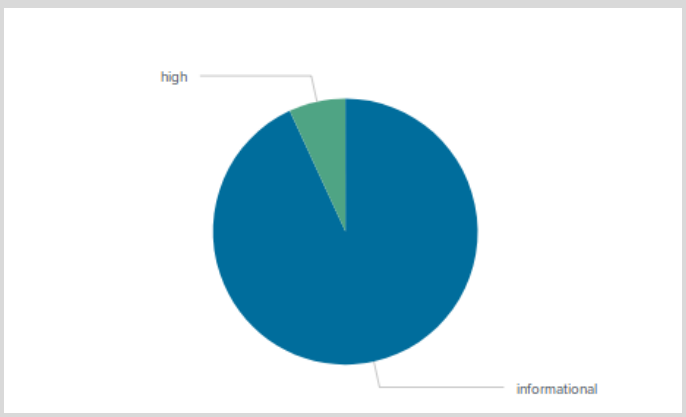
- **Windows Server Logs:** This server contains intellectual property of VSI's next-generation virtual reality programs.
- **Apache Server Logs:** This server is used for VSI's main public-facing website vsi-company.com.

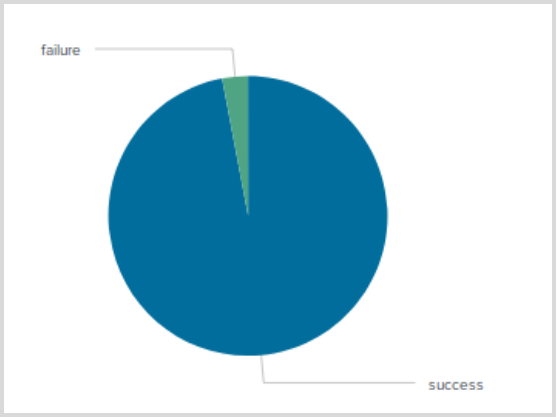
Windows Server Logs

Reports:

1. A report with a table of signatures and associated SignatureID.
   source="windows_server_logs.csv" | table signature signature_id signature | dedup signature_id signature
2. A report that provides the count and percent of the severity.
   source="windows_server_logs.csv" | top severity
3. A report that provides a comparison between the success and failure of Windows activities.
   source="windows_server_logs.csv" | top status



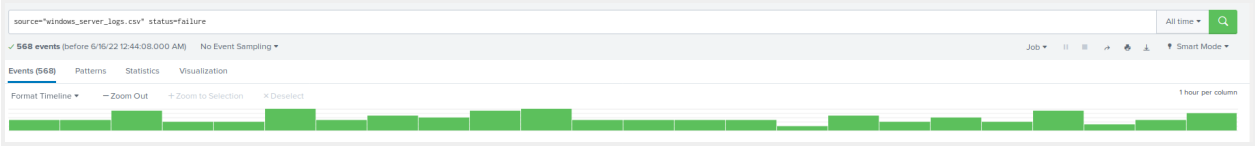




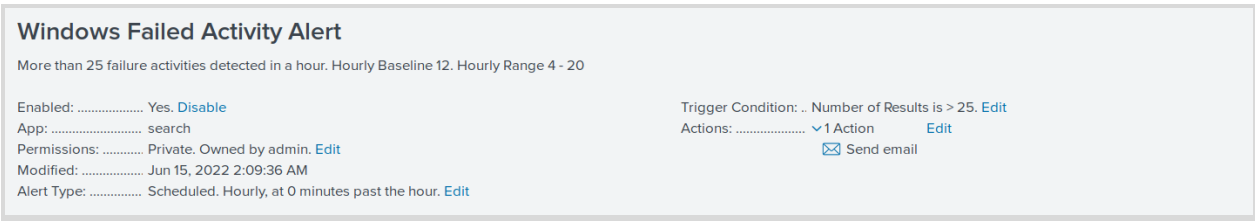
Alerts:

Failed Windows activity Alert

source="windows_server_logs.csv" status=failure

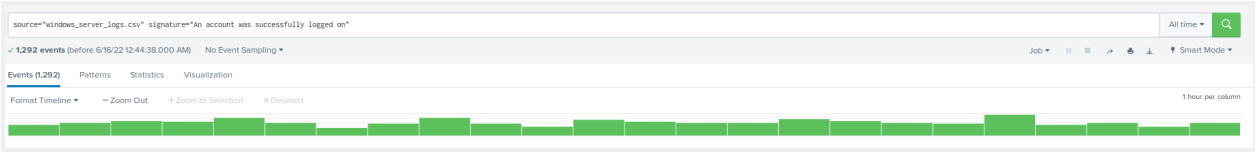


Range 4 - 20
Baseline 12
Threshold 25

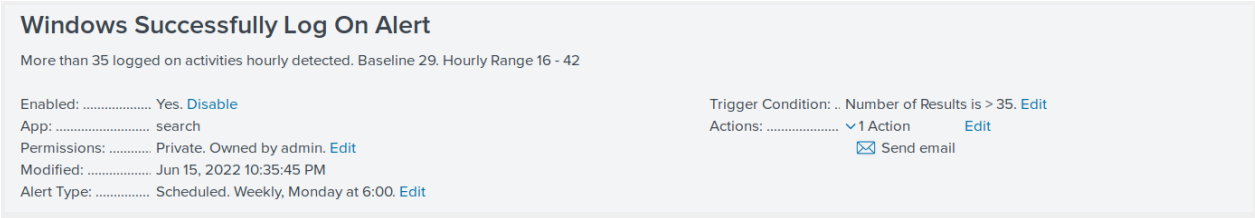


Successfully logged on account alert

source="windows_server_logs.csv" signature="An account was successfully logged on"

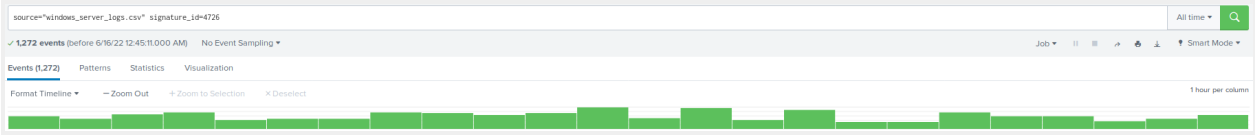


Range 16 - 42
Baseline 29
Threshold 35



User account deleted alert

source="windows_server_logs.csv" signature_id=4726



Range 14 - 44
Baseline 29
Threshold 35

Windows Account Deleted Alert

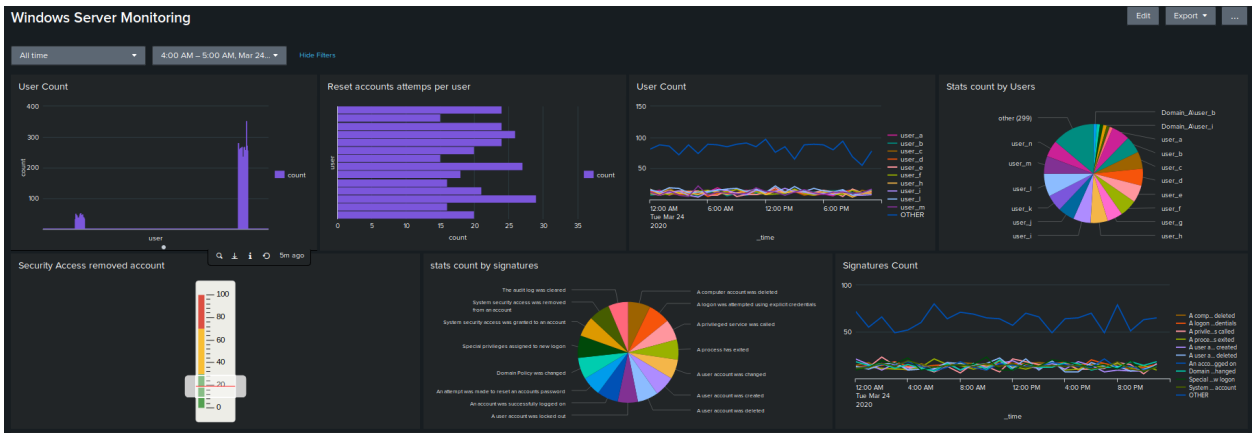
More than 35 deleted accounts hourly detected. Baseline 29. Hourly Range 14 - 44

Enabled: ..... Yes. Disable
App: ..... search
Permissions: ..... Private. Owned by admin. Edit
Modified: ..... Jun 15, 2022 10:32:27 PM
Alert Type: ..... Scheduled. Hourly, at 0 minutes past the hour. Edit

Trigger Condition: .. Number of Results is > 35. Edit
Actions: ..... 1 Action Edit
Send email

Visualizations and Dashboards:

1. A line chart that displays the different signature field values over time.
   source="windows_server_logs.csv" | timechart span=1h count by signature
2. A line chart that displays the different user field values over time.
   source="windows_server_logs.csv" | timechart span=1h count by user
3. A bar, column, or pie chart that illustrates the count of different signatures.
   source="windows_server_logs.csv" | stats count by signature
4. A bar, column, or pie chart that illustrates the count of different users.
   source="windows_server_logs.csv" | stats count by user
5. A statistical chart that illustrates the count of different users.
   source="windows_server_logs.csv" | stats count by user
6. radial gauge **source="windows_server_logs.csv" signature="System security access was removed from an account" | stats count**
7. Additionally **source="windows_server_logs.csv" signature="An attempt was made to reset an accounts password" | stats count by user**
8. Additionally **source="windows_server_logs.csv" | stats count by signature | eventstats sum(count) as total | eval % = round(count/total*100) | fields - total**
9. **Adding features to the Dashboard:** adding the ability to change the time range for all visualizations.



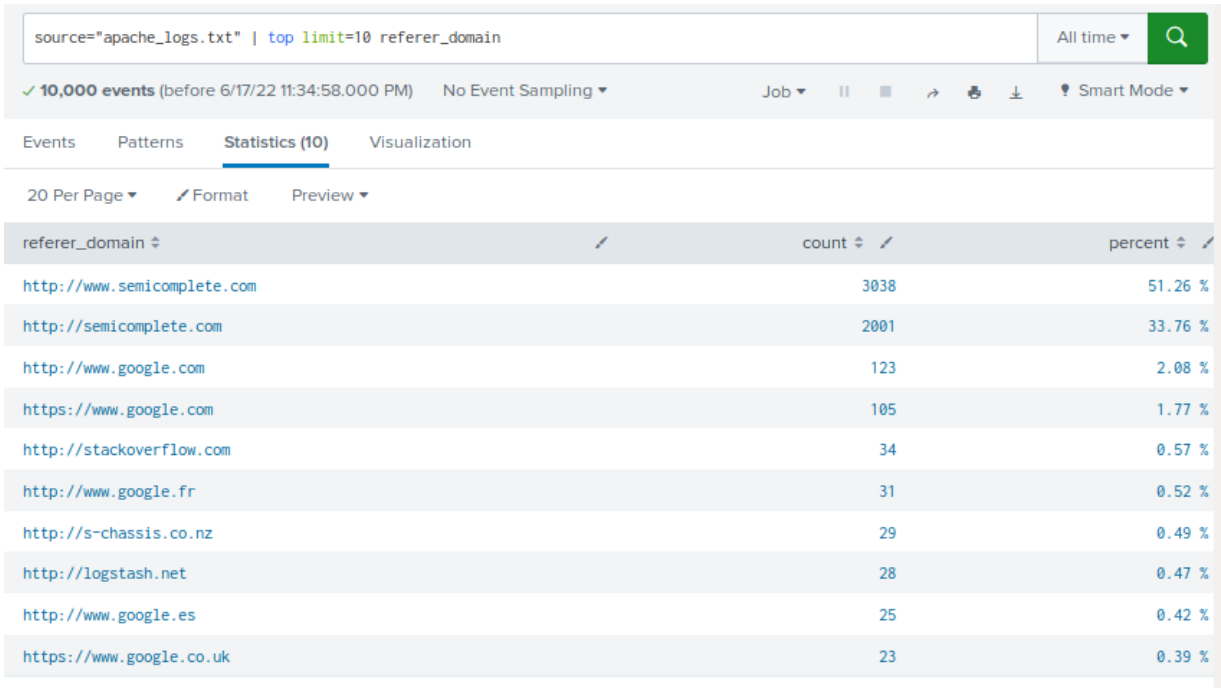
Signature percents from total Signatures

signature	count	%
A computer account was deleted	340	7.00 %
A logon was attempted using explicit credentials	337	7.00 %
A privileged service was called	317	7.00 %
A user account was created	313	7.00 %
A user account was deleted	318	7.00 %
An account was successfully logged on	323	7.00 %
Domain Policy was changed	329	7.00 %
Special privileges assigned to new logon	342	7.00 %
System security access was removed from an account	321	7.00 %
A process has exited	309	6.00 %
A user account was changed	299	6.00 %
A user account was locked out	309	6.00 %
An attempt was made to reset an accounts password	295	6.00 %
System security access was granted to an account	309	6.00 %
The audit log was cleared	303	6.00 %

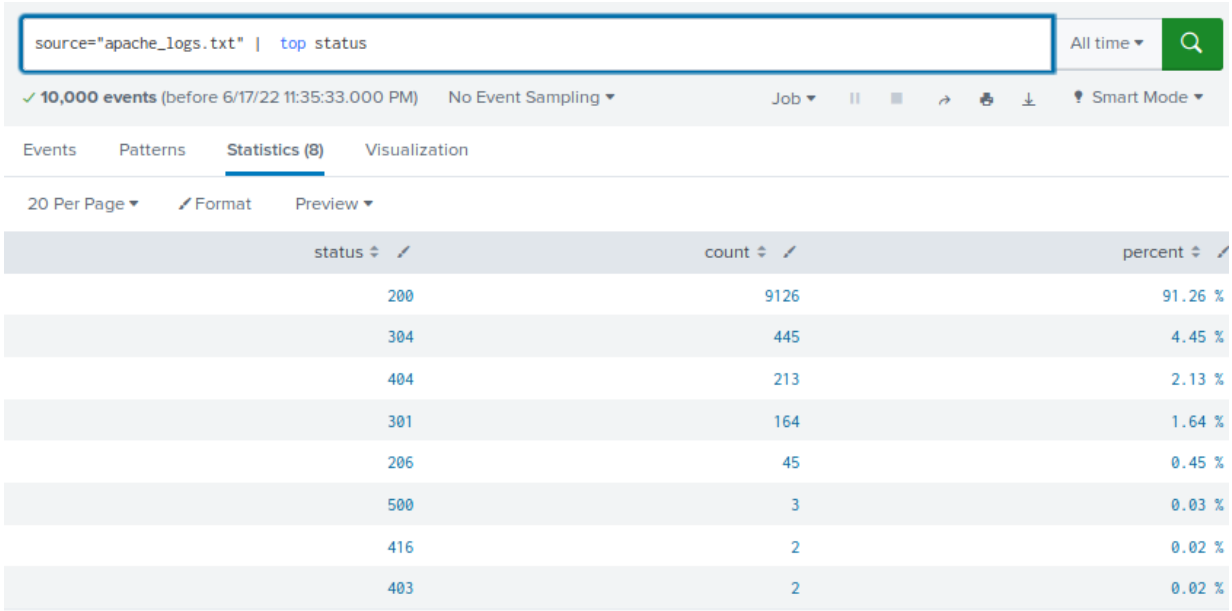
Apache Web Server

Reports:

1. A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc).
   source="apache_logs.txt" | top limit=20 method
2. A report that shows the top 10 domains that referred to VSI's website.
   source="apache_logs.txt" | top limit=10 referer_domain
3. A report that shows the count of the HTTP response codes.
   source="apache_logs.txt" | top status



referer_domain	count	percent
http://www.semicomplete.com	3038	51.26 %
http://semicomplete.com	2001	33.76 %
http://www.google.com	123	2.08 %
https://www.google.com	105	1.77 %
http://stackoverflow.com	34	0.57 %
http://www.google.fr	31	0.52 %
http://s-chassis.co.nz	29	0.49 %
http://logstash.net	28	0.47 %
http://www.google.es	25	0.42 %
https://www.google.co.uk	23	0.39 %

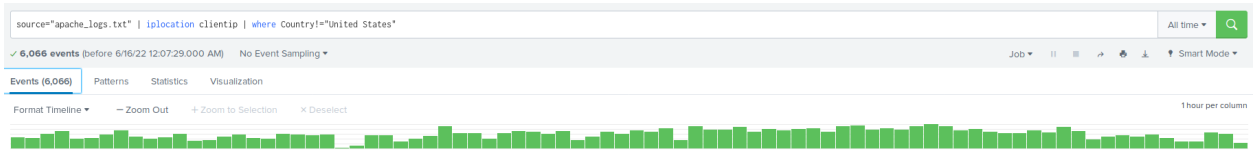


status	count	percent
200	9126	91.26 %
304	445	4.45 %
404	213	2.13 %
301	164	1.64 %
206	45	0.45 %
500	3	0.03 %
416	2	0.02 %
403	2	0.02 %

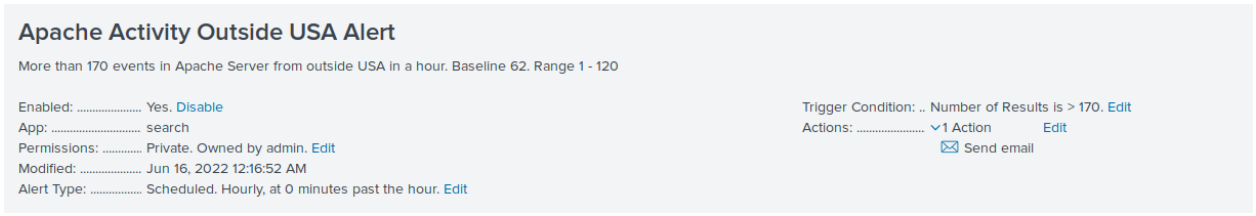
Alerts:

International Activity Alert

source="apache_logs.txt" | iplocation clientip | where Country!="United States"

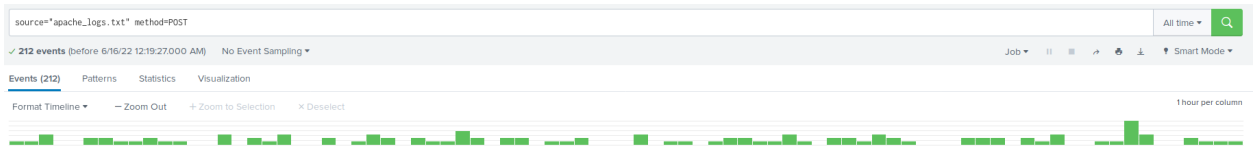


Range 1 - 120
Baseline 62
Threshold 170

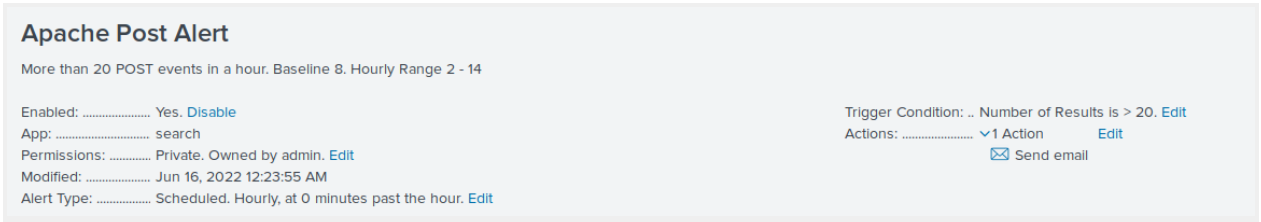


HTTP POST Method Alert

source=”apache_logs.txt” method=POST



Range 2 -14
Baseline 8
Threshold 20



Visualizations and Dashboards:

1. A line chart that displays the different HTTP methods field over time.
   source="apache_logs.txt" | timechart span=1h count by method
2. A geographical map showing the location based on the clientip field.
   source="apache_logs.txt" | iplocation clientip | geostats count
3. A bar, column, or pie chart that displays the number of different URIs.
   source="apache_logs.txt" | top limit=10 uri
4. A bar, column, or pie chart that displays the counts of the top 10 countries.
   source="apache_logs.txt" | iplocation clientip | top limit=10 Country
5. A statistical chart that illustrates the count of different user agents.
   source="apache_logs.txt" | top limit=10 useragent
6. radial gauge
   source="apache_logs.txt" status=404 | stats count as total
7. **Adding features to the Dashboard:** adding the ability to change the time range for all visualizations.