Defensive Security Project
by: Dylan Strube, Alan De Santiago

Table of Contents

This document contains the following resources:

01

Monitoring Environment

02

Attack Analysis

03

Project Summary & Future Mitigations

Monitoring Environment

Scenario

- We are taking the roles of SOC analysts for Virtual Space Industries.
- We were instructed by VSI to use logs to determine user activity baselines, and create alerts to monitor for future incidents.
- VSI hired us to check for vulnerabilities in their system and create a custom security monitoring environment.
- VSI experiences an attack, and our security environment is put to the test.

[“Add-On” App]

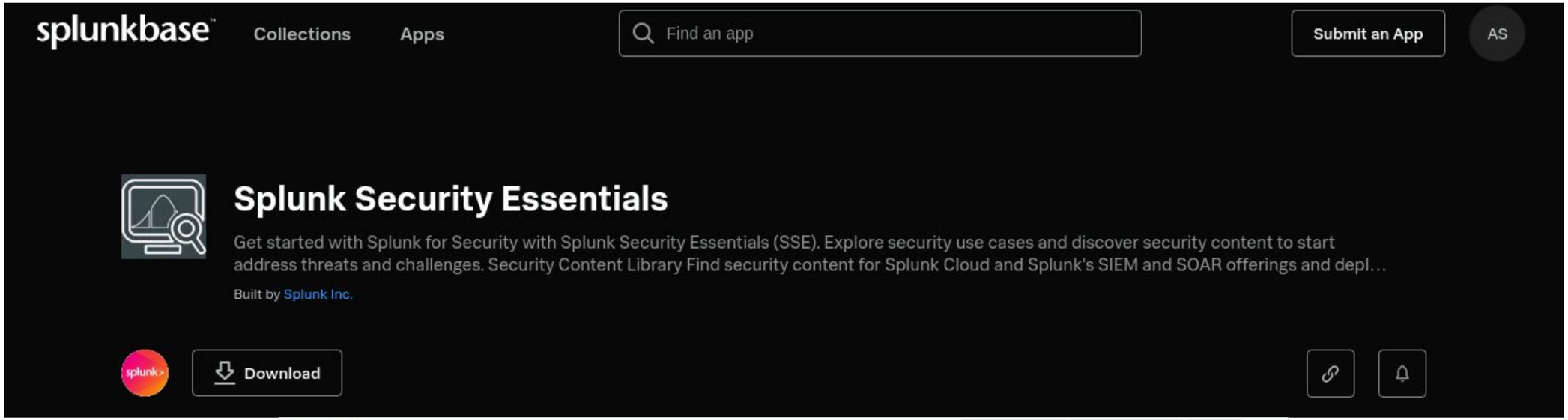
Splunk Security Essentials

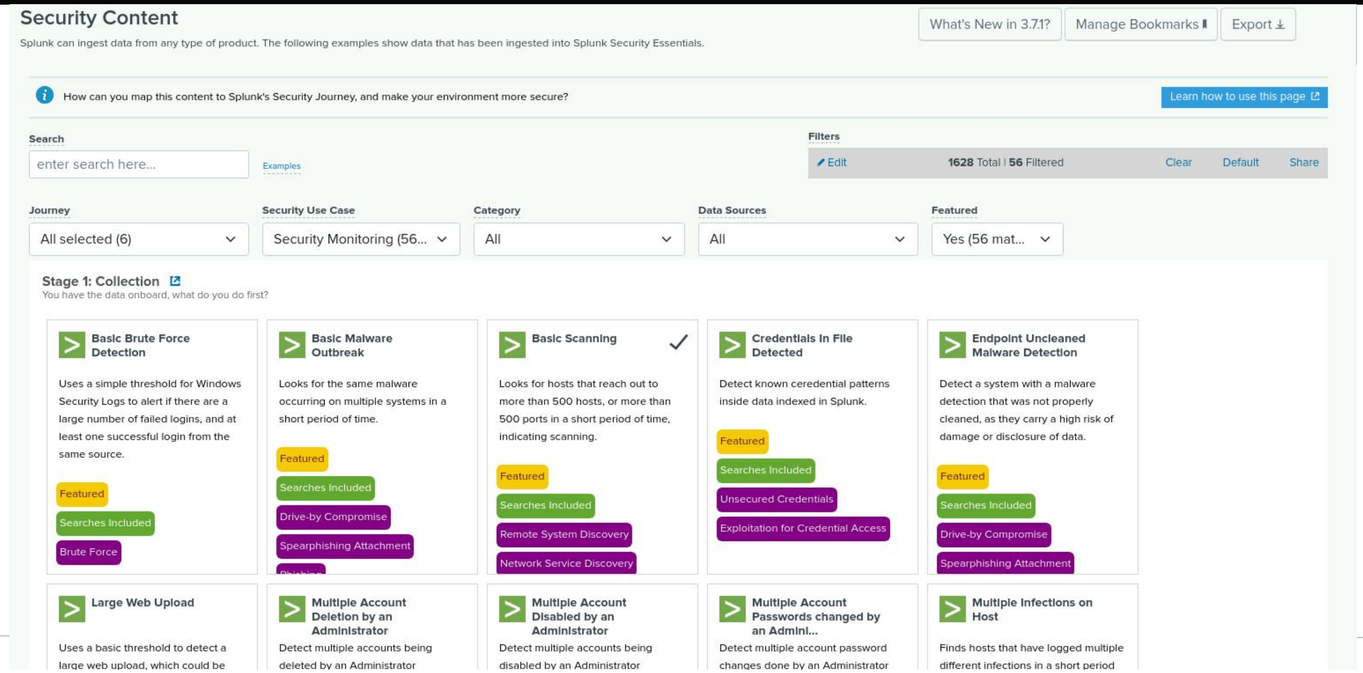
Splunk Security Essentials comes with many pre-built security monitoring and data recommendations.

Splunk Security Essentials

Given that this app provides extensive coverage of the most common threats, it helps to ensure that all SOC analysts are comfortable and competent in dealing with threats. So these pre-built tools are useful because analysts can choose the proper tool in order to deal with security issues at the lowest level.

Splunk Security Essentials





Logs Analyzed

1 Windows Logs

In the first Windows Server Log we discovered, after setting some alerts, that on Thursday, Feb. 20 that between 1-5 pm there was a suspicious volume of failed activity.

2 Apache Logs

The apache logs we examined contained useful information in determining our baselines. It showed a good representation of normal web activity and provided a solid foundation for us to build alerts and reports off of.

Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Event Code Count	Lists the logged events and the number of occurrences.
Severity Count	Displays the severity of logged events and the number of their occurrences.
Success/Failure Rate	Displays the rates of success and failures of Windows events.

Images of Reports—Windows

signature	signature_id
A user account was deleted	4726
A user account was created	4720
A computer account was deleted	4743
An account was successfully logged on	4624
Special privileges assigned to new logon	4672
An attempt was made to reset an accounts password	4724
System security access was granted to an account	4717
A privileged service was called	4673
A logon was attempted using explicit credentials	4648
A user account was locked out	4740
Domain Policy was changed	4739
A user account was changed	4738
A process has exited	4689
The audit log was cleared	1102
System security access was removed from an account	4718

Events (4,764) Patterns **Statistics (2)** Visualization

20 Per Page ▾ Format Preview ▾

severity	count	percent
informational	4435	93.094039
high	329	6.905961

status	count	percent
success	4622	97.019312
failure	142	2.980688

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Excessive Failure Alert	An alert that goes off when the threshold for hourly failures is reached.	6	11

JUSTIFICATION: We first calculated the amount of hourly failures and used that as our baseline. When deciding on a threshold, we wanted to avoid false-positives and opted to use a higher than usual value, 11.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Account Successfully logged on	An alert that goes off when the threshold for logged in accounts is reached.	[12]	[30]

JUSTIFICATION: Calculated the average number of accounts logged on, and then set the threshold to a larger number to avoid triggering the alert constantly.

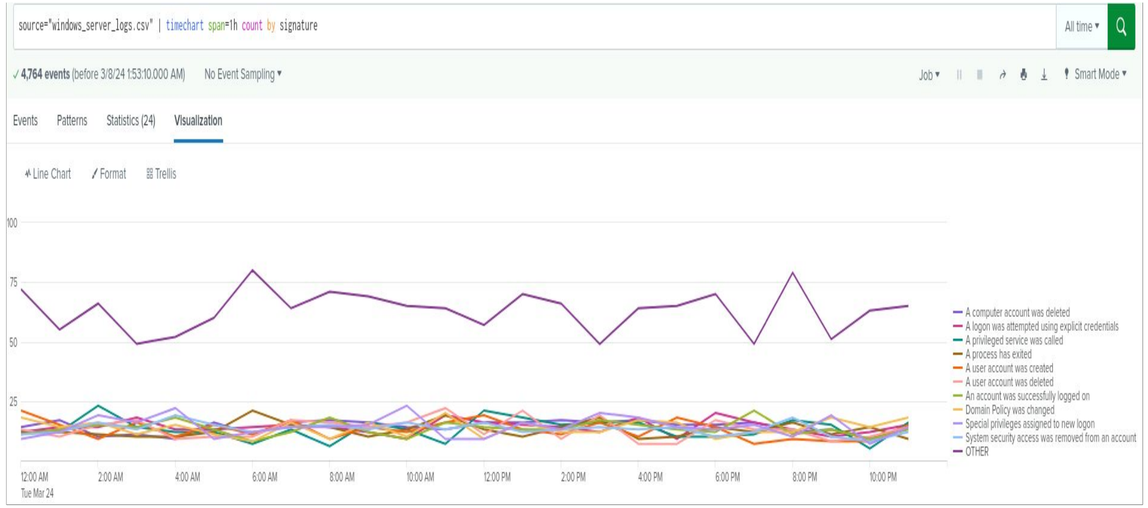
Alerts—Windows

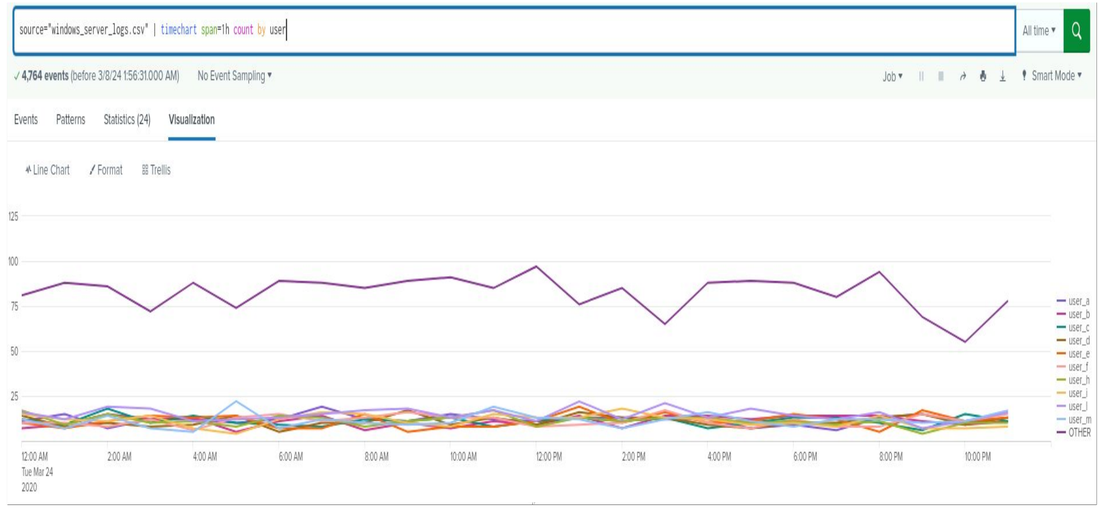
Designed the following alerts:

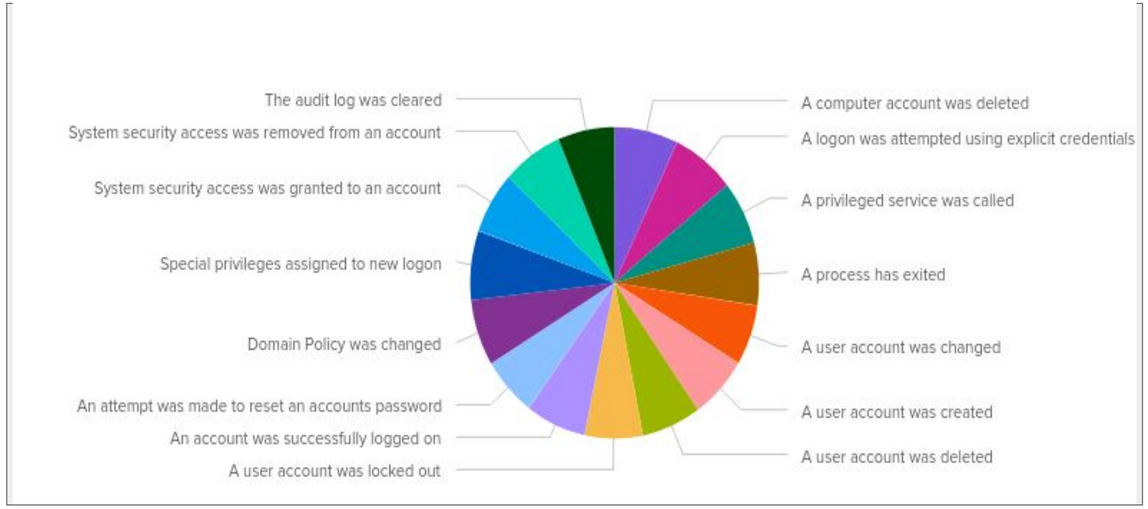
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Account Deletions	An alert that goes off when the threshold reaches	14	22

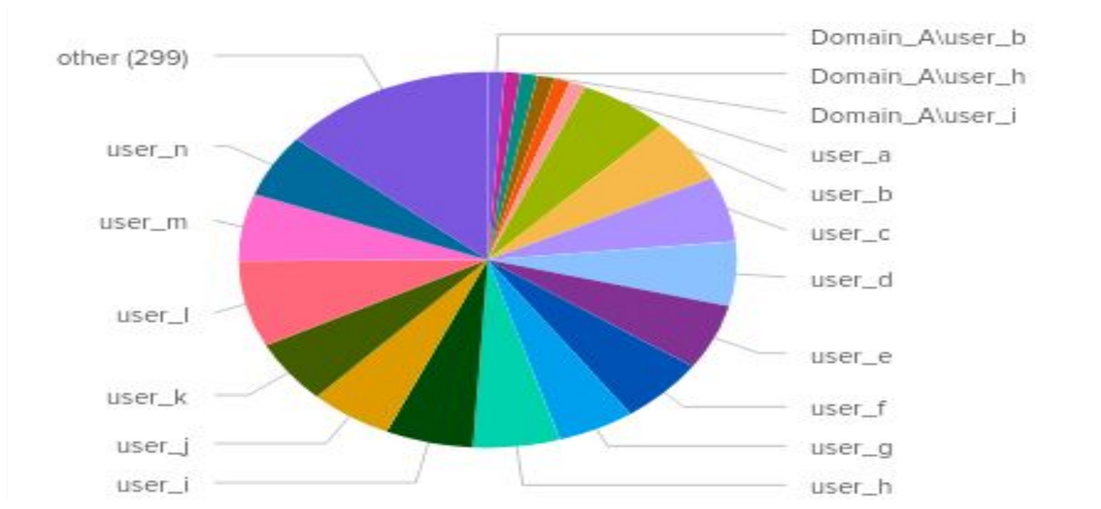
JUSTIFICATION: We first calculated the amount of hourly failures and used that as our baseline. When deciding on a threshold, we wanted to avoid false-positives and opted to use a higher than usual value, 11.

Dashboards—Windows

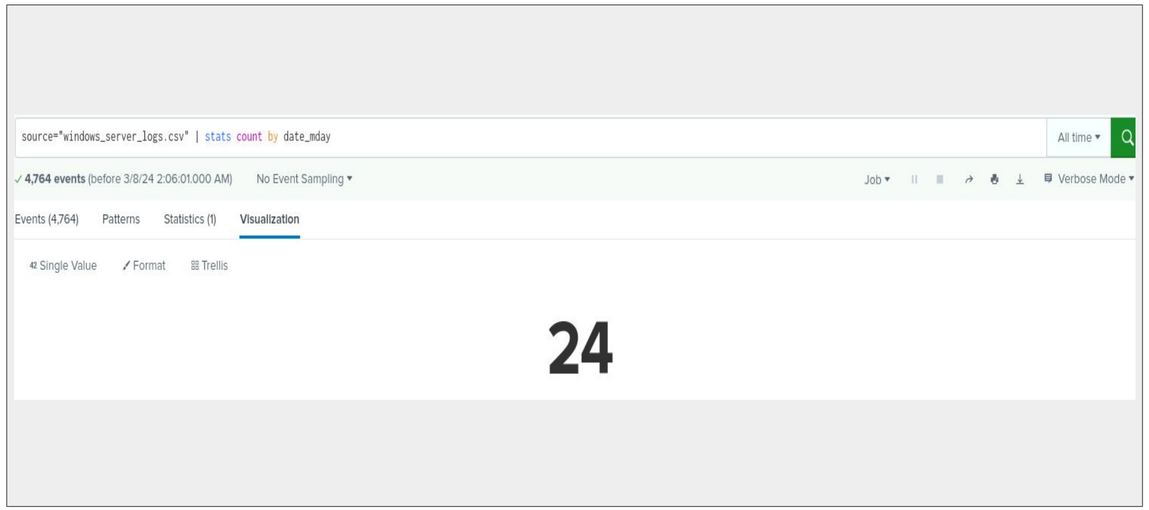








Dashboards—Windows



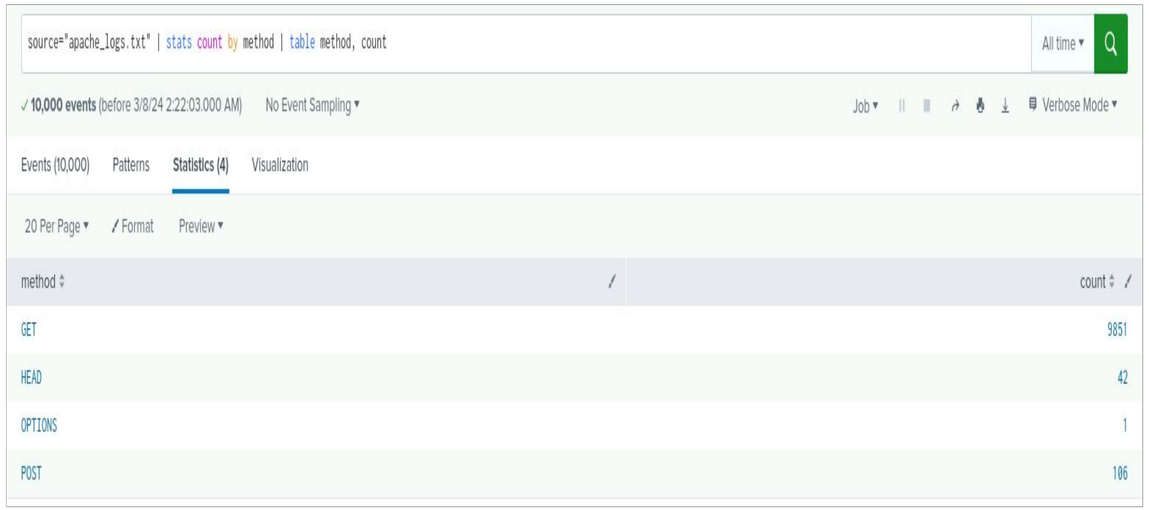
Apache Logs

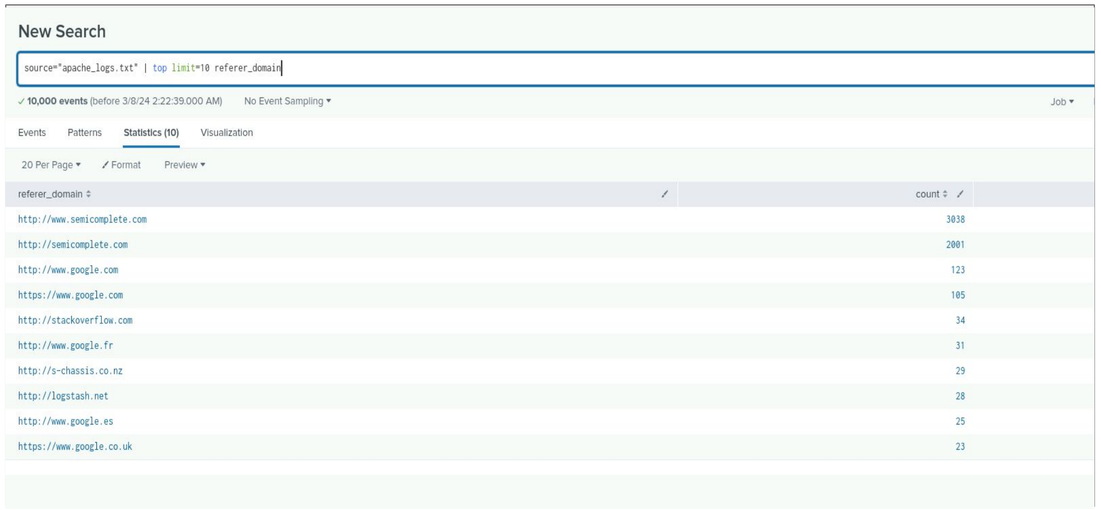
Reports—Apache

Designed the following reports:

Report Name	Report Description
Method Count	This report counts the number of HTTP requests with each method.
Top 10 Domains	This report returns to us a list of the Top 10 domains we are receiving activity from.
Status Report	This report tells us the count of each status code our HTTP requests have.
Traffic Origin	This report shows us a map of where incoming traffic originates from.

Images of Reports—Apache





Report Image

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Foreign Activity	An alert that triggers when foreign traffic exceeds the threshold count.	73	120

JUSTIFICATION: We averaged the count of traffic coming in from outside the US and used that as our baseline. We decided to set our alert threshold to the highest hourly count we observed.

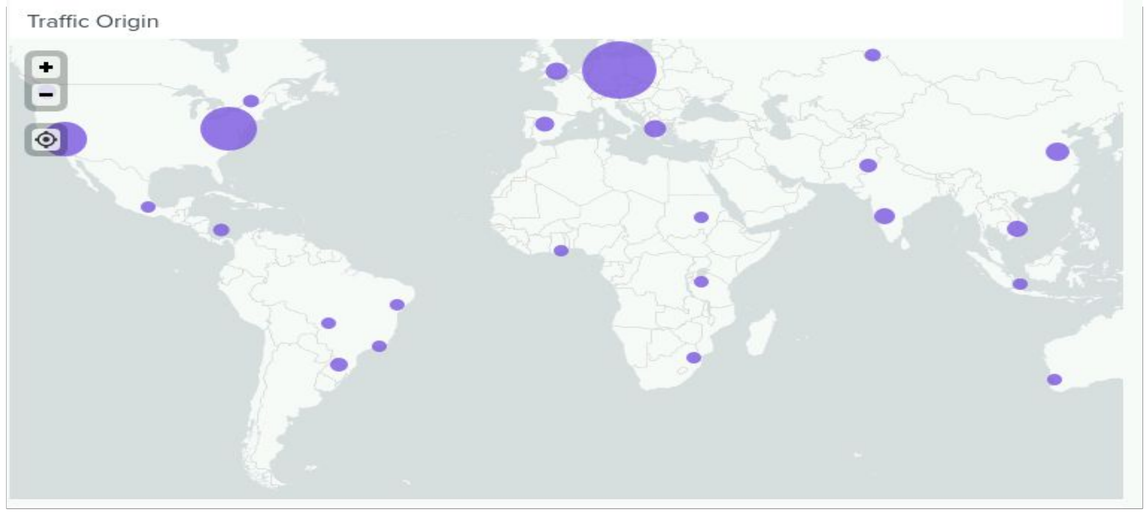
Alerts—Apache

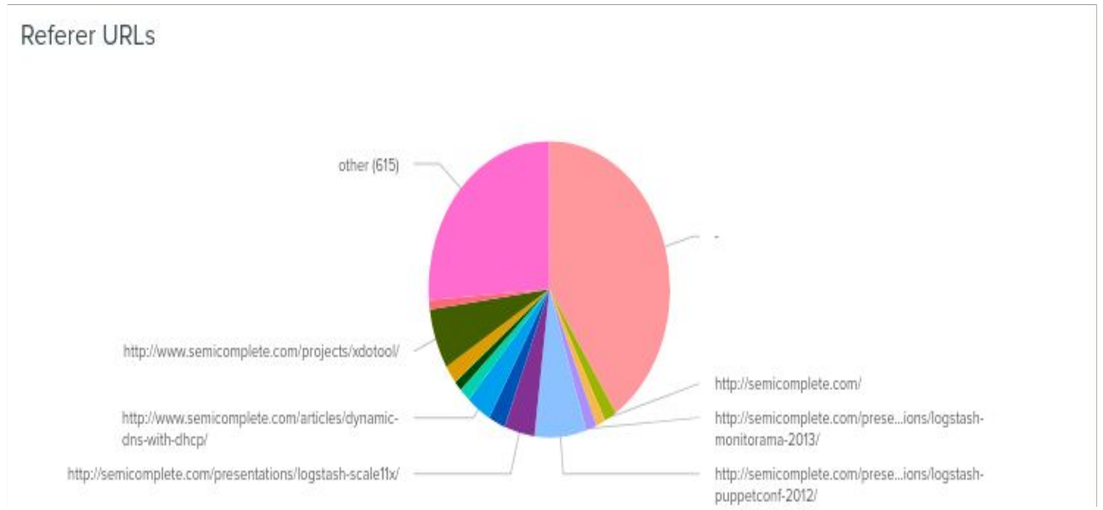
Designed the following alerts:

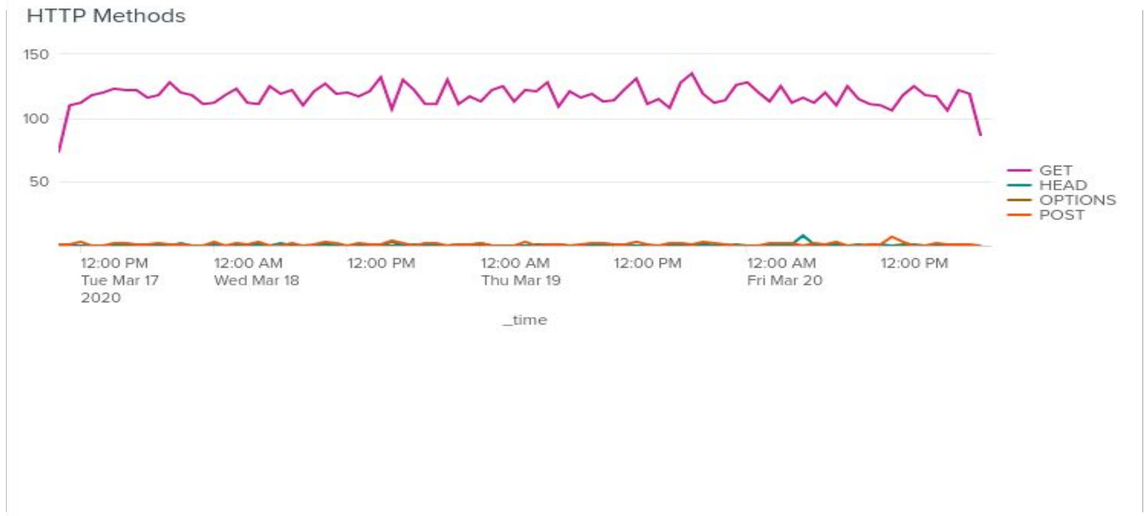
Alert Name	Alert Description	Alert Baseline	Alert Threshold
POST HTTP Request Alert	[An alert that triggers when hourly HTTP requests exceeds the threshold count.	2	8

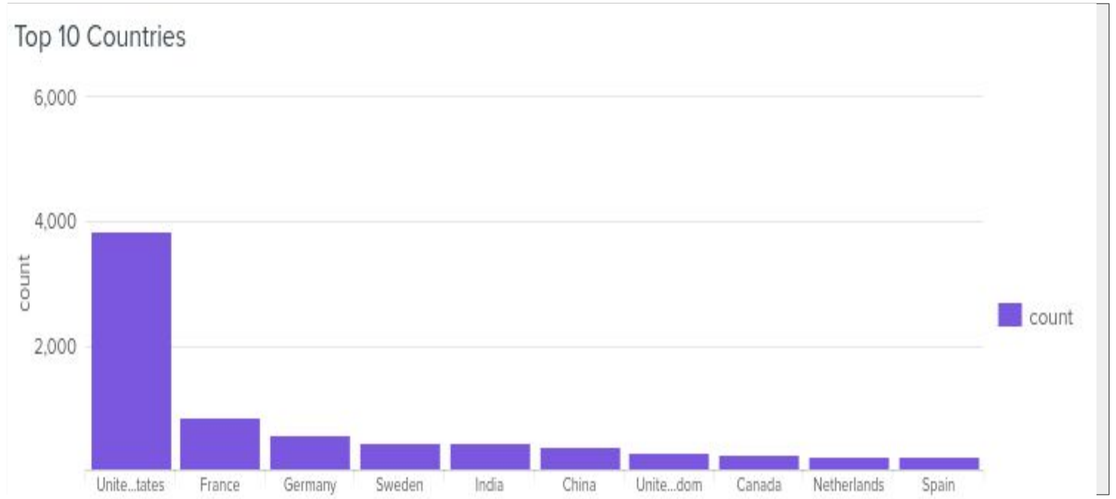
JUSTIFICATION: We averaged the hourly count of HTTP requests to get our baseline and set our threshold above our highest observed count.

Dashboards—Apache







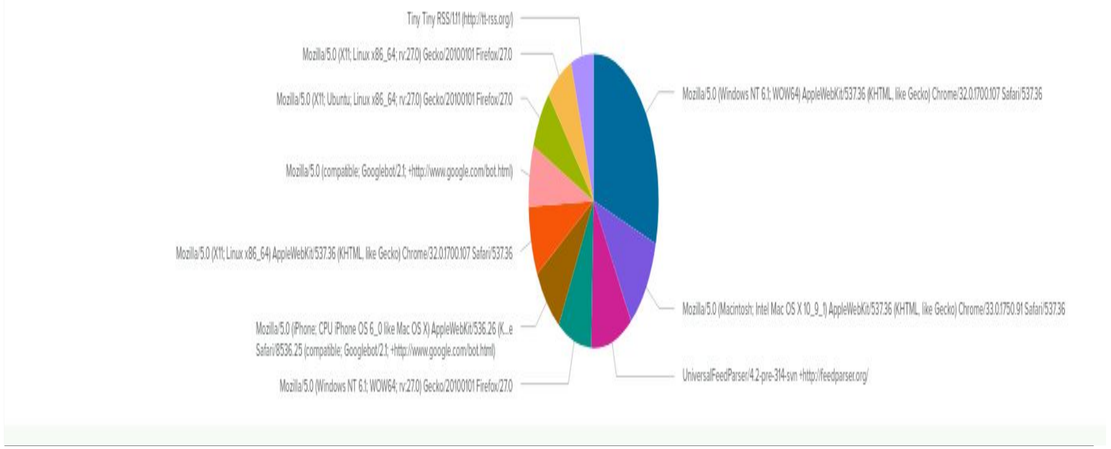


Dashboards—Apache

Today's Date

19

Top 10 User Agents



Place image here

Place image here

Attack Analysis

Attack Summary—Windows

Summarize your findings from your reports when analyzing the attack logs.

- From 1-5 pm there were several Man-in-The-Middle Weakness alerts on the report.
- 2 users were responsible for the activity, user_a and user_k, they had a very high level of activity during certain periods of the day.

```
“A computer account was deleted” 59
“The audit log was cleared” 127
“System security access was granted to an account” 160
“An account was successfully logged on” 91
"An attempt was made to reset an accounts password" 64
“A user account was created” 127
“A user account was changed” 68
“System security access was removed from an account” 75
“An account was successfully logged on” 67
“Special privileges assigned to new logon” 71
“A user account was deleted” 72
“Domain policy was changed” 67
“A process has exited” 59
“A user account was locked out” 86
“A privileged service was called” 114
“A process has exited” 84
“Password policy modified” 75
“A logon was attempted using explicit credentials” 86
“A user account was created” 53
```

Attack Summary—Windows

Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

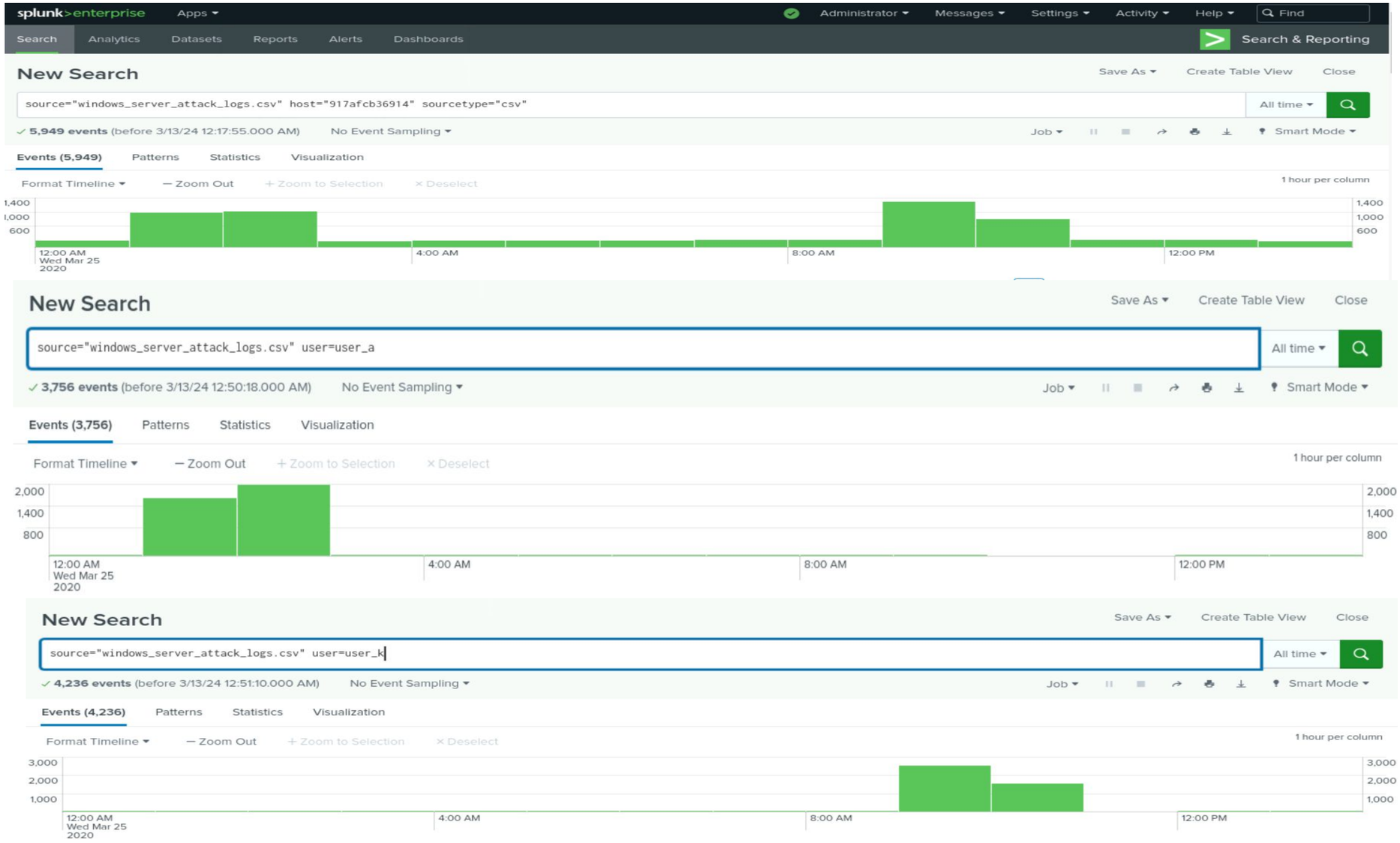
- Yes, our thresholds were set up properly and would alert us to these attacks.

Attack Summary—Windows

Summarize your findings from your dashboards when analyzing the attack logs.

- There were several attempted Man in the Middle attacks, but our alert was set to the proper threshold.

Screenshots of Attack Logs



Attack Summary—Apache

Summarize your findings from your reports when analyzing the attack logs.

- Our reports were formulated correctly and displayed important information when searching through our web server logs.
- A massive amount of network traffic was detected from foreign countries.
- VSI’s login page received 1,296 POST requests in a single hour.
- Our conclusion is that the login page was experiencing a brute force attack.

Summary and Future Mitigations

Attack Summary—Apache

Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

- All of our alerts went off properly and would have notified us of the attack.
- It would be in our best interest to raise our thresholds in order to avoid false positives, as most of our thresholds were extremely low.

Project 3 Summary

- What were your overall findings from the attack that took place?

  We have concluded that the attack that went down was a brute force attack on VSI's login page. The attacker was using a server located in Ukraine to attack the page.

- To protect VSI from future attacks, what future mitigations would you recommend?

  Some mitigations we can recommend to VSI include:

- Incorporate CAPTCHAs to the login page
- Blacklist foreign traffic from sensitive pages (assuming no employees are located in said country)

Attack Summary—Apache

Summarize your findings from your dashboards when analyzing the attack logs.

- Our dashboards displayed accurate information that was useful in determining what attack was underway.