Defensive Security Project

Table of Contents

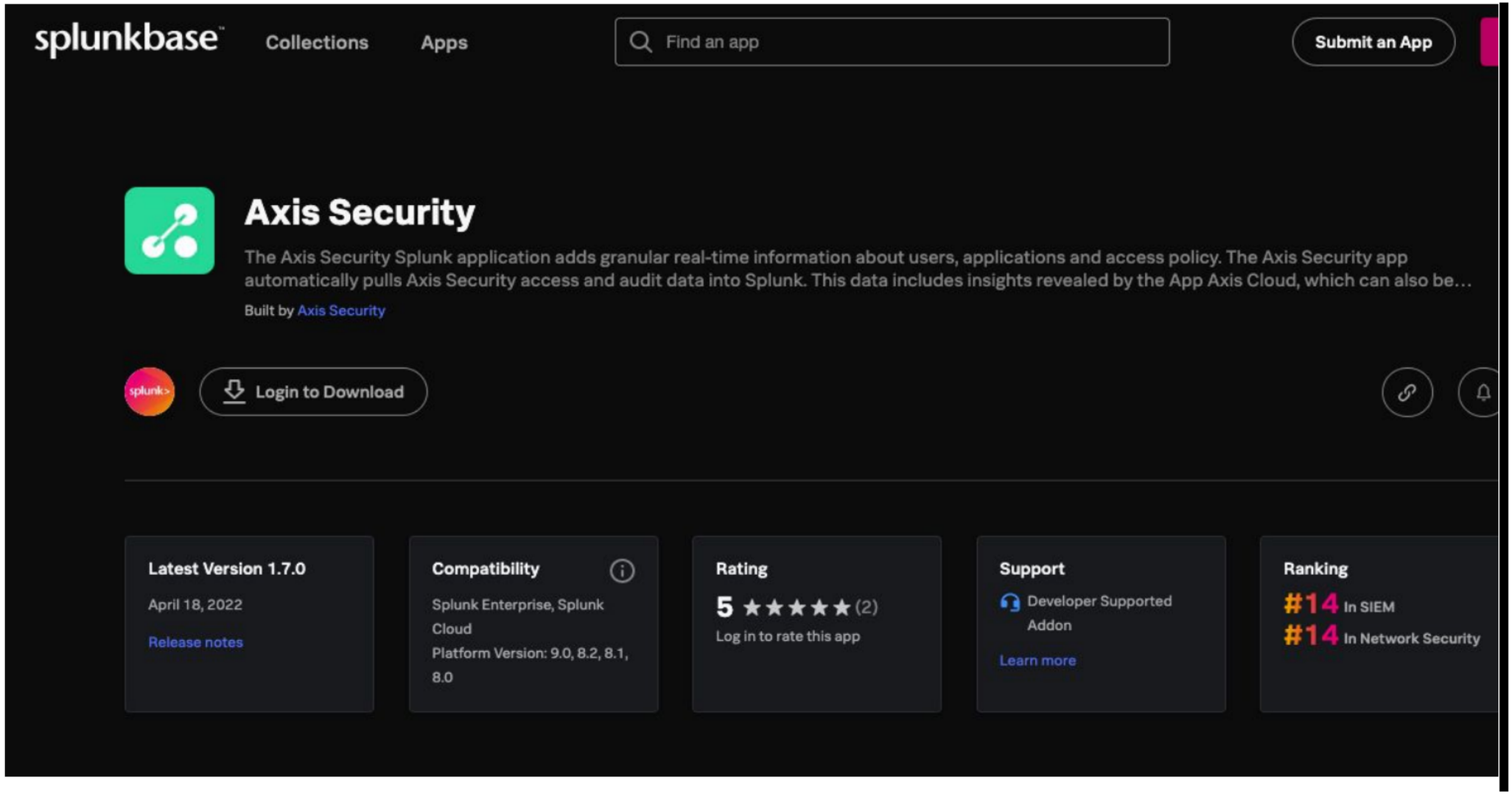
This document contains the following resources:

01 Monitoring Environment
02 Attack Analysis
03 Project Summary & Future Mitigations

Scenario

- VSI is experiencing cyber attacks on their Windows and Apache Servers. The Apache server hosts the company’s main, public-facing web page. The Windows servers contains the intellectual property of VSI.
- Logs from both the Windows and Apache servers were examined for ‘normal’ day-to-day activity
- A separate set of logs were examined containing suspicious levels of activity

Axis Security

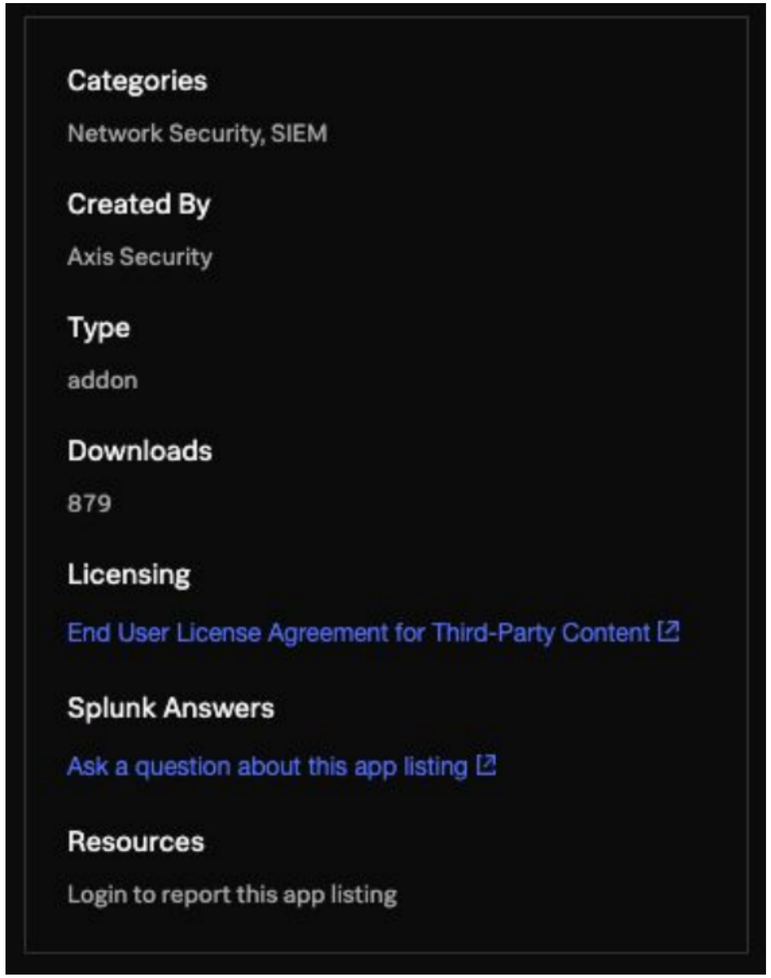


Axis Security

The Axis Security Splunk App allows users to detect and investigate security incidents by logging granular user requests at the application level.

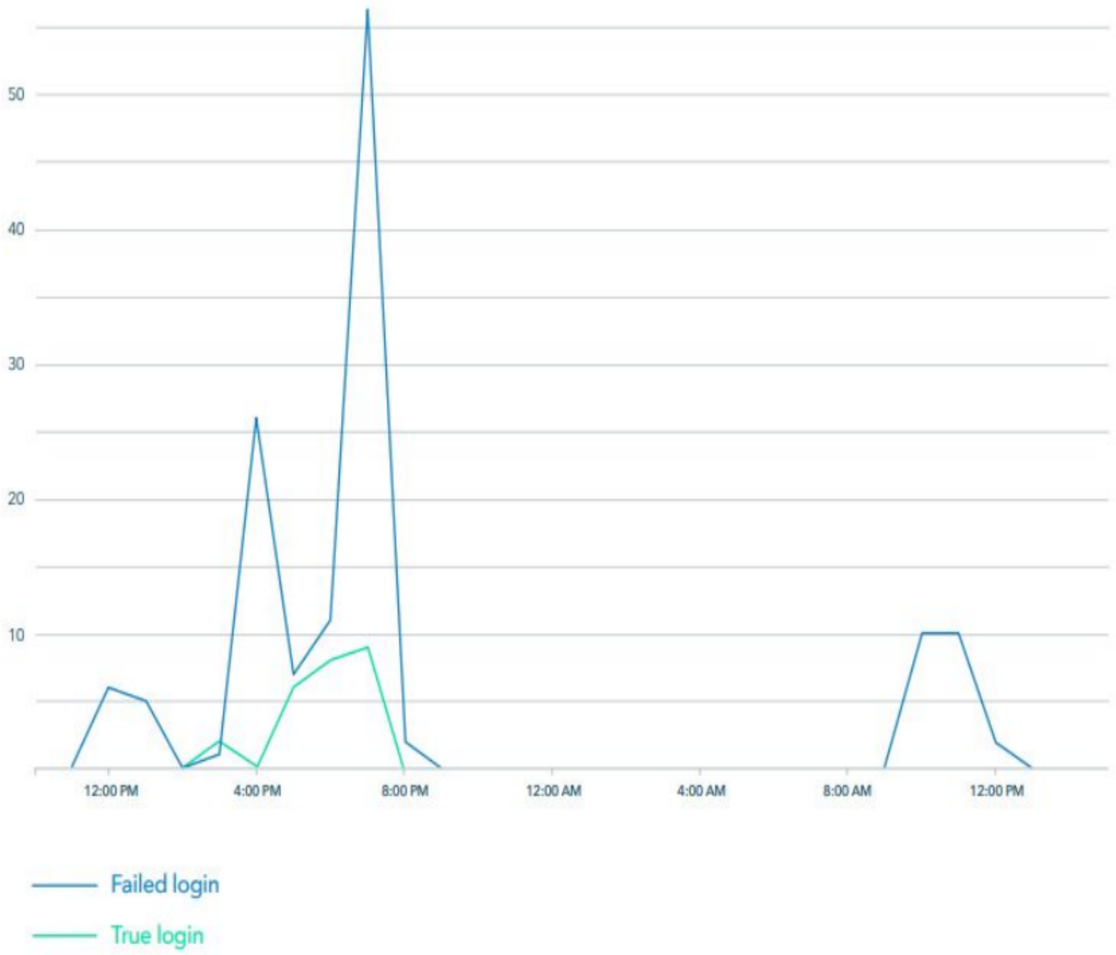
Axis reviews details on user account requests for applications to discover if there has been a breach.

Axis also creates reporting dashboards and scanning logs directly in the splunk environment.



Axis Security

Detecting A Brute Force Attack: Axis Security App pulls app-centric data into Splunk Enterprise to provide, visual information of scenarios like failed login attempts vs true logins



Application-centric view of login activity from the Axis Security Splunk App

Logs Analyzed

Windows Logs

1 **Apache Logs**

VSI’s Windows servers contain the intellectual property of the company. The Windows server logs contained information about the user accounts and their activities on the servers. This includes logins, account management, and authentication policy change.

Webserver log events that shows activities within VSI’s domain. These logs document how traffic flows through VSI’s main homepage and its subdomain paths, monitors what and where requests are originating from and whether they are successful or not.

These logs also document what visitors request from the webserver and their initial HTTP methods of action.

Reports—Windows

Designed the following Reports:

Report Name	Report Description
Signatures & Signature IDs	Report that provides a table that shows the ID number associated with the specific signature for Windows Activity
Severity Report - Windows	Report of the number and percentage of the severity of the Windows logs from Tuesday 3/24/2020
Failed Activity - Windows	Report shows the number and percentages of failed activities on 3/24/2020

Images of Reports—Windows

Signatures and Signature IDs

```
(index=* OR index=_*) source="windows_server_logs.csv" host="windows_server_logs" sourcetype="csv" | table signature_id, signature, user, status, severity, time | fields "signature", "signature_id" | dedup "signature"  | rename signature AS
    RootObject.signature signature_id AS RootObject.signature_id | fields "RootObject.signature" "RootObject.signature_id"
```

All time

✓ **4,764 events** (before 2/3/23 12:54:13.000 AM) No Event Sampling

Job Smart Mode

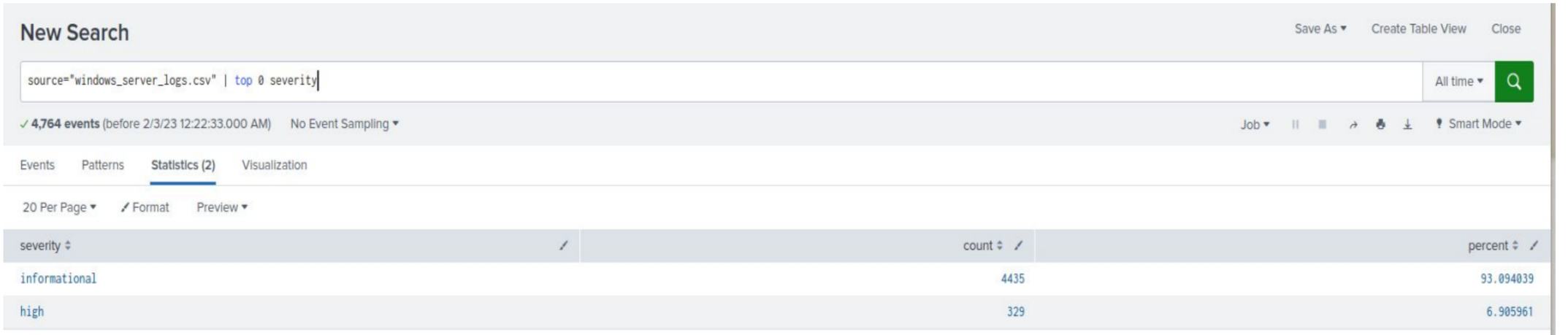
Events Patterns **Statistics (15)** Visualization

20 Per Page Format Preview

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

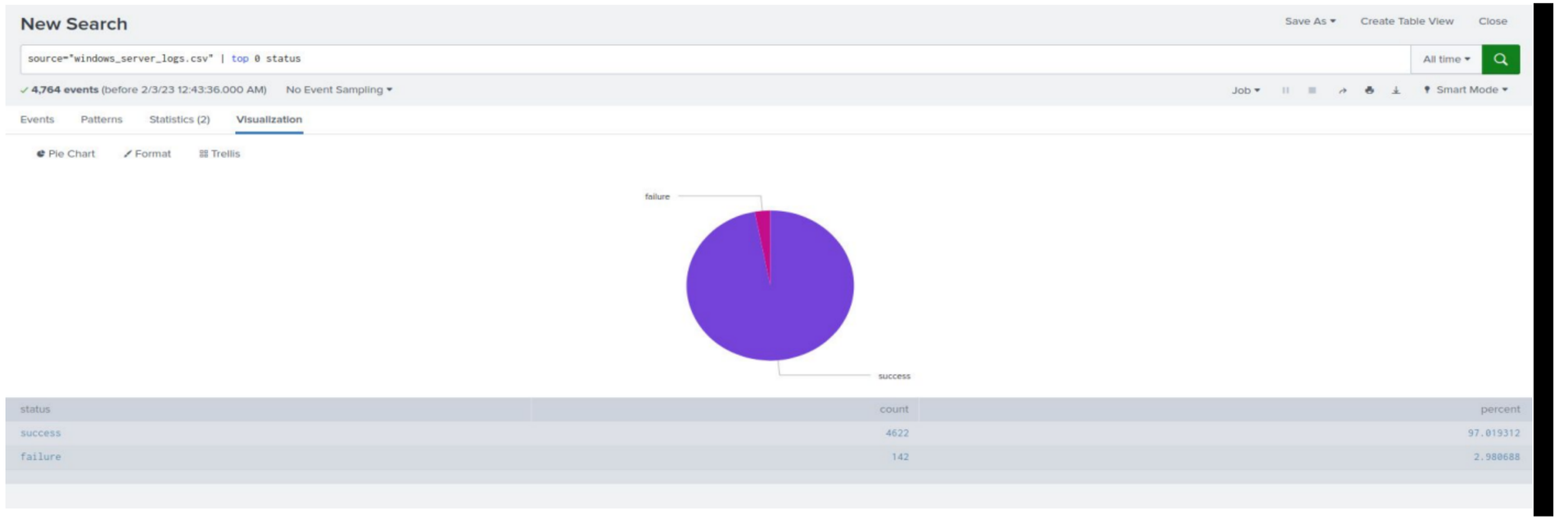
Image of Reports - Windows

Severity



Successful &

Failed Activities



Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Activity - Windows	Alert for failed activities on the VSI	Windows server 32	>50

JUSTIFICATION: Based on the standard level of failed activities for VSI, the baseline was approximately 32 failed activities per hour. The threshold was set to 50. This would avoid potential alert fatigue and still provide security.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Account Logins - Windows	Alert for the number of account logins for the	VSI Windows Server 52	>80

JUSTIFICATION: After examining the average amount of logins per hour, the baseline was set to 52. The threshold was set at 80. On an average day only one hour would have triggered this alert, when there were 84 logins. This threshold may be a little too low but that could be examined in the future.

Alerts—Windows

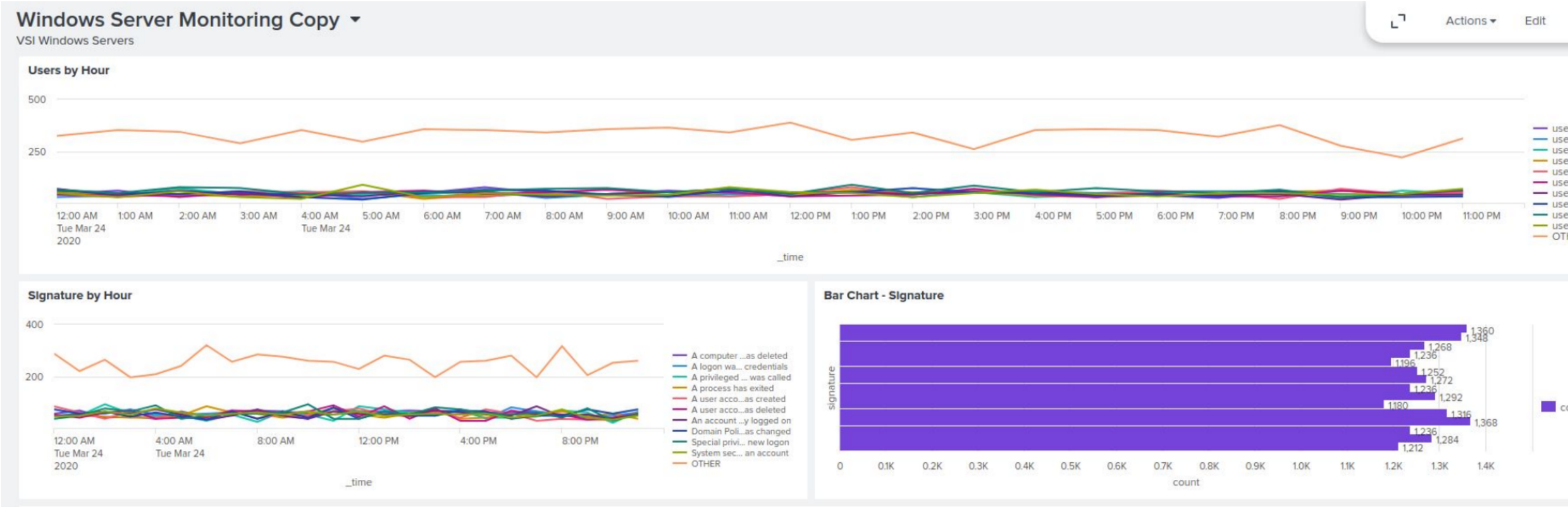
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Deleted Accounts - Windows	An alert for suspicious numbers of accounts deleted on the	VSI Windows server 56	>100

JUSTIFICATION: The baseline was determined by finding the average number of events per hour on a normal day. The threshold was set at 100. This is high enough that it won't be

triggered all the time by normal activity, but will be triggered by suspicious levels of activity

Dashboards—Windows



Dashboards—Windows

⚠

⚠

⚠

Reports—Apache

Designed the following reports:

Report Name	Report Description
HTTP methods table	HTTP methods used in the span of 4 days
Top 10 domain Referers	The top 10 domains that refer to VSI's Website
HTTP Response Status Count	Shows the count of each HTTP response Code

Images of Reports—Apache

HTTP Methods Table

Top 10 Domain Referers

⚠

HTTP Response Status
Code (Left)

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Alarming Hourly Activity outside the United States	Will post an alert and email after the hourly activity outside the United States' threshold is exceeded.	230 events	255 events

JUSTIFICATION: The log report pulled a relatively tight deviation for each hour (per 24 hours), as well as the averages for each hour.
While the 90th percentile deviated wider on certain hours of the day, I concluded 255 as a lower threshold estimation and may change to 260-265 depending on future log activities.

■

Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly HTTP POST Threshold Met	Threshold for the hourly count of HTTP POST method has been exceeded	25 method events	40 method events

JUSTIFICATION: The average POST methods over 4 days is roughly 25, with normal 20s to 30s and the occasional 40s. Having an alert trigger at 30 seems too excessive.

⚠

■

Dashboards—Apache

Geographical Activity

HTTP requests over 4 days

Dashboards—Apache

Top 15 Searched uri’s

Top 10 Country Appearances

■

Dashboard—Apache

4 day UserAgent Count

■

⚠

⚠

Attack Summary—Windows

Observations:

- [redacted]- ‘High’ level severity events jumped from ~7% on a normal day to ~20% on the day of the attack
- [redacted]- 8:00
  - There were 105 failed activities at this time on the day of the attack
- [redacted]- 11:00-13:00
  - There were an abnormal number of logins on the day of the attack
  - From 11:00-12:00 there were 588 successful logins and 231 from 12:00-13:00
  - **user_j** was the primary account logging in

Attack Summary—Windows

Alerts:

- Alert for **failed activities** would have been triggered by the attack
  - Threshold was >50 failed activities
  - This threshold was correct
- Alert for **hourly account logins** would have been triggered by the attack
  - Threshold was set to >80 logins per hour
  - Alert would have been triggered at 11:00 and 12:00
- Alert for **deleted accounts** would not have been triggered by the attack ○ There were approximately 27 events per hour on the day of the attack and that is well

below the threshold of >100

- This threshold could be examined further, but the decrease in normal levels of activity could have been a result of the attack

Attack Summary—Windows

Dashboard Observations:

- [redacted]- suspicious activity was visible in the dashboard
  - ‘A user account was locked out’ - 1:00 - 3:00
  - ‘An attempt was made to reset and accounts password’ - 9:00-11:00
- [redacted]
  - **user_k** and **user_a** had unusual spikes in activity during the same timeframe as the suspicious signature activity above
- [redacted]

- While there was an increase in the numbers of some activities, the overall trends look very similar to the “normal” Windows server logs

Screenshots of Attack Logs

Signature

Task Category

Screenshots of Attack Logs

Signature over time

Attack Summary—Apache

Observations:

- On Wednesday 25th, VSI’s Apache web server received a sudden increase in HTTP traffic.
  - Starting at 19:00, peaking at 20:00 and ramped down till 21:00.

The method of requests were GET and POST related. Mainly POST. Which then triggered an alert, exceeding 1296 POST requests.

The occurring traffic targeted specifically 2 URIs

1. /VSI_Account_logon.php
2. /files/logstash/logstash-1.3.2-monolithic.jar

The sudden traffic spike mainly originated from Ukraine.

Attack Summary—Apache

Alerts:

- The alert for **hourly HTTP POST method** would have been triggered by the attack

- Threshold was set at >40 events hourly
- The trigger would occur between 19:00 and 20:00 with 1296 POST requests

- The alert for **hourly activity outside the United States** would have been triggered by the attack
  - Threshold was set at >255 events hourly
  - The trigger would occur between 19:00 and 20:00 with 864 events from Ukraine

Attack Summary—Apache

URI traffic count during attack

A key element to specify the attackers scope would be the URI event count. As well as the HTTP request methods.

Together, we can conclude a more probable cause for the attackers motives.

- Brute Force
- Path Traversal
- Code injection such as PHP and or SQL.

(Targeting web server log data, and possibly user access).

Screenshots of Attack Logs

HTTP method

Screenshot of Attack Logs

Total Events by Country (including USA)

Events by Country (excluding USA) over time

⚠

Project 3 Summary

- **What were your overall findings from the attack that took place?** The VSI Windows servers and Apache servers were both targeted by attackers. It looks like a brute force attack was attempted on the Windows servers based on the increased number of accounts being locked out and the unusual number of successful logins. Based on the dramatic increase in POST requests, the Apache servers were targeted by what appears to be a PHP injection. The attackers then conducted path traversal to access the /files/logstash directory. Based on the geostats from the logs, the attack appears to be coming from Ukraine.
- **To protect VSI from future attacks, what future mitigations would you recommend?**
  - Stronger password policies for the Windows servers.
  - Stronger user input validation to protect against web application attacks.

- Firewall policy to block dramatic spikes in traffic from a single region.