Defensive Security Project

Henry Hyun
JD Sevigny
Zach Zentner
Zebulun Eaves
Ryta Oberemok
David Xue

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

- Our team was tasked with developing a defensive solution to protect Virtual Space Industries' (VSI) following products:
  - Administrative webpage: https://vsi-corporation.azurewebsites.net/
  - Apache Server
  - Windows OS
- Windows Server Logs and Apache Server Logs were provided for evaluation
- Using Splunk as our primary tool our team proceeded to do the following:
  - Analyze the server logs
  - Create reports and alerts to monitor for potential attacks
  - Install Splunk Add-on for Microsoft Windows for additional surveillance

Splunk Add-on for Microsoft Windows

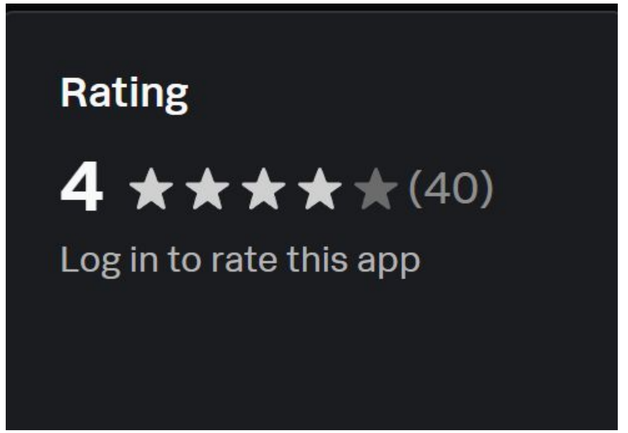
Splunk Add-on for Microsoft Windows

This Add-on for Windows allows a Splunk software administrator to collect the following:

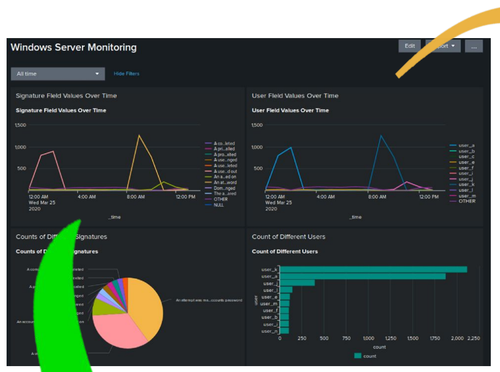
- CPU, disk, I/O, memory, log, configuration, and user data with data inputs
- Active Directory and Domain Name Server debug logs from Windows hosts that act as domain controllers for a supported version of a Windows Server

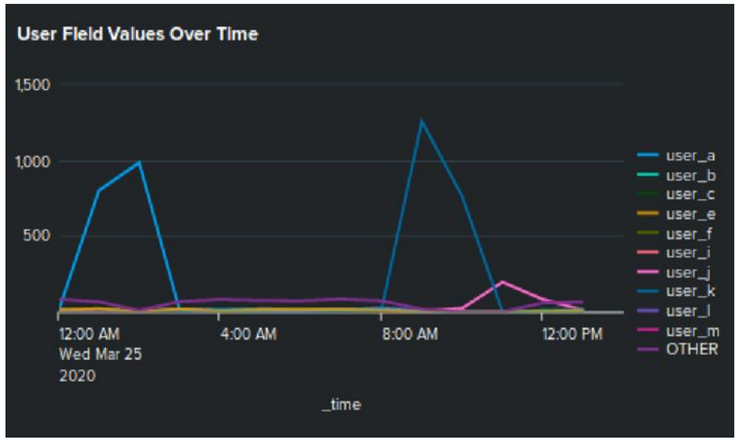
  (Active Directory audit policy configuration IS required since Active Directory doesn't log certain events by default)
- Domain Name Server debug logs from Windows hosts that run a Windows DNS Server

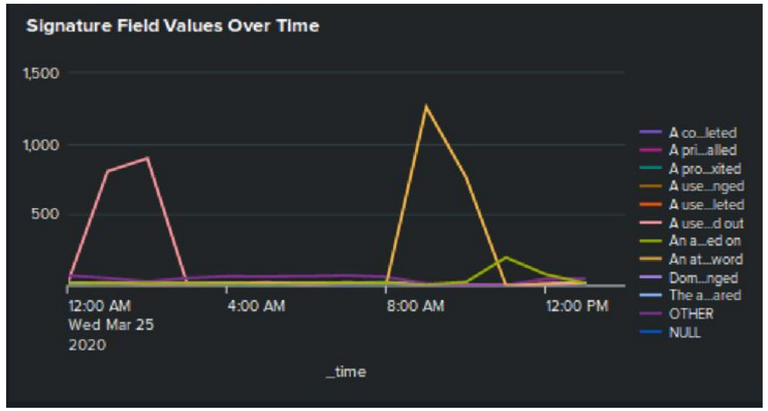
  (MUST enable debug logging since Windows DNS Server doesn't log certain events by default)



Splunk Add-on for Microsoft Windows cont…





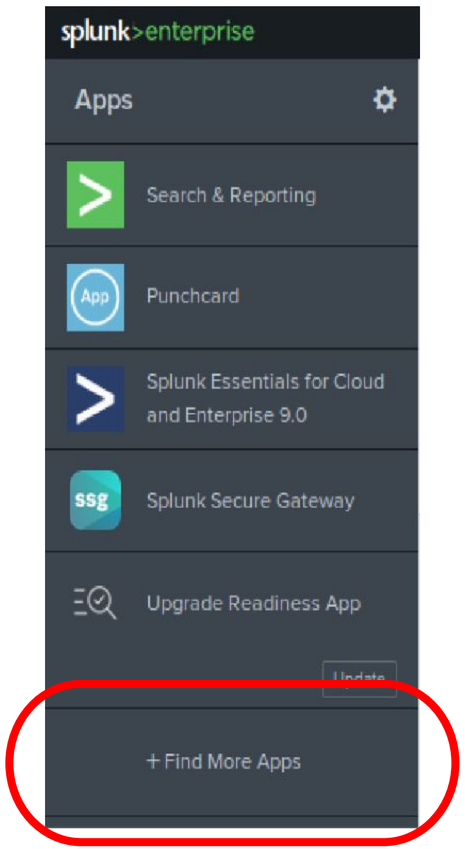


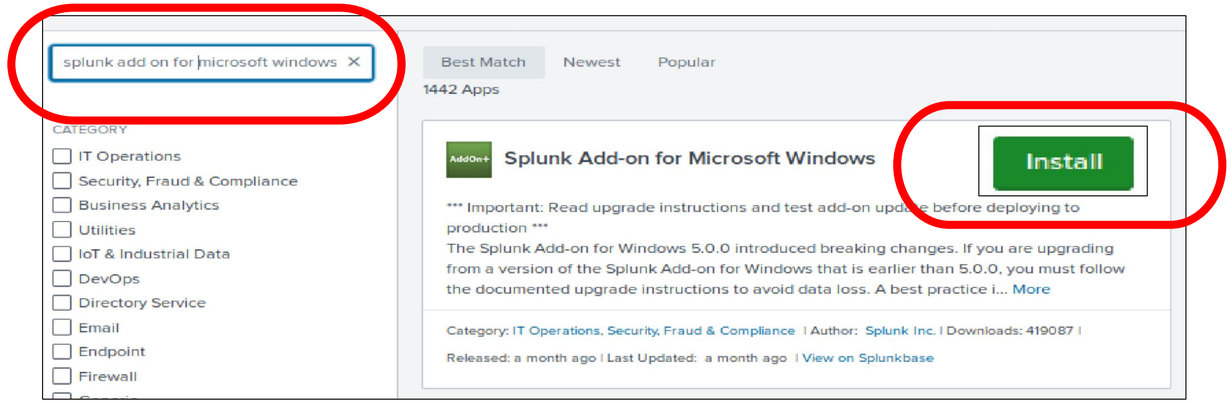
While monitoring the attack logs, we saw what appeared to be an attempted Brute Force attack. Benefits of this add on to help fight such attacks include:

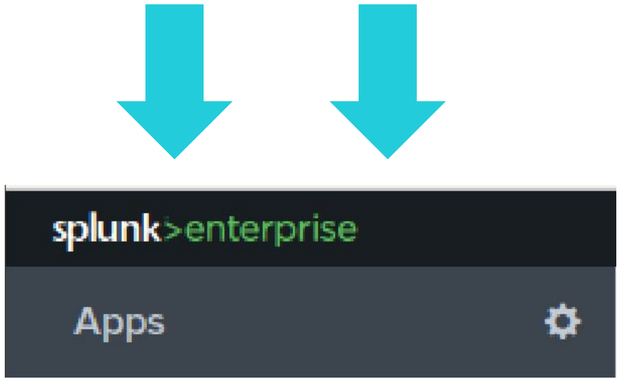
- real time monitoring which can identify different patterns of attacks
- additional alerts that can be created/sent to security teams for quicker response
- integration with other security solutions allowing for automated responses
  - for example, triggering an automatic IP block or initiate an account lockout

Splunk Add-on for Microsoft Windows Installation

Application installation is easy!







Logs Analyzed

1 Windows Logs

- Signature: e.g. “an account was successfully logged on.”
- Signature_id e.g. 4624
- User: Windows Account Users
- Status: success and failure of Windows activities
- Severity Level including high, informational

2 Apache Logs

- method, HTTP methods (GET, POST, HEAD, etc.)
- referer_domain, domains that refer to VSI’s web
- status, HTTP response code (e.g. 200, 304, etc.
- clientip, the user IP address from a specific county
- useragent, the browser used by user

Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Signature Report	A report with a table of signatures and associated signature IDs
Severity Report	A report that displays the severity levels, the count, and the percentage
Windows Activity Report	A report that provides a comparison between the success and failure of Windows activities

Images of Windows Signature Report

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv" | table signature_id, signature | dedup signature_id, signature
```

15 results 20 per page ▾

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

Images of Windows Severity Report

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv" | top limit=20 severity
```

Stat Count by Severity (correct)

Edit ▾ | More Info ▾ | Add to Dashboard

Severity level count and percentage

All time ▾

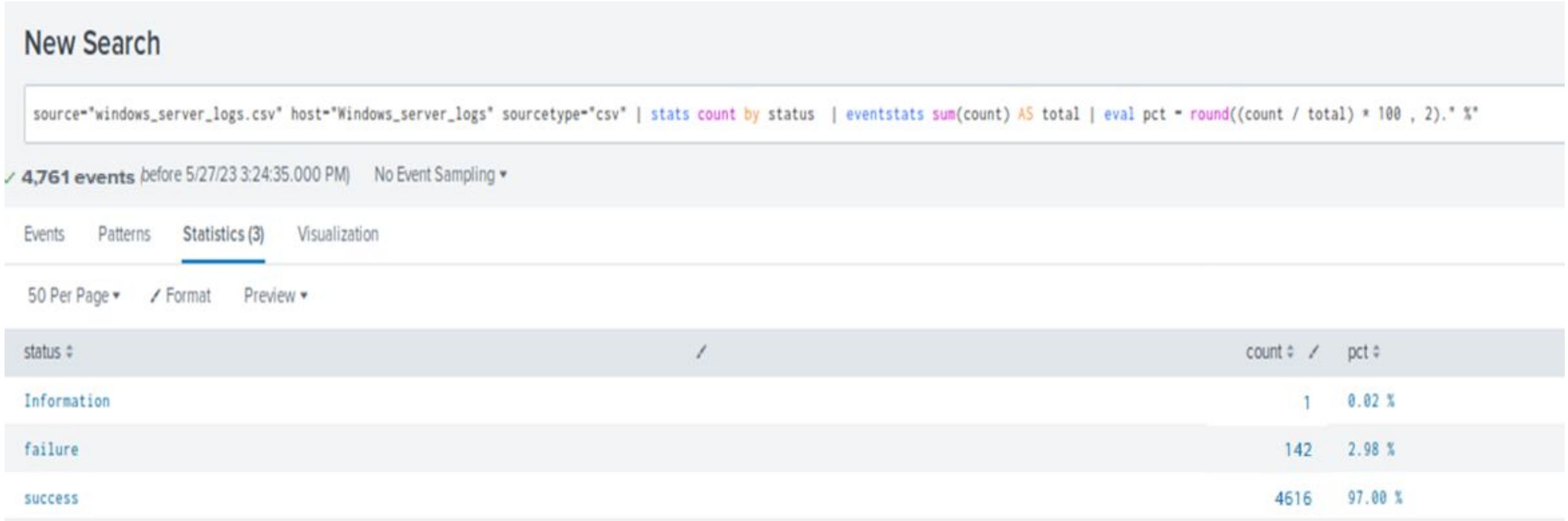
✓ **4,761 events** (before 5/24/23 3:04:22.000 AM)

Job ▾

2 results 20 per page ▾

severity ⇕	count ⇕	percent ⇕
informational	4429	93.085330
high	329	6.914670

Images of Windows Activity Report



Alerts — Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Failed Windows activity	Failed Windows Activities over 15	10	15

JUSTIFICATION: normally, the highest Failed Windows activity quantity is 10 and average is 6, so set the altered threshold as 15 with 5 extra as a buffer.

Alerts – Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Successful Logged-on Alert	An Account was Successfully Logged-on (ID:4624) over 30	23	30

JUSTIFICATION: normally, the highest An Account was Successful Logged-on (ID:4624) is 23 and lowest is 8, so set the altered threshold as 30 with 7 extra as a buffer.

Designed the following alerts:

Alerts – Windows

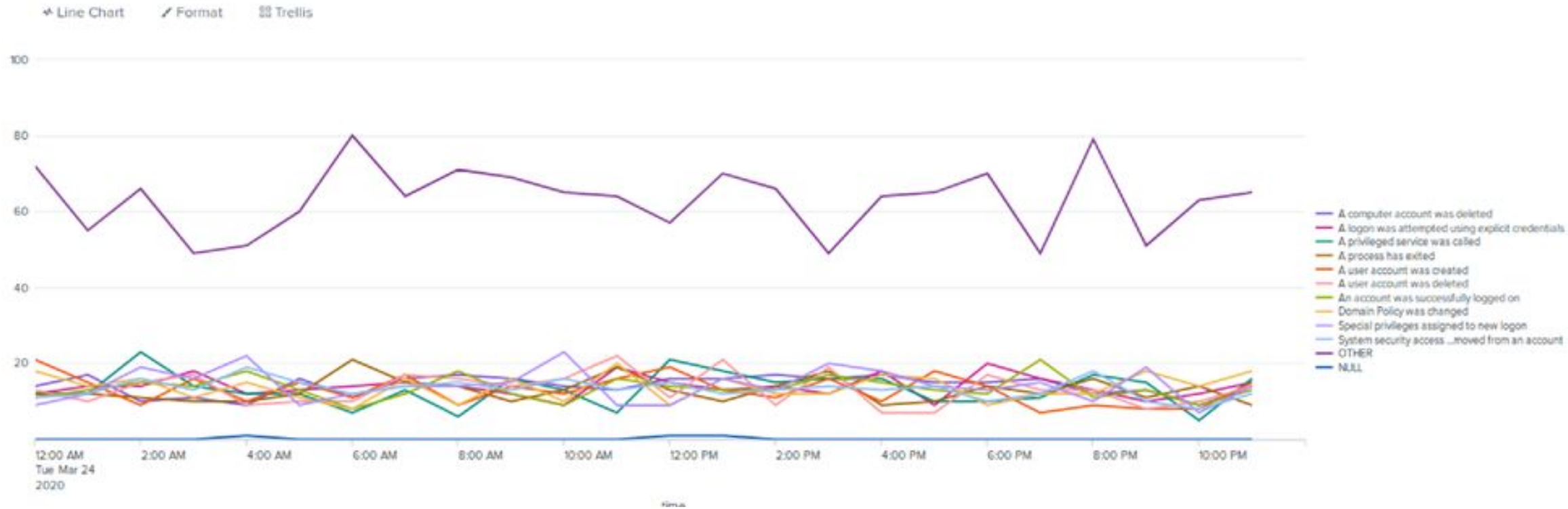
Alert Name	Alert Description	Alert Baseline	Alert Threshold
User Accounts Deleted Alert	A user account was deleted(ID:4726)are over 30	22	30

JUSTIFICATION: normally, the highest A user account was deleted (ID:4726) is 22 and lowest is 7, so set the altered threshold as 30 with 8 extra as a buffer.

Dashboards — Windows

Signature Count Line Chart

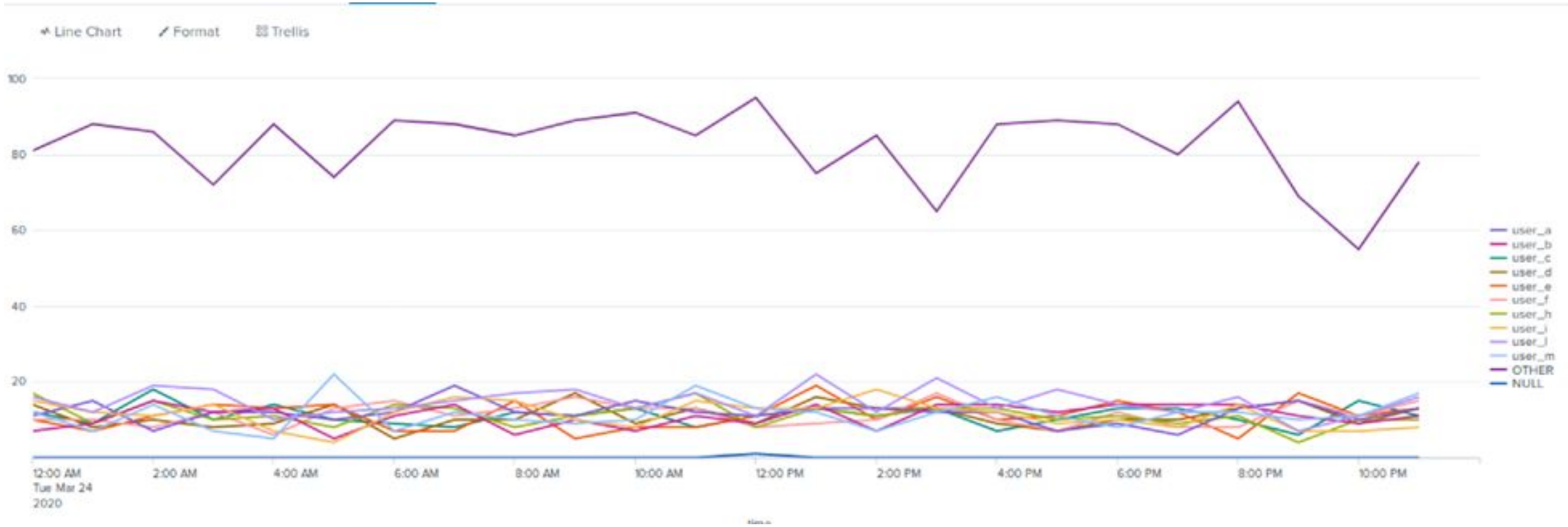
```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"| timechart span=1h count by signature
```



Dashboards — Windows

User Count Line Chart

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"| timechart span=1h count by user
```



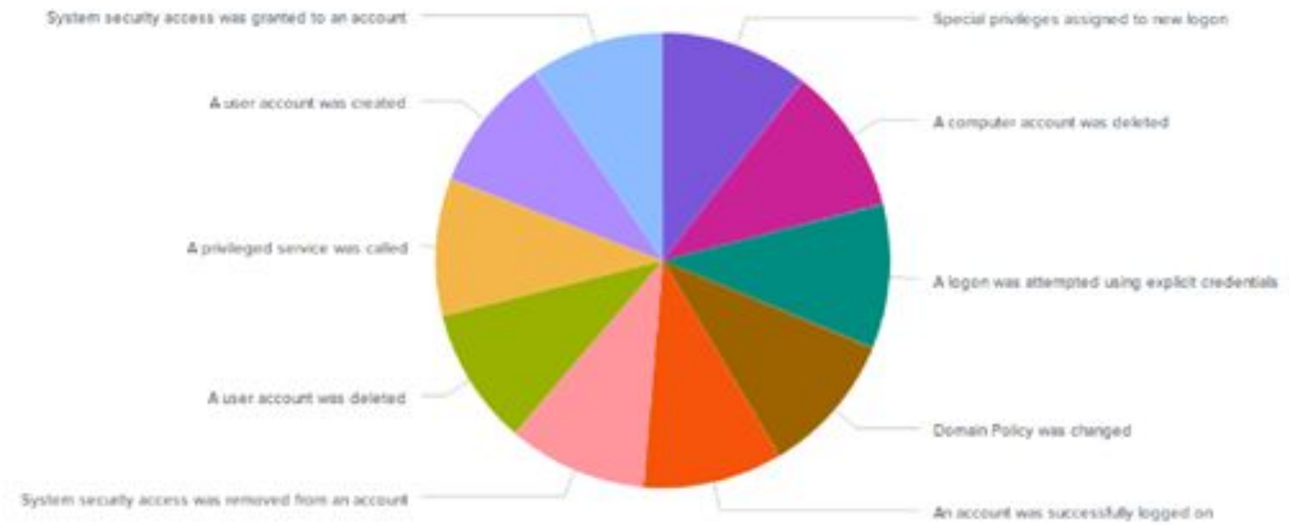
Dashboards — Windows

Signature Count Pie Chart

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"| top limit=10 signature
```

Events (4,761) Patterns Statistics (10) Visualization

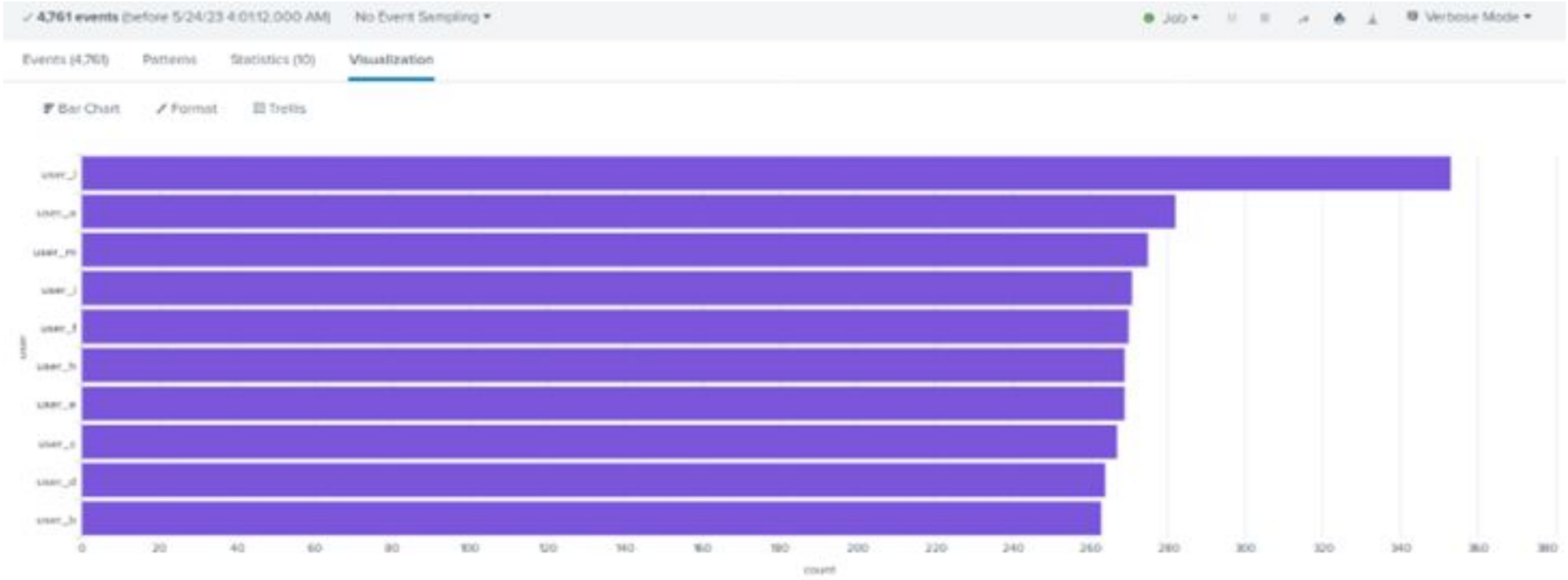
Pie Chart Format Trellis



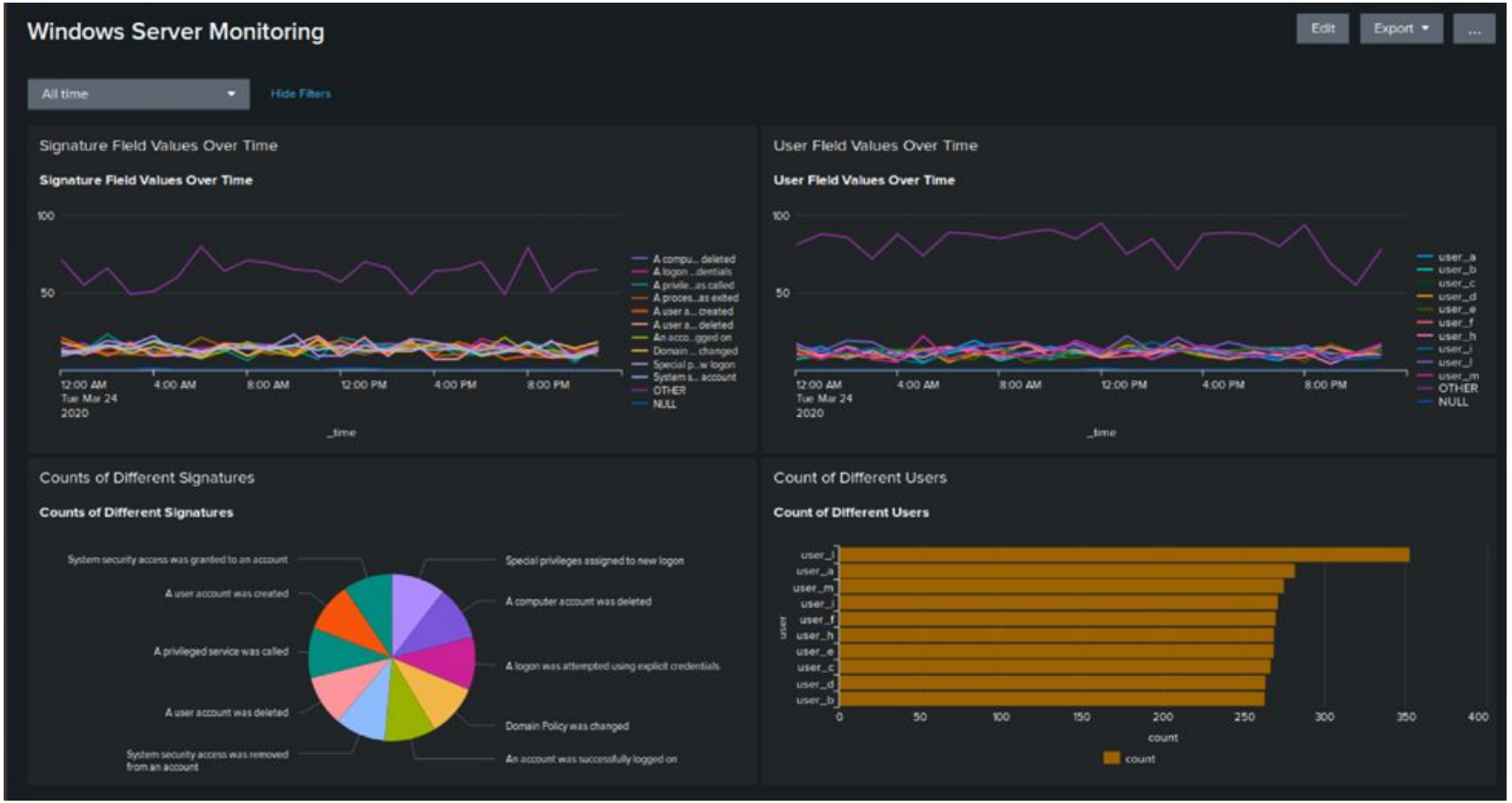
Dashboards — Windows

User Counts Bar Chart

```
source="windows_server_logs.csv" host="Windows_server_logs" sourcetype="csv"| top limit=10 user
```



Dashboards—Windows Server Monitoring



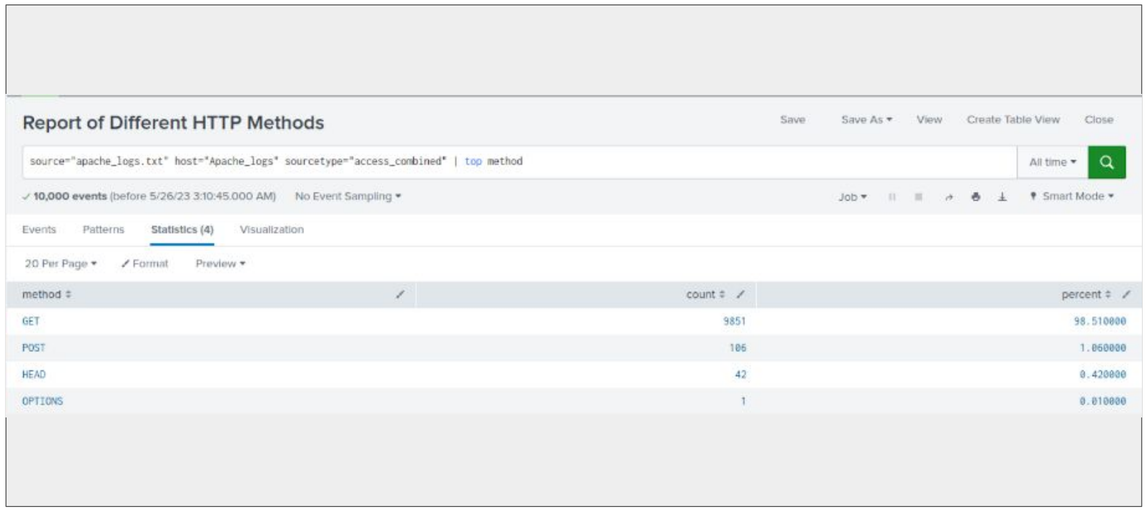
Apache Logs

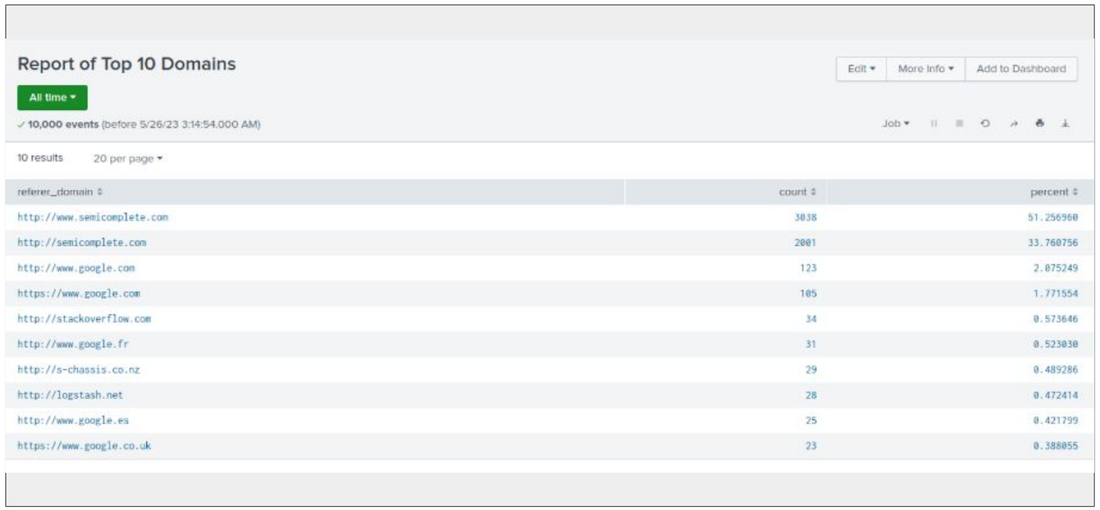
Reports—Apache

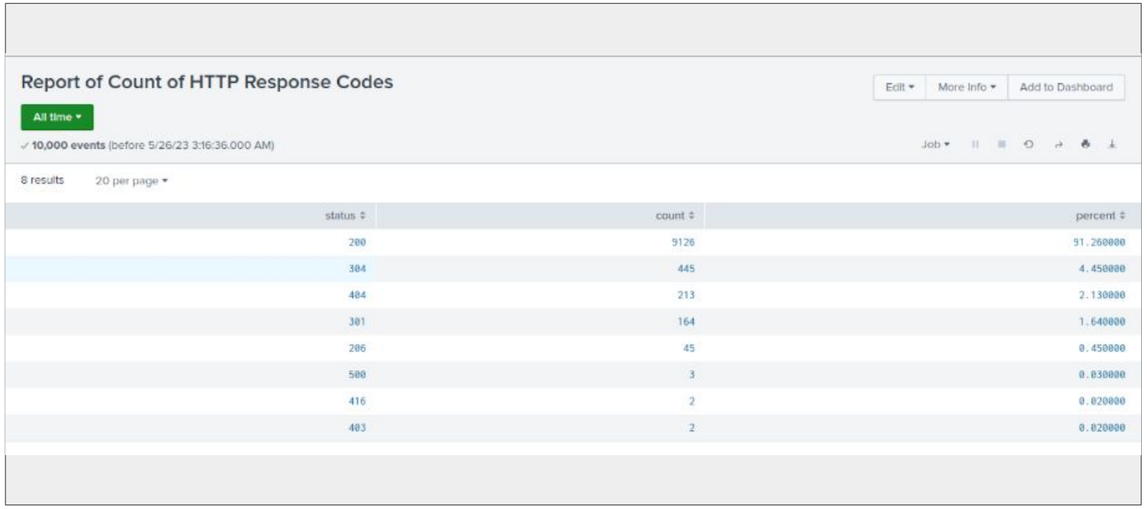
Designed the following reports:

Report Name	Report Description
Different HTTP Methods	Show the count and percentage of each HTTP method used
Top 10 Domains	Shows the top 10 referrer domains
HTTP Response Codes	Shows the count and percentage of each HTTP response code received

Images of Reports—Apache







Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Activity from Non-US Users	Sends out an alert when the count of non-US users exceed the set threshold	60	110

JUSTIFICATION: The normal activity appeared to be concentrated within the 40 - 80 range. There were a few counts that were above 100, but these could be considered rush/peak hours.

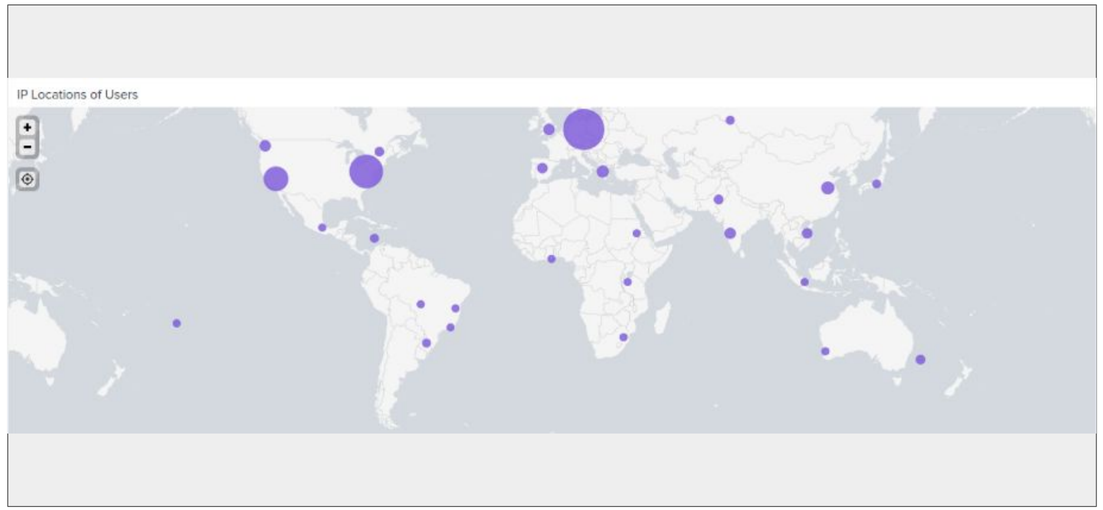
Alerts—Apache

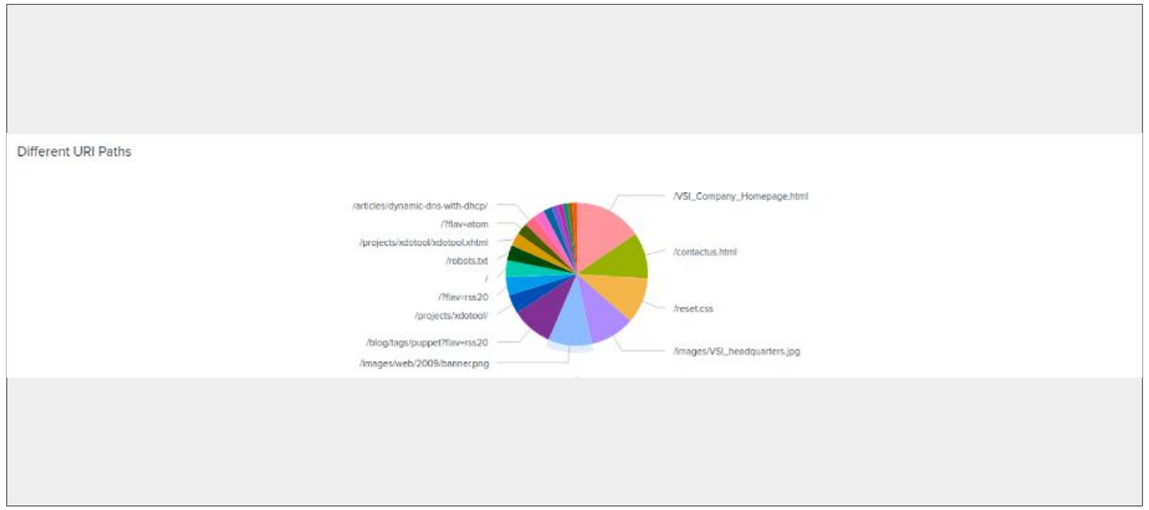
Designed the following alerts:

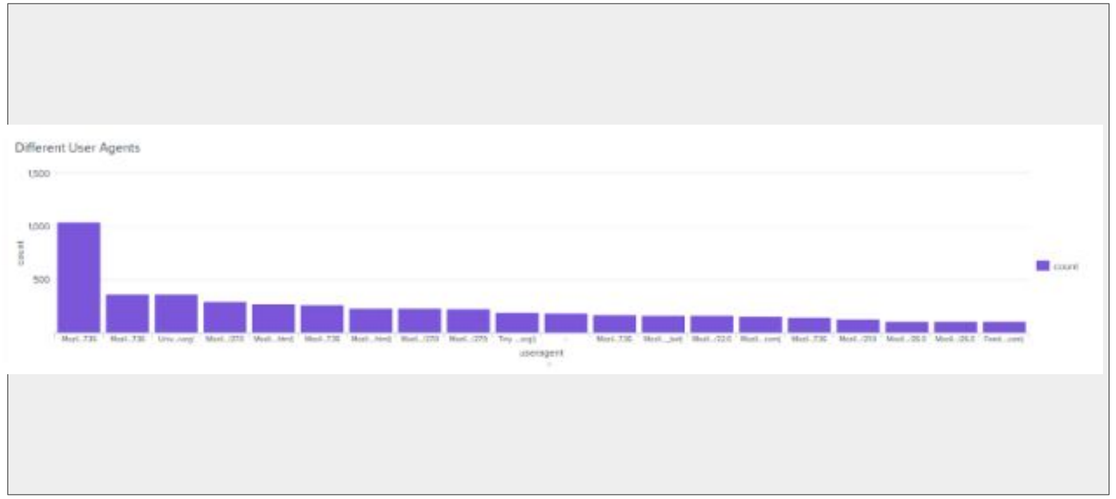
Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Count of HTTP Response Methods	Sends out an alert when the count of HTTP responses surpasses the threshold	3	10

JUSTIFICATION: Since the range of normal activity was primarily between 0 - 4 counts, the threshold was set to 10.

Dashboards—Apache







Attack Summary

Attack Summary—Windows

While analyzing the Windows attack logs, our team found the following:

- user_k is responsible for “An attempt was made to reset an account’s password”.
- The attempt to reset the account’s password was unsuccessful.
- Mitigate a password reset by having a strong password. A password should be at least 12 characters long, contain both upper and lowercase letters, numbers and symbols.
- user_a is responsible for “A user account was locked out”.
- The attacker attempted use brute force to login user_a’s account
- To mitigate this lower the threshold for user_k and user_a.

Attack Summary—Windows

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

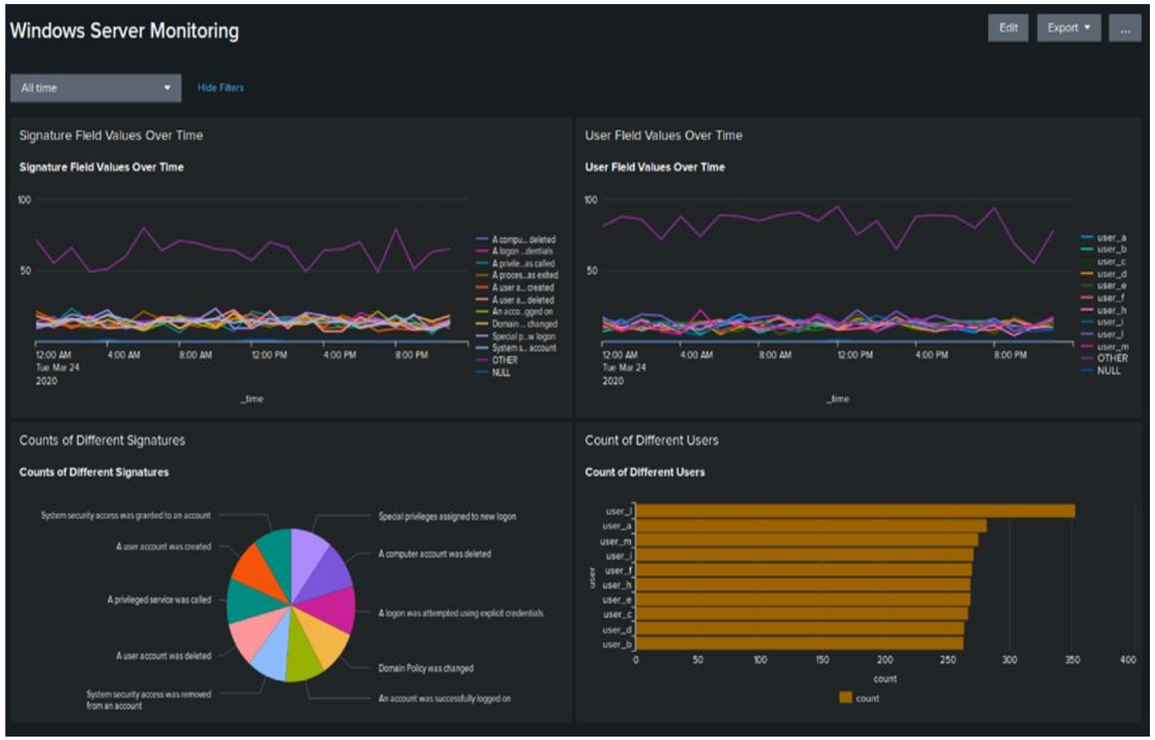
- The thresholds were correct, however lowering them to trigger an alert sooner can decrease the risk of a successful attack. The count of an attempt made to reset the account's password was 4,256 and A user account was locked out count was 3,622. The peak count for user_k was 4,236 and user_a was 3,756.
- A lower threshold will improve the detection of an attack and is less likely to go unnoticed.
- However, if a threshold is set too low there is a potential for false positives.

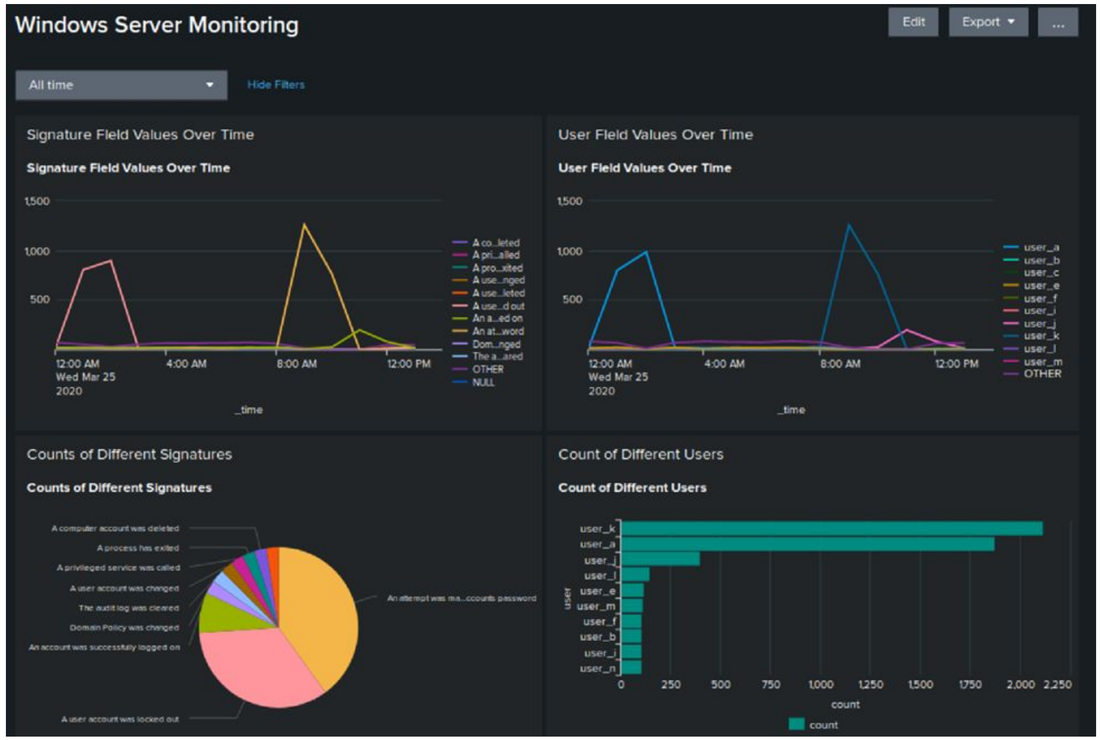
Attack Summary—Windows

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

- There were multiple attempts to log into a user account between 12 AM and 3 AM and multiple attempts to reset an account’s password between 8 AM and 11 AM on the same day Wednesday, March 25, 2020.
- There was a significant decrease in the signature count between “An attempt was made to reset an account’s password”, and “A user account was locked out” compared to the other eight signatures.
- there was a significant decrease in the user count of user_k and user_a compared to others users.

Screenshots of Attack Logs





Attack Summary—Apache

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

- There were suspicious changes in the HTTP methods Get which decreased 98% to 70% and POST which increased from 1% to 29% with the attack log. But there were no suspicious changes detected in the percentage of the two referrer domains. http://www.semicomplete.com changed from 51% to 49% and http://semicomplete.com changed from 33% up to 36% with the attack log.
- There was a suspicious change in the HTTP response code 404 that increased from 2% to 15% during the attack, which indicates someone is scanning for vulnerabilities and resources to use.
- To mitigate this check the web server logs to identify a pattern or source causing the increase of 404 errors to stop a potential attack at the beginning.

Attack Summary—Apache

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

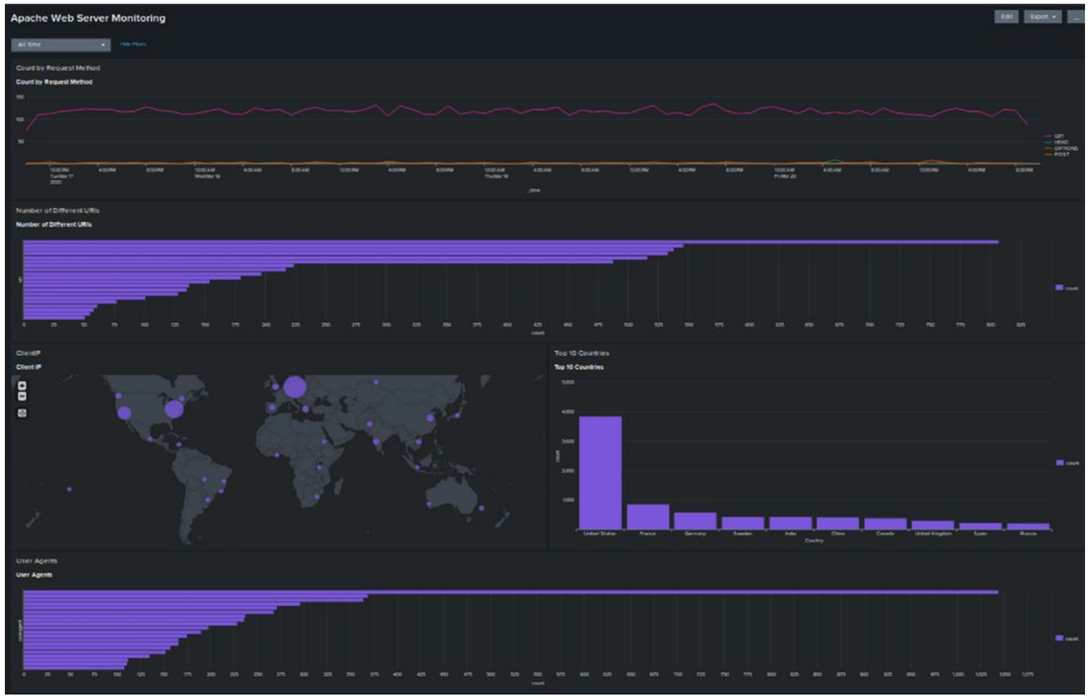
- Yes, the thresholds were correct and do not need to be changed.
- There was a suspicious volume of international activity coming from Ukraine in the cities of Kiev and kharkiv.
- The alert also detected a suspicious volume of HTTP POST activity occurring at the same time as the international activity coming from Ukraine.

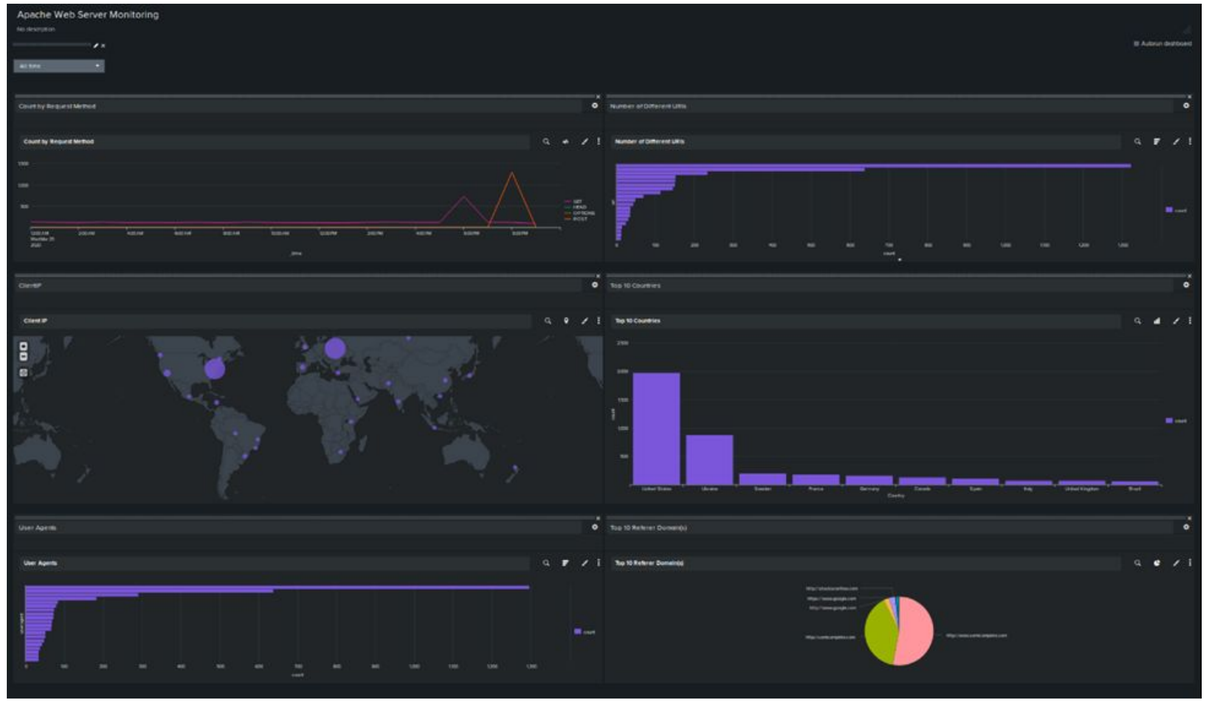
Attack Summary—Apache

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

- The Time Chart of HTTP methods showed suspicious GET method activity between 5 PM to 7 PM and POST activity from 7 PM to 9 PM.
- The peak count of the GET method was 729 and the POST method was 1,926.
- The dashboards also found activity coming from Ukraine with counts of 439 coming from Kiev and 433 from Kharkiv.
- On the URI dashboard there was a high count of activity with 1,323 and a suspicious amount of logon attempts for /VIS_Account_logon.php and /files/logstash/log…1.3.2-monolithic.jar. The attacker could be using a brute force method to logon to the VSI.

Screenshots of Attack Logs





VS

Summary and Future Mitigations

Project 3 Summary

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

- the server attack affected multiple users
- user_k made several attempts to 'reset an account password'
- user_a's account was 'locked out' due to number of incorrect password entries
- user_j also saw a hit for amount of 'successful logins' indicating the possibility the account was breached
- a high flux of the incoming traffic that attacked the apache server came from the Ukraine

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

- setting user specific alerts at lower thresholds to monitor their account(s) more closely
- requiring higher complexity for account passwords
    - multi-factor authentication can also be used for additional protection
- employees should be made aware of attacks and reminded of good security practices
- blocking incoming IP traffic from specific geographical locations (specifically Ukraine in this instance)
    - also consider blocking the user agent in case they try to mask their IP
- more Splunk Apps (like Apache add on, etc) can be downloaded for additional monitoring