Fable CyberSecurity Inc.
Critical Security Report for Client VSI

Collaborators: Joshua Emo, Tyler Crawford & Rana Mahal

Table of Contents

This document contains the following resources:

Monitoring Environment

Scenario

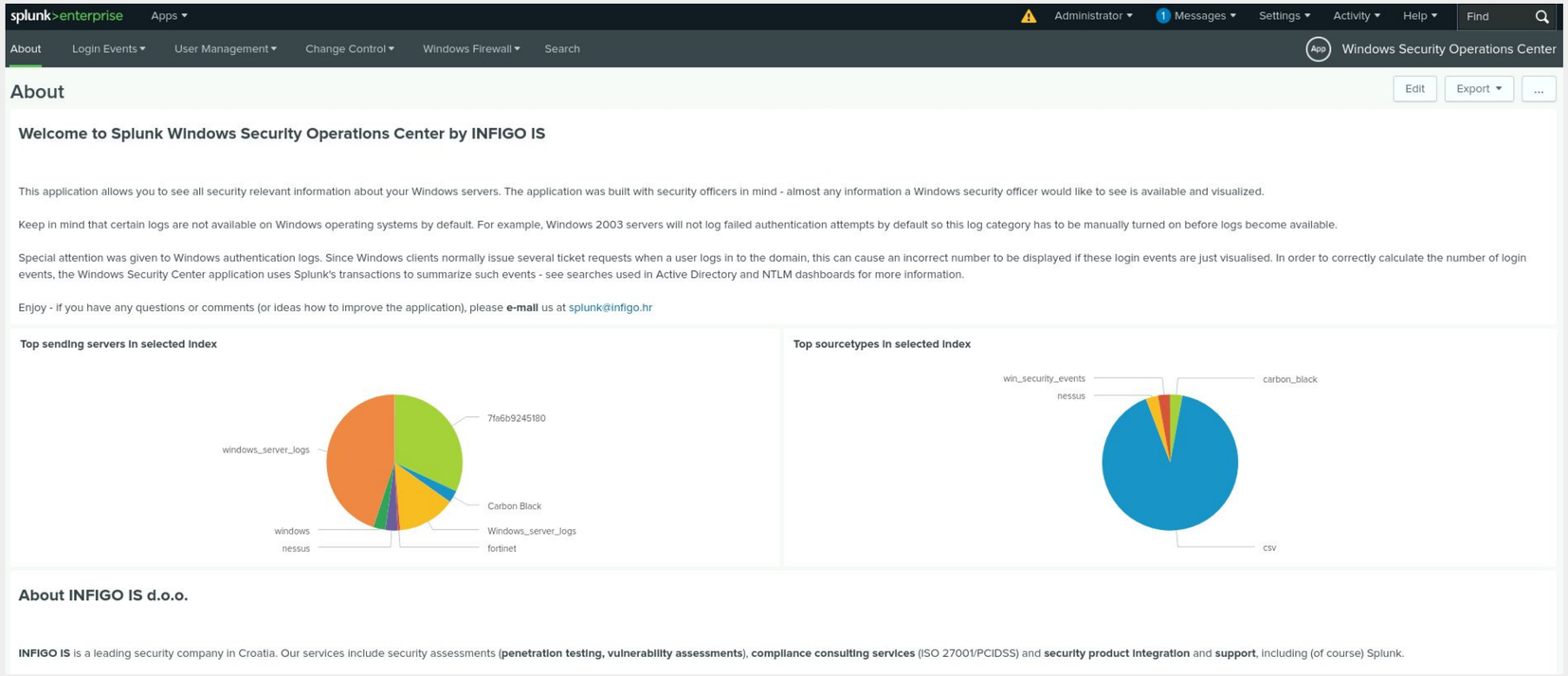
- We represent the analyst team at Fable CyberSecurity Inc. working on behalf of our client, Virtual Space Industries (VSI), a leader in the field of virtual reality for enterprise.
- Our client received intelligence suggesting that their competitor, JobeCorp, might launch cyber attacks aimed at disrupting their business operations.
- In response to this, we have been instructed to analyze and take proactive measures to safeguard their systems using Splunk as our main tool for monitoring and defense.
- Our primary goal is to protect two critical components of the client's infrastructure:
  - Apache Web Server: This server hosts their administrative webpage, a vital part of VSI's day-to-day operations.
  - Windows Operating System: This system supports many of their back-end operations, making it a key target for any potential attacks.
- Using historical log data provided by our networking team, we established baselines and created comprehensive reports, alerts, and dashboards in Splunk.
- These tools have enabled us to monitor our systems closely and respond to any suspicious activities, ensuring that we are well-prepared to counter any attempts by JobeCorp to disrupt our client's business.

Splunk Windows Security Operations Center

Splunk Windows Security Operations Center

We chose Windows Security Operations Center by INFIGO as our add-on app.

We decided to install this add-on as it allows us to track and monitor multiple Windows logs efficiently. The app allows for multiple reports and dashboards all within a central area.



Splunk Windows Security Operations Center

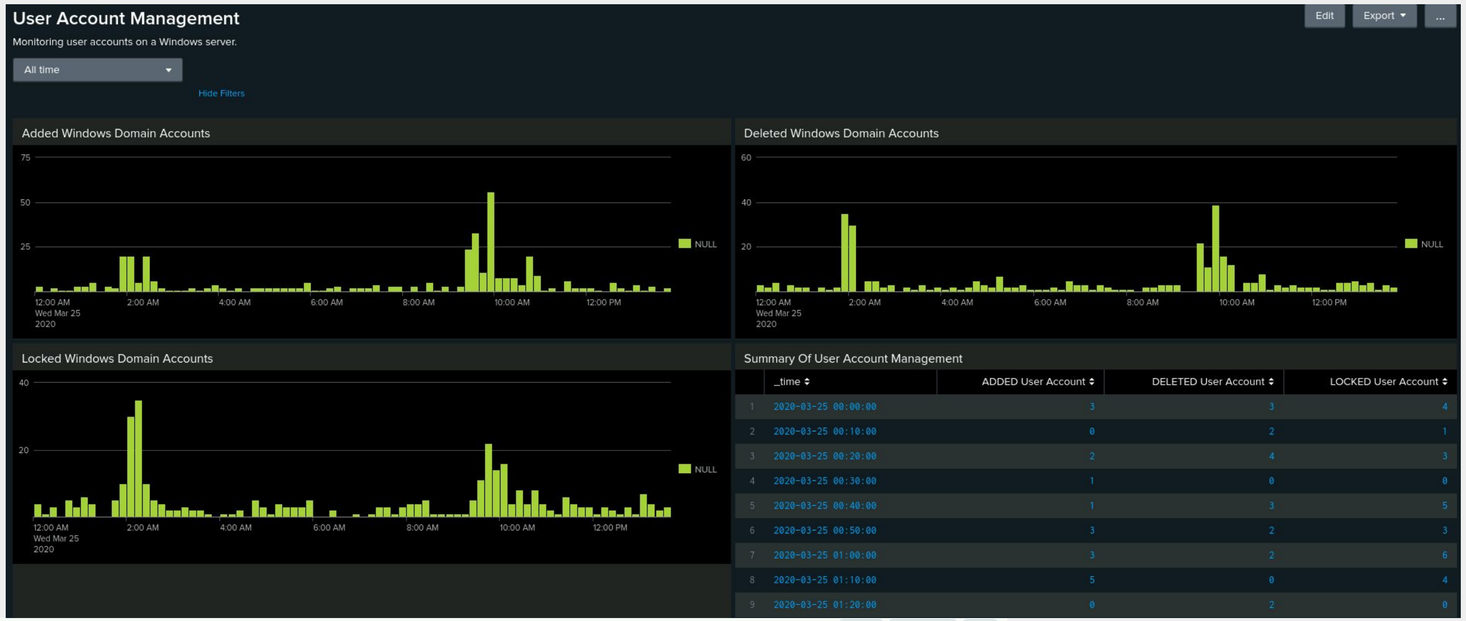
The Splunk Windows Security Operations Center allows for multiple dashboards, suited for monitoring multiple reports for Windows at once.

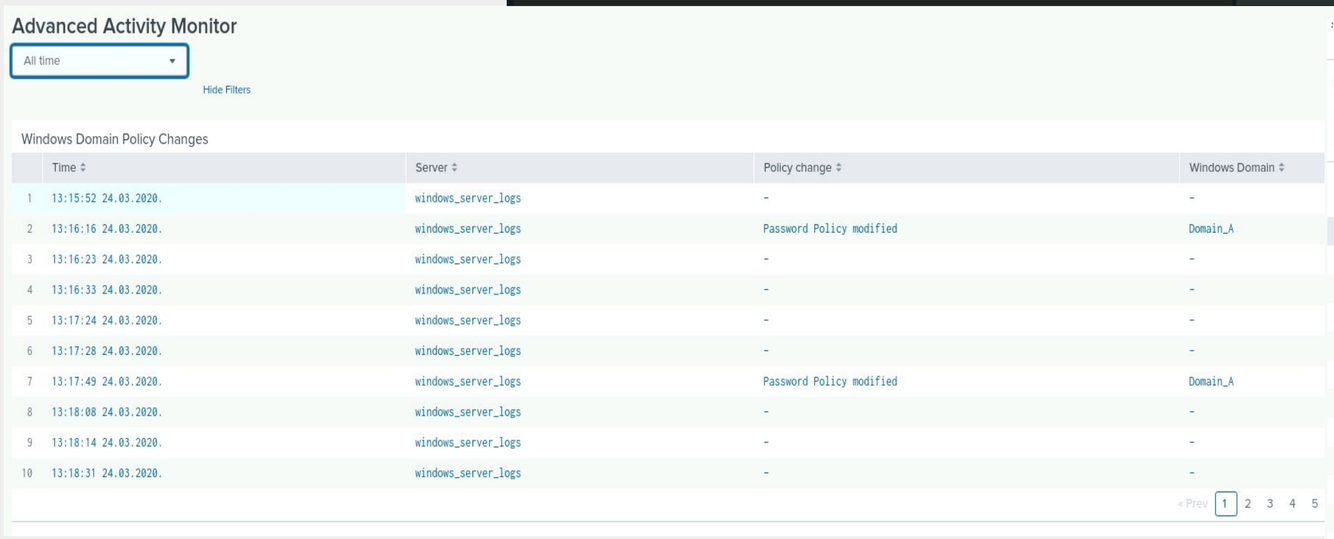
Some of it’s highlights include:

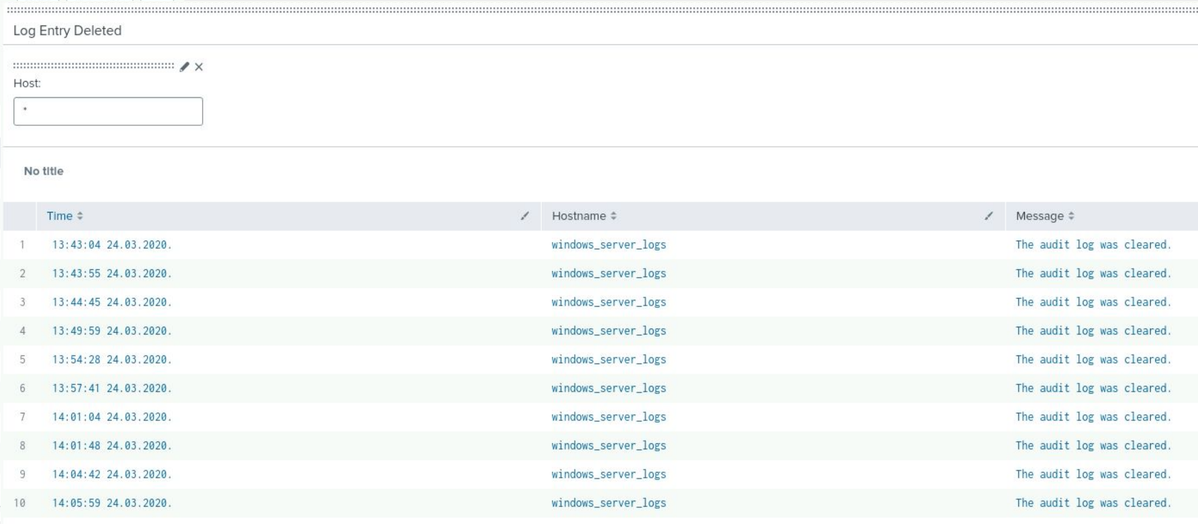
- Monitors successful and unsuccessful logins for Active Directory, NTLM, and RDP.
- Monitors Windows Domain account creation, deletion, logins, and locked accounts.
- Tracks if groups are created, deleted, or if members are added.
- Monitors Windows Domain Policy changes and audit logs.
- Logs Windows installation history, security patches, and lists the details of updates.
- Lists the configuration changes, blocked and allowed connections for firewalls.

These automated reports allow for efficiency when monitoring large amounts of data from Windows server logs.

Splunk Windows Security Operations Center







Logs Analyzed

1 Windows Logs

We analyzed the following logs:

- windows_server_logs.csv: Contains logs of normal activity for the windows server.
- windows_server_attack_logs.csv: Contains data from the cybersecurity incident.

We analyzed signatures, signature ids, users, user counts, and severity.

2 Apache Logs

We analyzed the following logs:

- apache_logs.txt: Contains logs of normal activity for the apache server.
- apache_attack_logs.txt: Contains logs of data from the cybersecurity attack incident.

We analyzed the geographical locations of the attacks and their statuses.

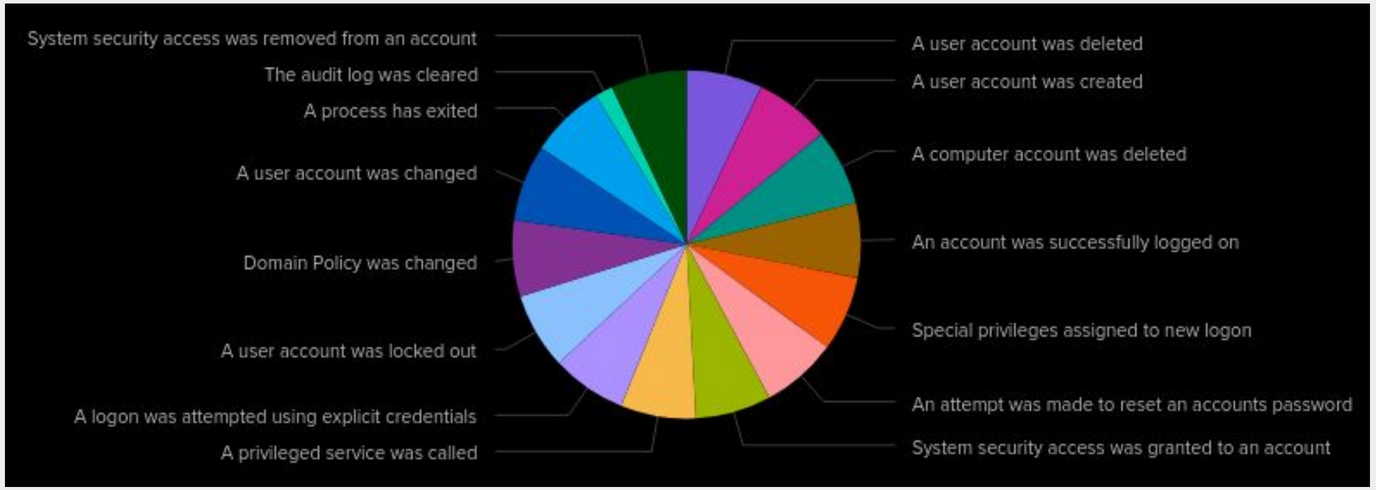
Windows Logs

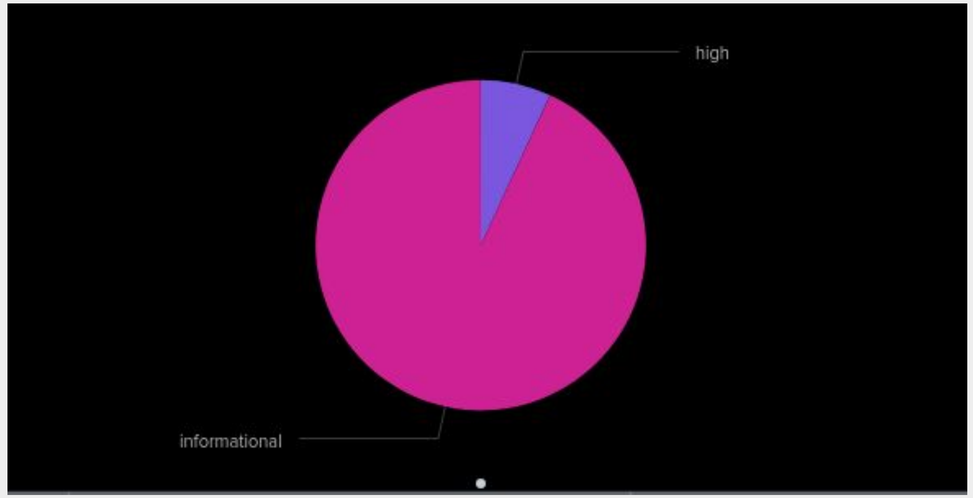
Reports—Windows

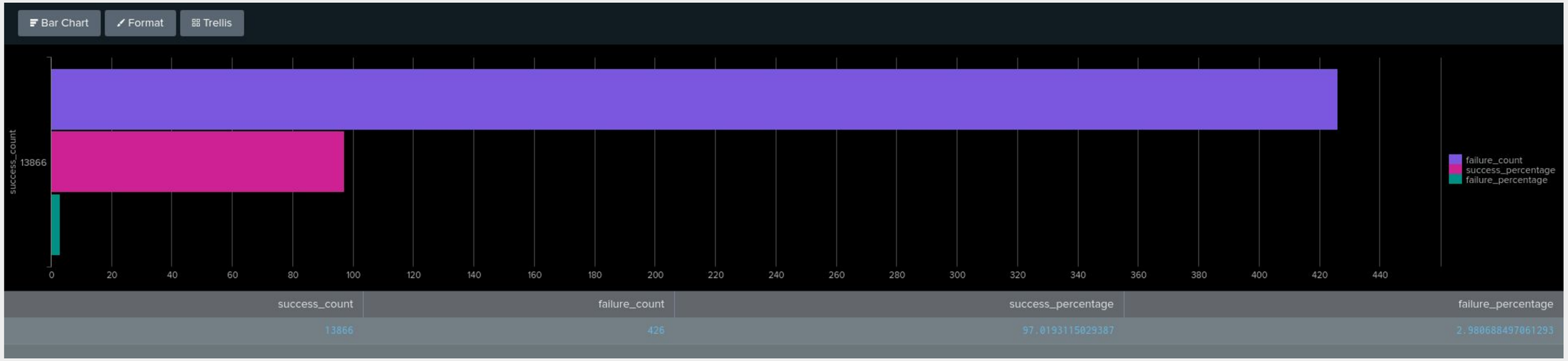
Designed the following reports:

Report Name	Report Description
Windows Event Signatures	Lists and describes all signatures within a log
Windows Success and Failure Activity	Lists all Windows events if they succeeded or failed
Windows Severity	Displays events with their severity

Images of Reports—Windows







Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Windows Failed Activity	Monitors failed activity from Windows logs	30	50

JUSTIFICATION: The average count of failed activities was 30 attempts. We set the alert trigger to 50 to capture any spikes in failed activity.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Windows Successful Login Alert	Alerts when a high amount of logins occur.	40	80

JUSTIFICATION: The average baseline was around 40 events, but fluctuated between 40-60 logins. We decided that the alert would trigger at 80 to avoid any normal activity to trigger a false negative. Employees of the organization or authentic users will be logging into the system and increased activity can vary.

Alerts—Windows

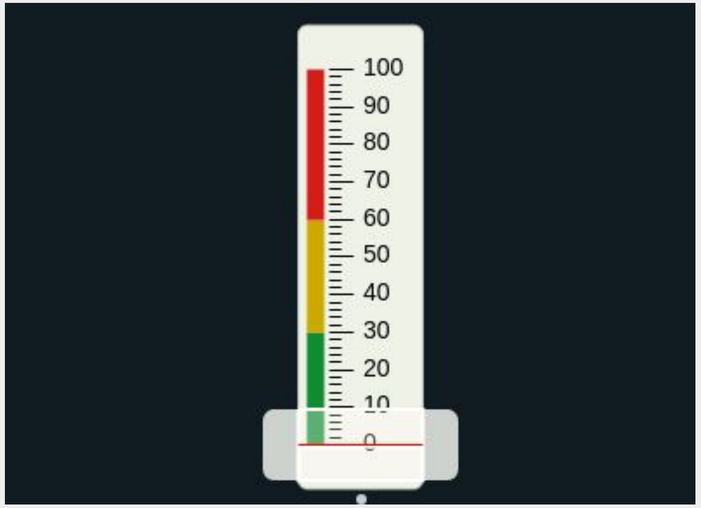
Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Hourly Windows Account Deletion	Alerts when a high amount of Windows accounts are deleted	40	60

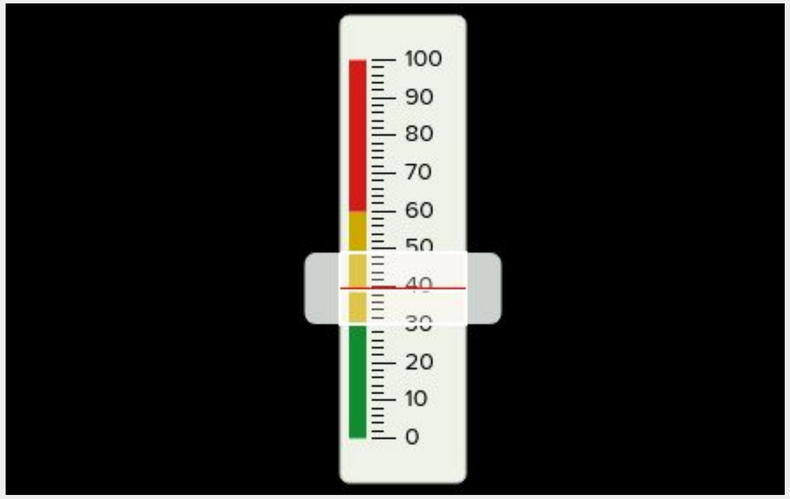
JUSTIFICATION: The alert baseline was 40. We chose 60 as the trigger to avoid any false negatives and to alert when a high amount of accounts are being deleted. A large amount of Windows accounts being removed would be flagged as abnormal.

Dashboards—Windows

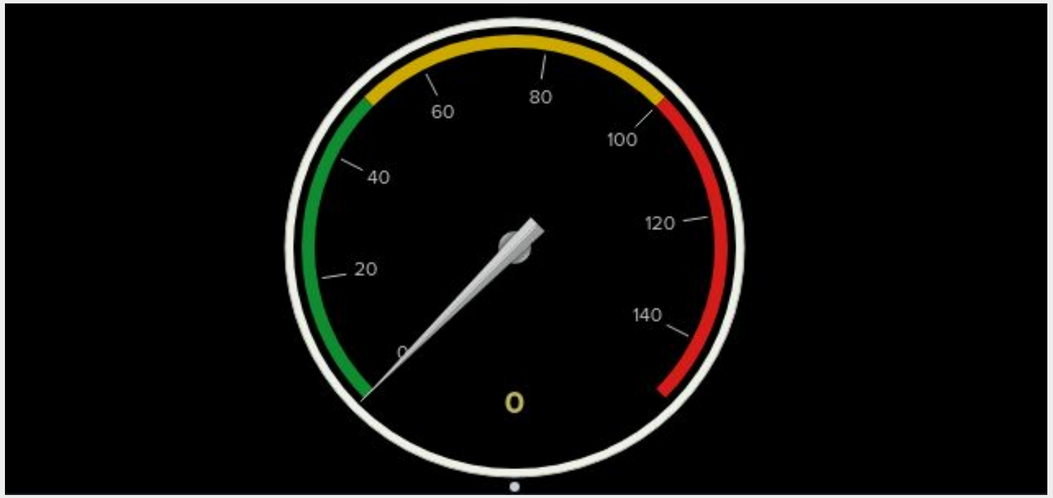
Alert - Failed Windows Activity



Alert - Account Deletion



Alert - Successful Login



Critical/High Severity Monitoring

Dashboards—Windows

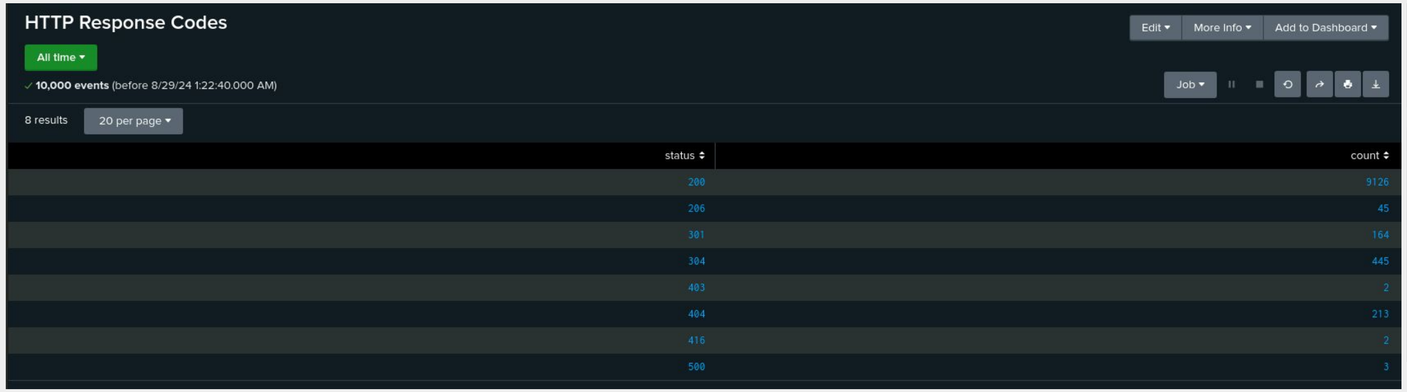
Apache Logs

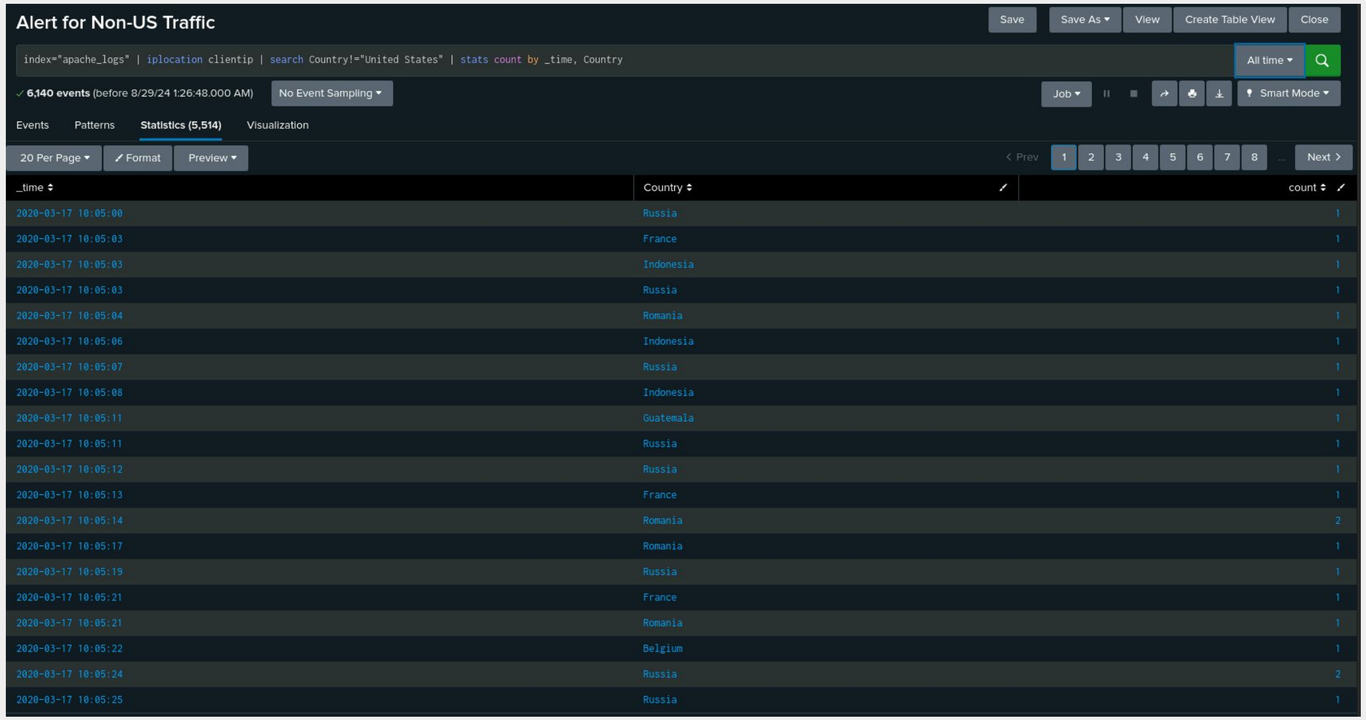
Reports—Apache

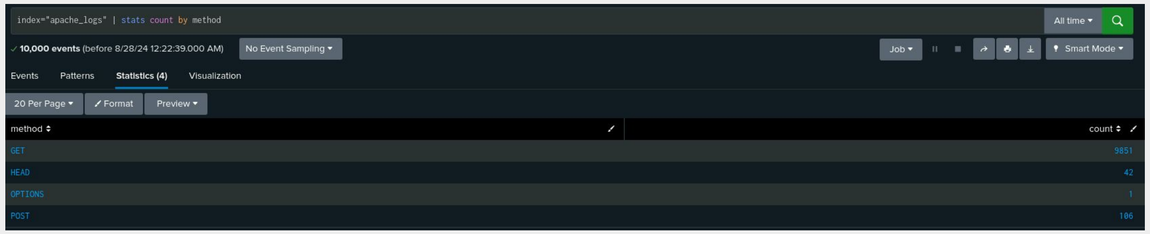
Designed the following reports:

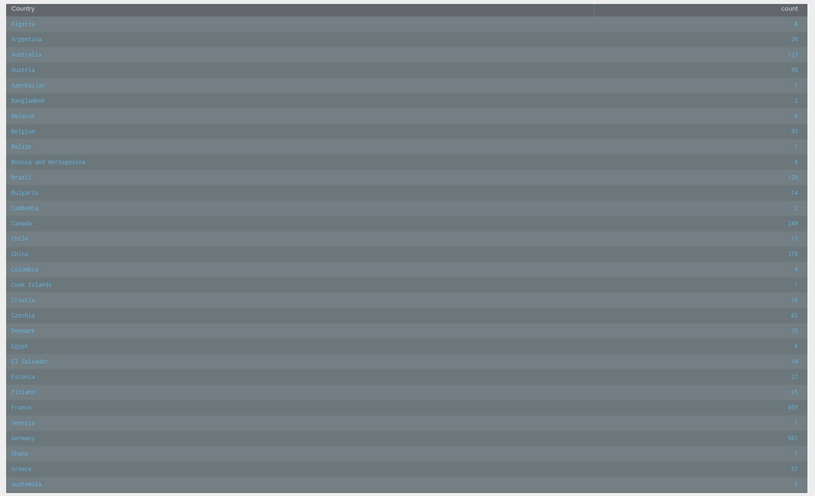
Report Name	Report Description
HTTP Methods Report	Tracks different HTTP requests made to server
Referrer Domains	A List of the top 10 domains referring traffic to the server
HTTP Response Report	Lists all HTTP Response codes returned by the server

Images of Reports—Apache









Alerts—Apache

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
Non-US Alert	Monitors high volume of traffic coming from countries other than the United States	30/hr	50/hr

JUSTIFICATION: The average baseline for server interactions from international countries aside from the United States was 20-30 per hour with a few notable exceptions (France, Germany, Sweden, India, China) We set the alert to trigger at 50 attempts per hour to see any spikes in international activity which would indicate an attack by international bad actors while still allowing for small spikes in activity internationally, without triggering false alerts too easily.

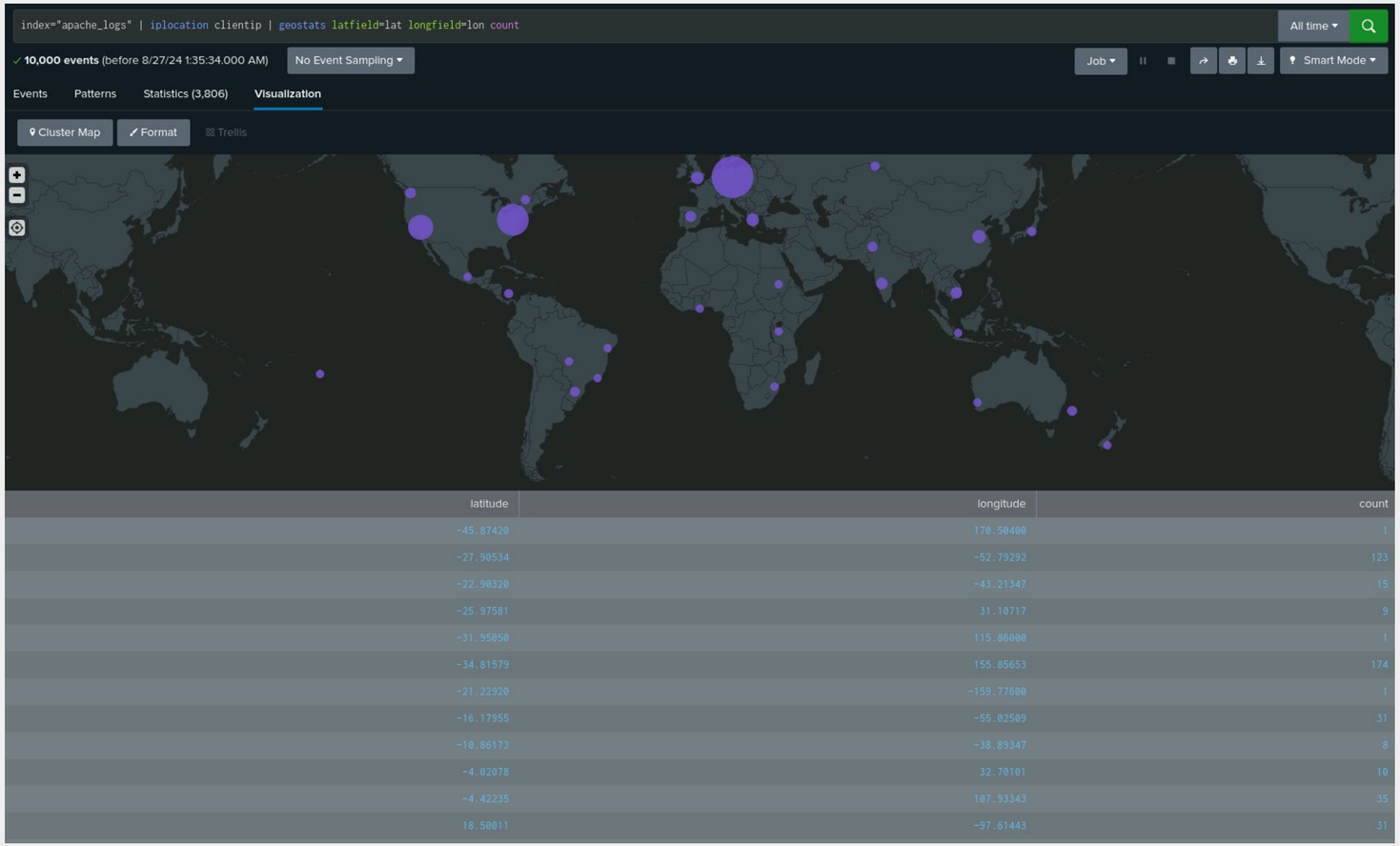
Alerts—Apache

Designed the following alerts:

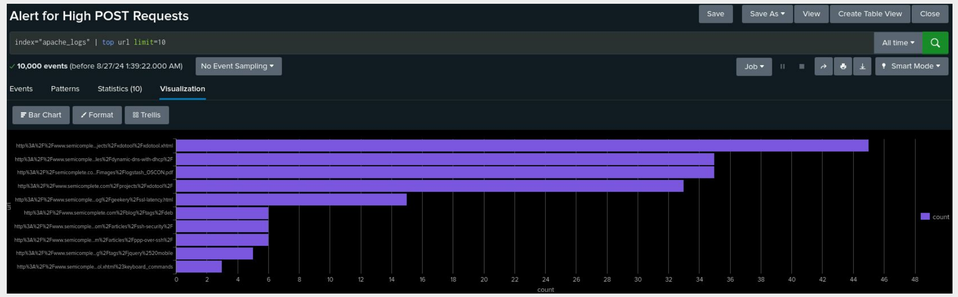
Alert Name	Alert Description	Alert Baseline	Alert Threshold
HTTP POST Alert	Tracks volume of HTTP POST Requests	2-6 / hr	30 / hr

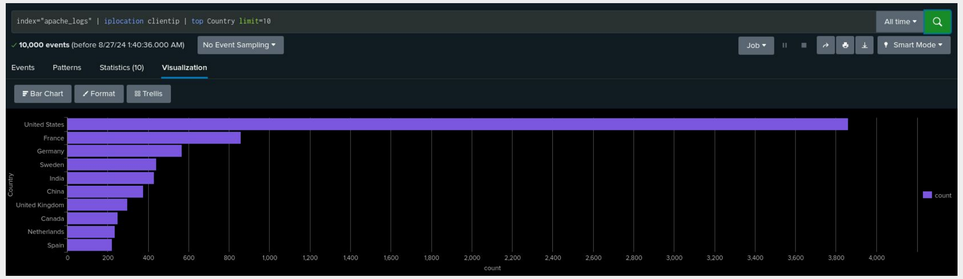
JUSTIFICATION: POST requests are used to submit data to the server, we set the alert at 5 times the baseline to allow a threshold for spikes in normal activity as we found the deviation from the baseline of 2 to be 4 requests, while there were routine spikes in normal data of 10-12 spikes. The high threshold will allow for deviation from the baseline while indicating for potential attacks using malicious uploading such as targeted data submissions or data exploitations involving upload attacks.

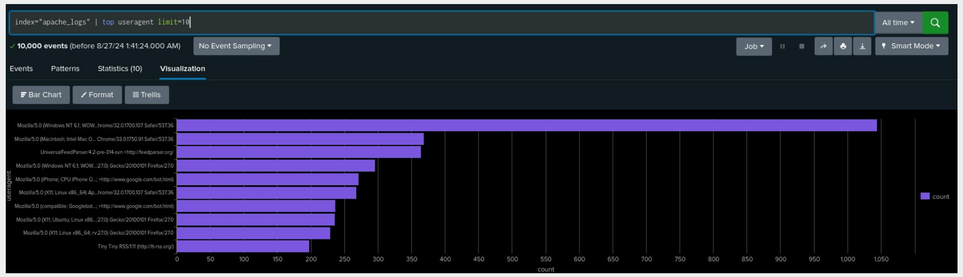
Dashboards—Apache



latitude	longitude	count
-45.87420	170.50400	1
-27.90534	-52.79292	123
-22.90320	-43.21347	15
-25.97581	31.10717	9
-31.95050	115.86000	1
-34.81579	155.85653	174
-21.22920	-159.77600	1
-16.17955	-55.02509	31
-10.86173	-38.89347	8
-4.02078	32.70101	10
-4.42235	107.93343	35
18.50011	-97.61443	31







Attack Analysis

Attack Summary—Windows

Upon analyzing the attack logs, we found the following details:

- From 1:00 to 3:00 AM, 2,128 events resulted in user accounts were locked out.
- From 9:00 to 11:00 AM, 1,811 events of attempted password resets were recorded.
- User activity from users “user_a” and “user_k” increased during the attacks.
- 1,111 events were marked as high severity.

Attack Summary—Windows

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

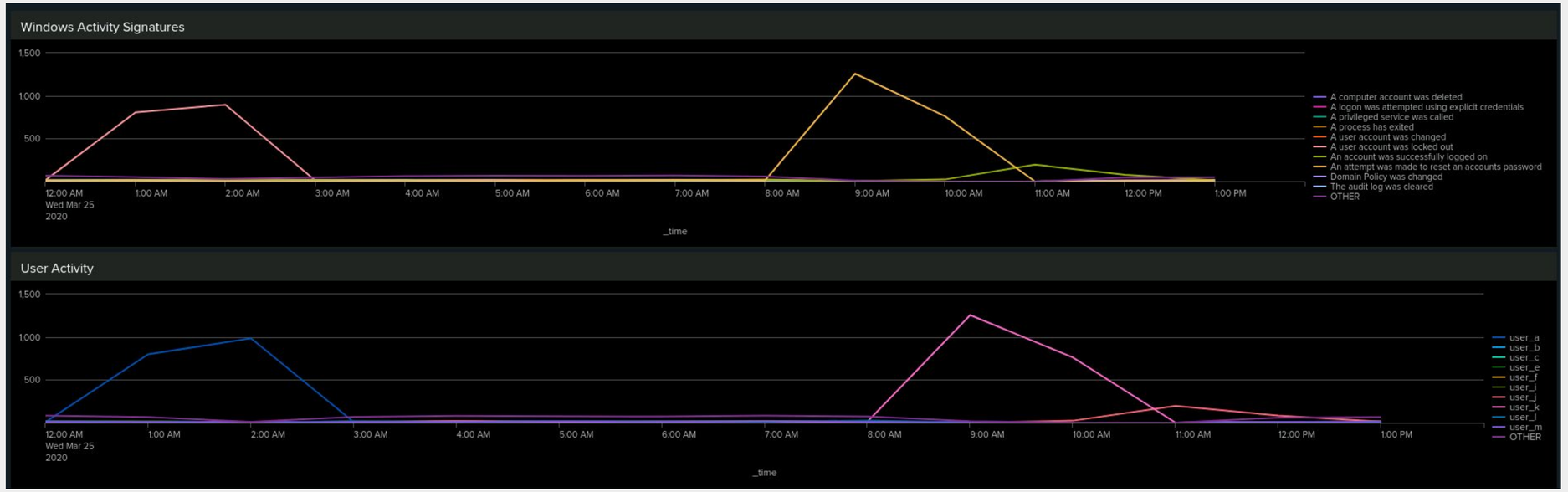
- The failed Windows activity alert triggered during user lockouts and attempted password resets. The attacks exceeded the threshold over 35, prompting the alert.
- The successful login activity alert would’ve triggered at 11 AM, when 196 events were recorded.
- The account deletion alert didn’t trigger as the alert threshold were 60 events. We’ve adjusted the threshold down to 50 accordingly.

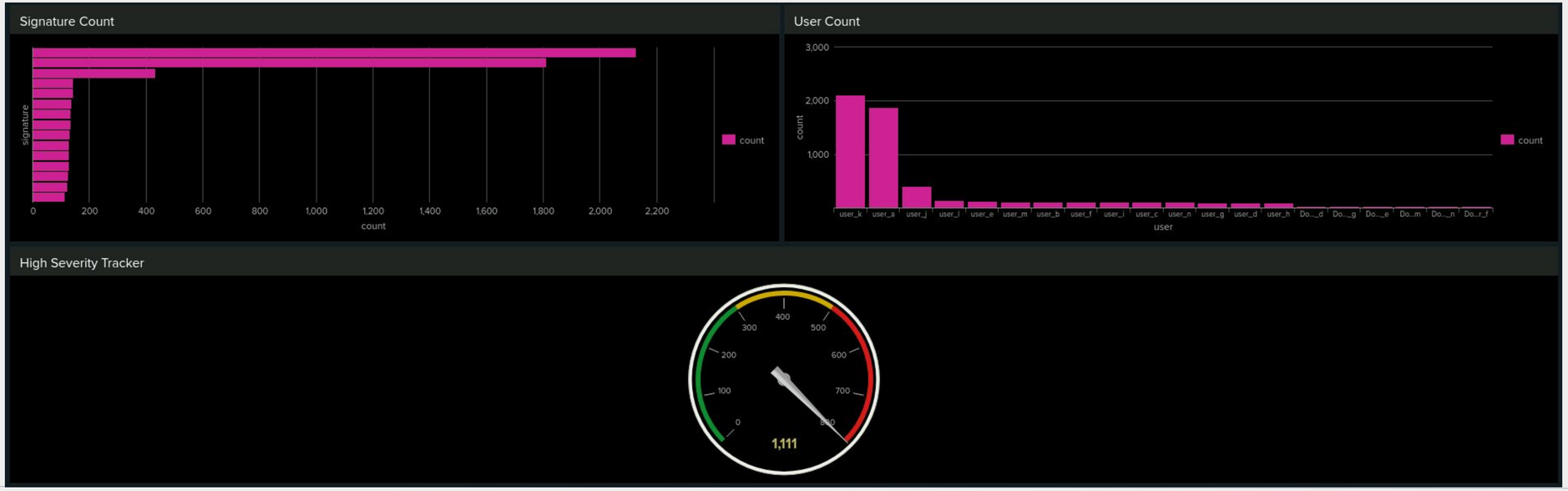
Attack Summary—Windows

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

- Both attacks involved brute-force attacks and credential stuffing.
- The first attack occurred from 1 AM to 3 AM with a spike of user account becoming locked out.
- The second attack occurred from 9 AM to 11 AM with attempts to reset account passwords.
- High activity from user_a and user_k were detected during the attacks.
- We believe JobeCorp attempted to obtain unauthorized access into the systems using these methods.

Screenshots of Attack Logs





Attack Summary—Apache

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

- Spike in GET requests to 9,851 from 5:00PM to 6:00PM and then a drop of to 3,157 suggesting the attack shifted focus from retrieving content to aggressive data submission
- Significant increase in POST requests at 7:30 PM to 8:30 PM from 2-6 average to nearly 1500, indicating a targeted data submission or exploitation attempt. Buildup of POST requests from 6:00PM to 7:30PM indicating an impending attack. Proper alert setup would have given early warning of these indicators.
- Spike in 404 errors from 213 to 679 indicating extensive probing for non-existent resources which shows attacker attempts to identify hidden files
- New referrer “logstash-metrics-sf-2012.10” emerged during attack, indicating it was a part of the attack vector.
- Overall traffic reduced, more focused attacks.
- Minimal server disruptions (500 and 403 errors) indicating the attack was not DDOS oriented, and was focused on probing and targeted actions
- Spike in specific URIs being accessed
- Dashboards did not provide any additional information that was not apparent from reports

Attack Summary—Apache`

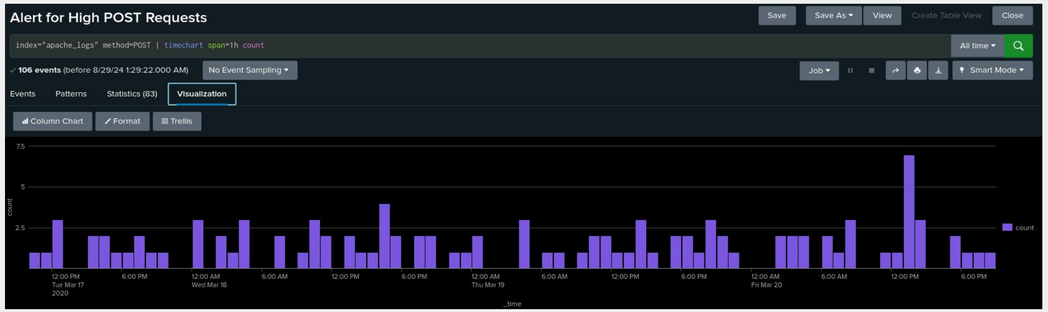
Summarize your findings from your alerts when analyzing the attack logs. Were the thresholds correct?

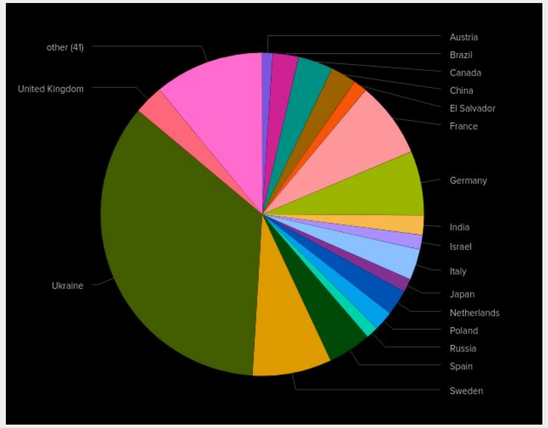
- Alert for high POST requests
  - The alert triggered correctly due to a significant spike in POST requests, with the count reaching nearly 1500 at 8PM
  - Threshold was set to 30 POST requests per hour, which was appropriate given the baseline of 2-6 requests per hour with spikes up to 20 requests per hour.
- Alert for International Activity
  - The alert triggered correctly due to a significant spike in activity from Ukraine, reaching its apex at 8PM.
  - Looking through the attack logs found significant spikes in Eastern USA which was not caught through the alert, which was an adjustment needing to be made, so we created a separate alert for Domestic activity spikes.

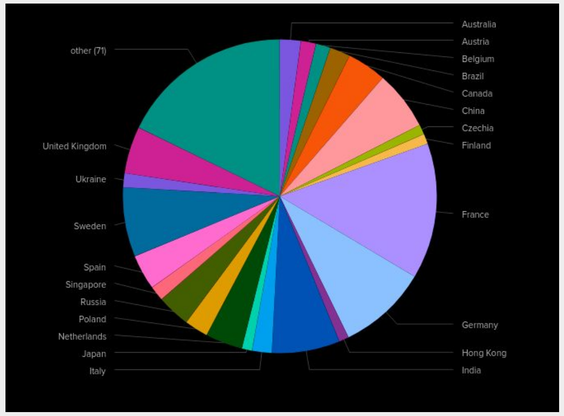
Attack Summary— Apache URIs

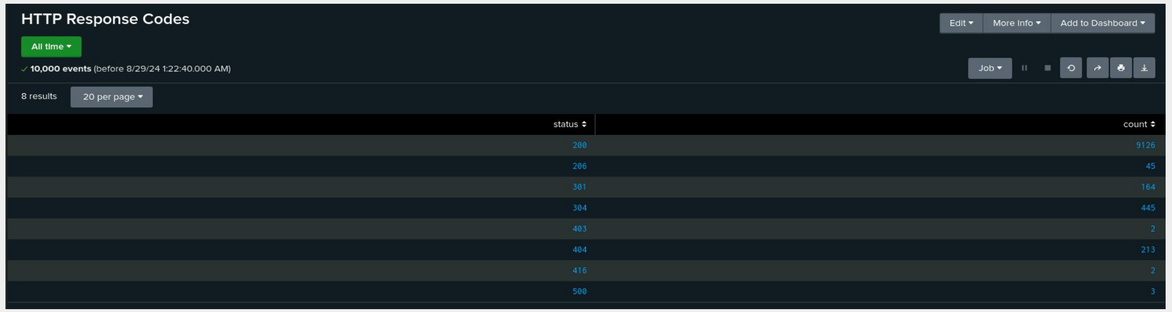
- Normal URI Access (Before the Attack)
  - /VSI_Company_Homepage.html: 807 accesses
  - Root Directory (/): 575 accesses
  - /contactus.html: 546 accesses
- Attack URI Access (During the Attack)
  - /VSI_Account_logon.php: 1323 accesses
  - /files/logstash/logstash-1.3.2-monolithic.jar: 638 accesses
  - /VSI_Company_Homepage.html: 235 accesses
- Key findings: URI account logon saw dramatic increase from 128 to 1323 during the attack, suggesting a targeted attempt to exploit the login page. logstash monolithic.jar file also saw a rise from 101 to 638 accesses, indicating the attacker was highly interested in attempting to exploit or extract this file. The logon page also noticed a spike at 6PM indicating an impending attack. Proper alert setup would have shown this as well.
- Decrease traffic from Homepage and Contact Us page, confirming the attack shifted from a general traffic attack towards a targeted resource attack.

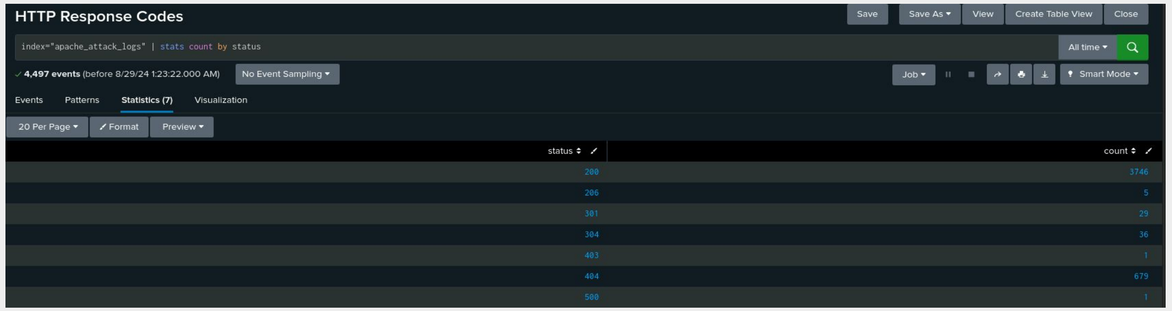
Screenshots of Attack Logs

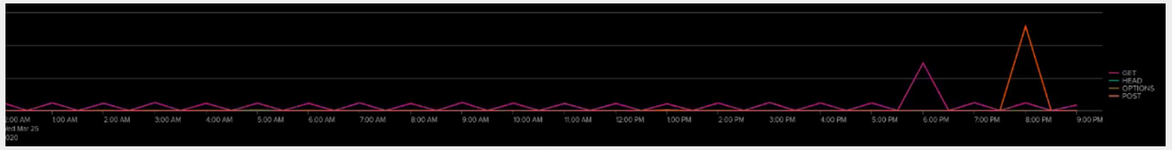












Summary and Future Mitigations

Project 3 Summary

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

Three main attacks took place, involving brute force attacks on the Windows servers to obtain user access and one targeted data submission attack on the Apache servers, in coordination with a botnet looking for backdoors into the system via Domain Traversal.

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

1. Implement Rate Limiting - Limit the amount of login attempts from specific IPs or users.
2. Lockout Policies - Set lockout policies for attempted access.
3. Password Policies - Enforce strong password policies to prevent any unauthorized logins.
4. MFA (Multi-Factor Authentication) - Require multi-factor authentication.
5. Denial of Service Protection - Use a DoS/DDoS protection software such as Cloudflare to prevent excess server requests.
6. Restrict Access - Restricting access to critical files like the monolithic.jar file to only authorized users or internal systems.
7. File Integrity Monitoring - Implement File Integrity monitoring to detect any unauthorized changes or access to sensitive files.
8. Apply a WAF (Web Application Firewall) and implement Geo-Blocking to block traffic from countries where no legitimate business is conducted or where attacks are likely to originate (such as Ukraine).
9. Fine-Tune alert thresholds and regularly review alerts and logs as we had some thresholds too high or too low initially and had to then adjust them. Early alert monitoring would’ve also shown the impending attack that spiked at 8PM, as there were indications of the Attacker gearing up for a larger attack, and lightly testing the servers for vulnerabilities.