# Defensive Security Project
by: Emyrca Feliciano Estrada

# Table of Contents

This document contains the following resources:

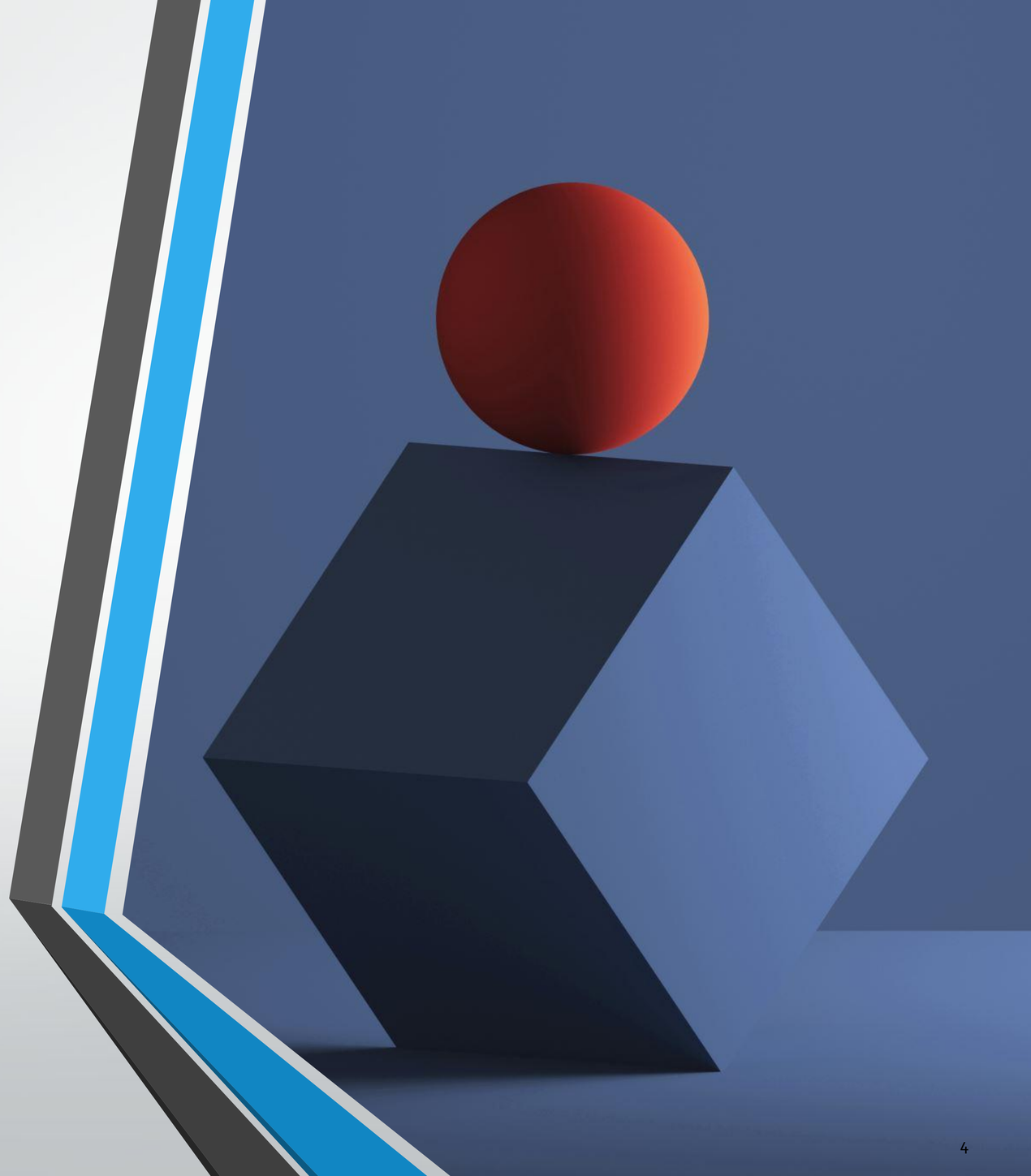
# Windows Environment

# SCENARIO

In this Scenario at Virtual Space Industries (VSI), our mission is to safeguard the integrity and security of VSI's digital assets against potential cyber threats. As Security Operations Center (SOC) analysts, our primary responsibility is to employ Splunk, a sophisticated log analysis tool, to fortify VSI's defenses against any attacks orchestrated by JobeCorp, a rival company rumored to be targeting VSI.

Our surveillance efforts focus on critical components of VSI's infrastructure, including the Apache Web Server, which hosts VSI's administrative webpage, and the Windows Operating System, vital for many back-end operations. Leveraging historical logs provided by the networking team, we establish baselines to discern normal patterns of system activity. With these insights, we craft comprehensive reports, set up proactive alerts to detect deviations from the norm, and design intuitive dashboards for real-time monitoring.

With the combined efforts of the SOC team and insights derived from Splunk, VSI is well-equipped to thwart any malicious endeavors from JobeCorp, safeguarding its reputation and ensuring continued success in the realm of virtual reality innovation.



# Logs Analyzed

## Windows Logs

- These logs document various activities such as system events, security audits, and system errors. They encompass application logs (which record events triggered by software applications), security logs (which track both successful and unsuccessful login attempts, as well as resource usage), and system logs (which capture events generated by components of the Windows system). These logs are integral to maintaining system integrity and security.

## Apache Logs

- These logs document the server's activities and the requests it handles. They consist of access logs (which capture all requests processed by the server) and error logs (which record all errors that occur while processing requests). These logs are crucial for monitoring server performance and troubleshooting issues.

# Windows Logs

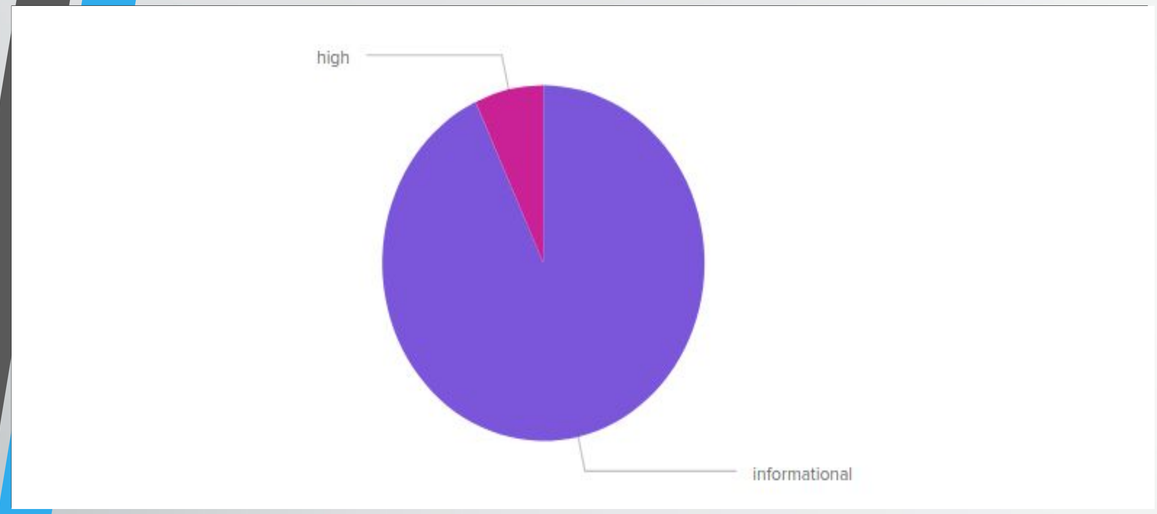
# Reports—Windows

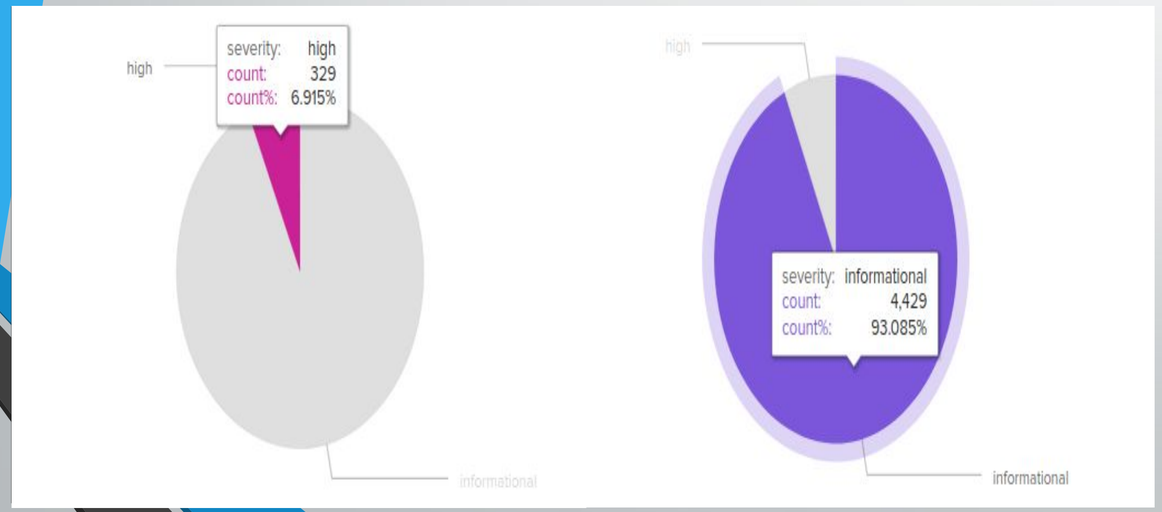
- Designed the following reports:

| Report Name | Report Description |
| --- | --- |
| **Windows Report Severity Levels** | A report that displays the severity levels, and the count and percentage of each. |
| **Windows Report Signatures** | A report with a table of signatures and associated signature IDs. |
| **Windows Report Success & Failure** | A report that provides a comparison between the success and failure of Windows activities. |

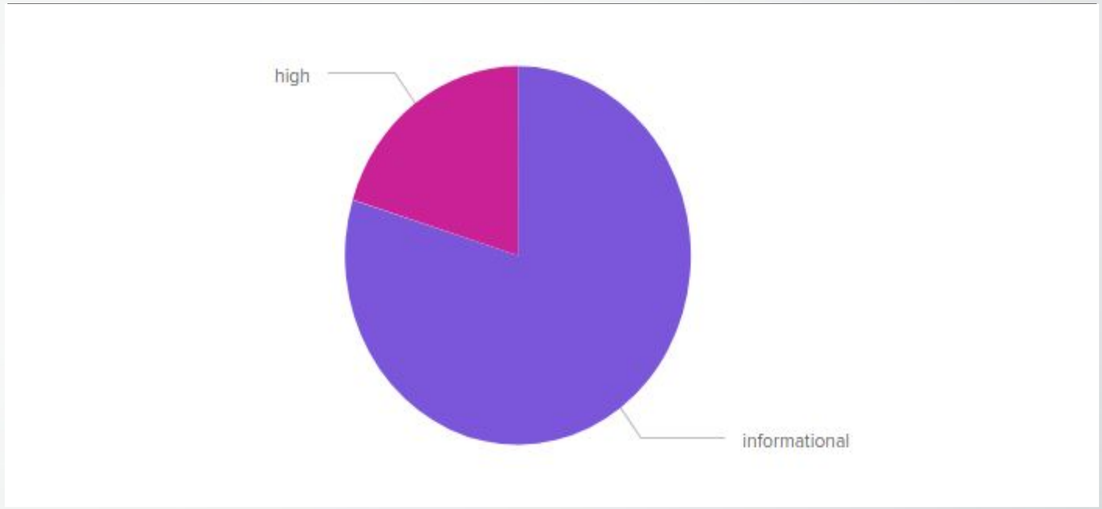
# Reports—Windows (Severity Levels)

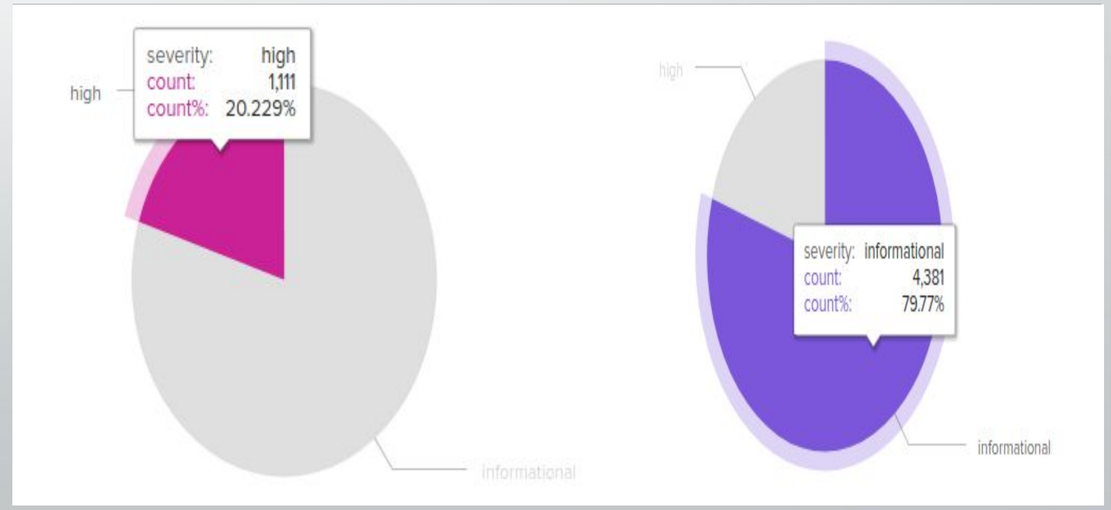
## Regular Report:




## Attack Report



# Reports—Windows (Signatures, Signature ID)

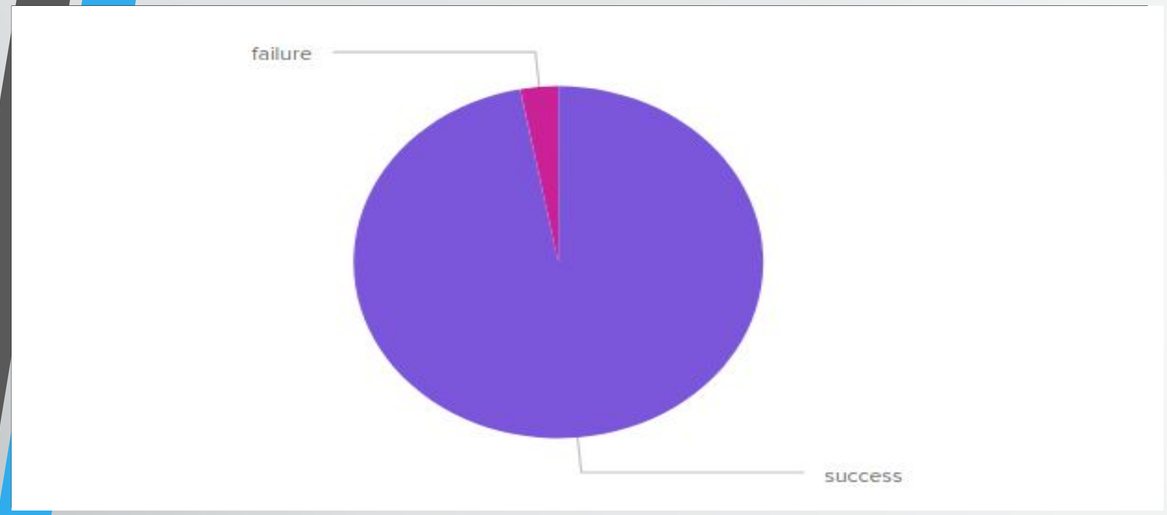
## Signatures

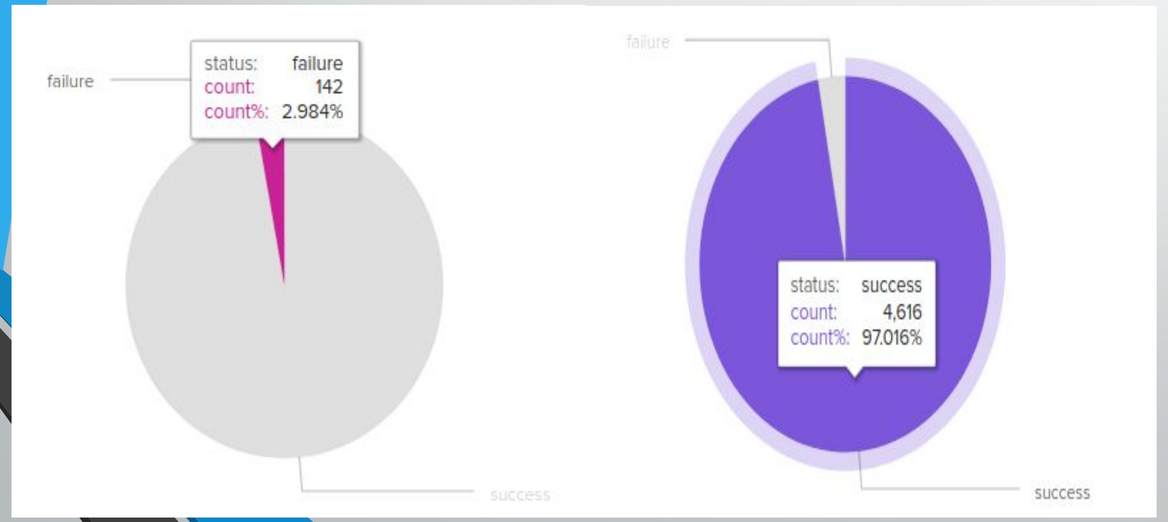
## Signature ID

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

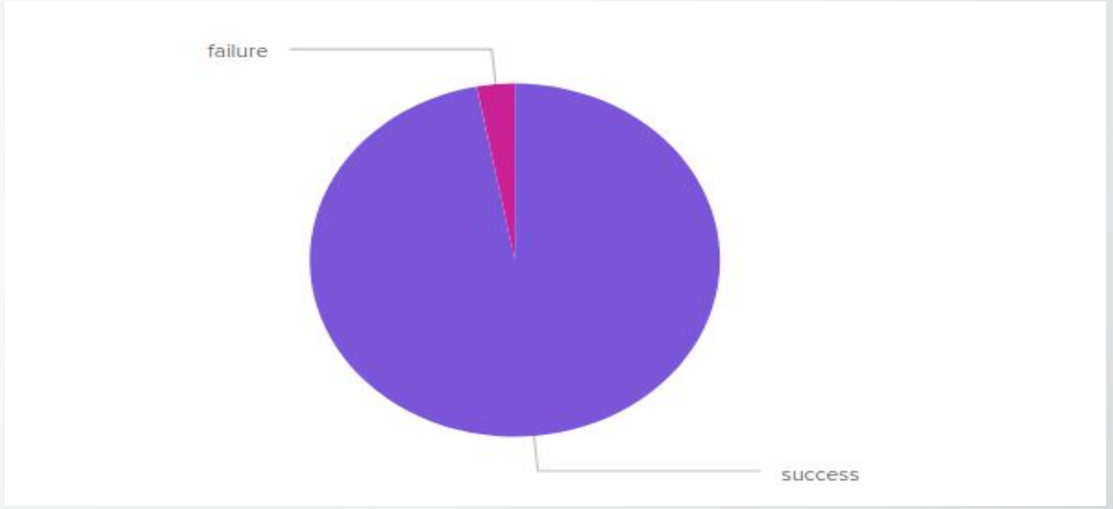
# Reports—Windows (Success & Failure)

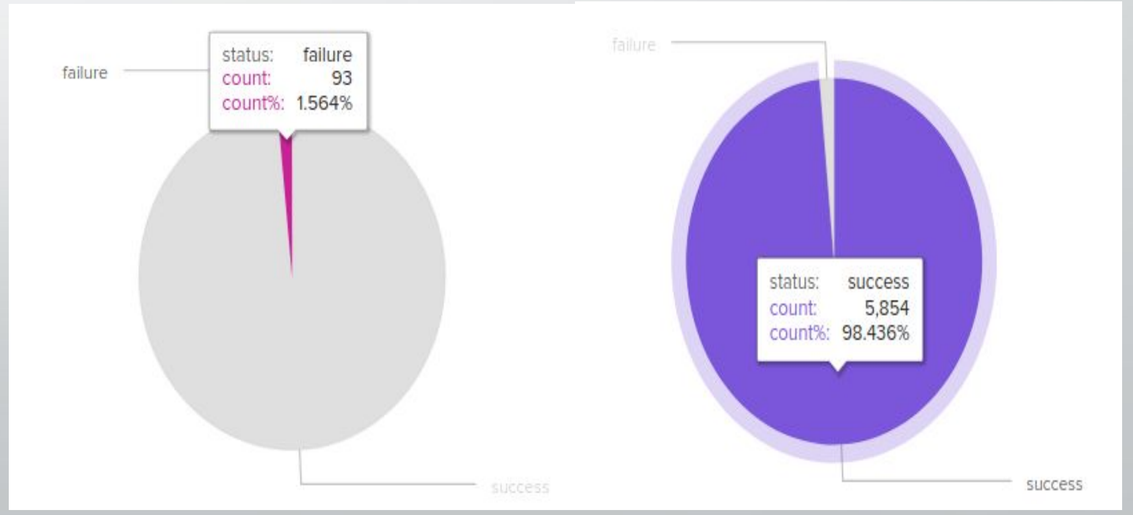
## Regular Report:




## Attack Report



# Alerts—Windows

- Designed the following Alerts:

| Alerts Name & Condition | Alerts Description |
| --- | --- |
| **Windows Alert Account Deletion**<br>Baseline: >35<br>Threshold: 1 Hour | Alert that's triggered when the threshold has been reached for the hourly count of the windows signature “a user account was deleted.” |
| **Windows Alert Failed Activities**<br>Baseline: >15<br>Threshold: 1 Hour | Alert that’s triggered when the threshold has been reached for the hourly level of failed Windows Activity. |
| **Windows Report Successful Logins**<br>Baseline: >25<br>Threshold: 1 Hour | Alert that’s triggered when the threshold has been reached for the hourly count of the windows signature “an account was successfully logged on.” |

# Alerts–Windows

- **Justification**

## Windows Alert Account Deletion

**Baseline: >15**
Establishes a benchmark for typical account management activities, aiding in the detection of deviations indicative of potential security breaches or insider threats.

**Threshold:  1 Hour**
If the threshold for account deletions is surpassed, it could indicate potential insider threats, such as disgruntled employees attempting to sabotage systems by removing accounts. Rapid detection is crucial to prevent unauthorized access and data breaches resulting from compromised credentials.

## Windows Alert Failed Activities

**Baseline: >110**
Defines the expected level of failed login attempts, serving as a reference point for identifying abnormal patterns that may signify unauthorized access attempts or system issues.

**Threshold: 1 Hour**
Exceeding the threshold for failed activities may indicate brute-force attacks or attempts to gain unauthorized access to systems. Prompt detection is essential to thwart potential breaches, prevent data loss, and safeguard sensitive information from malicious actors attempting to exploit vulnerabilities.

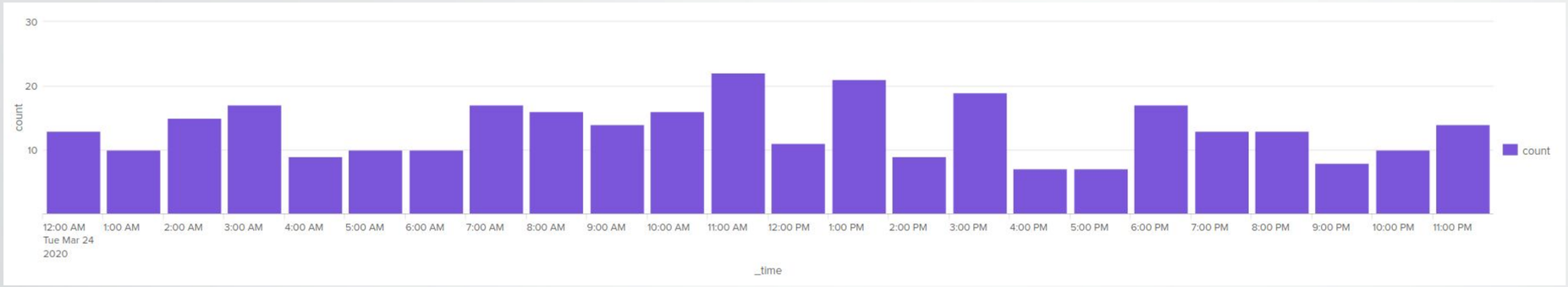
## Windows Report Successful Logins

**Baseline: >110**
Sets a standard for the volume of successful login events, facilitating the detection of anomalies such as unusual login patterns or suspicious access attempts.

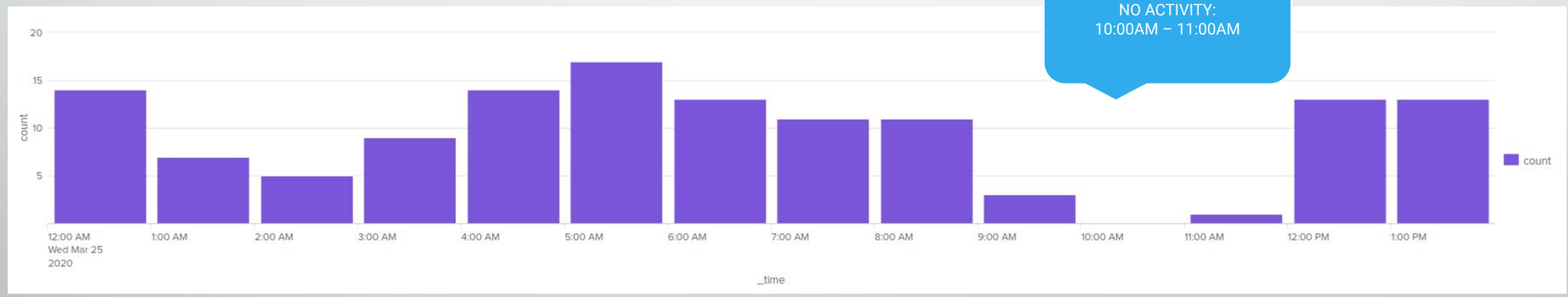
**Threshold: 1 Hour**
If the threshold for successful logins is exceeded, it could indicate unauthorized access attempts by malicious actors who have successfully obtained valid credentials or exploited vulnerabilities. Timely detection enables swift response measures to mitigate risks, prevent further unauthorized access, and protect sensitive data from unauthorized disclosure or manipulation.

# Alerts—Windows (Account Deletion)

## Regular Alerts

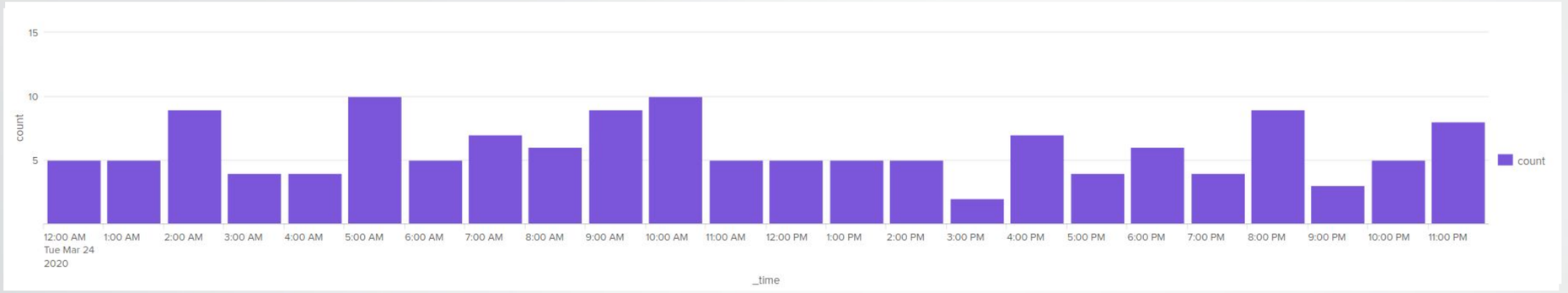



## Attack Alerts

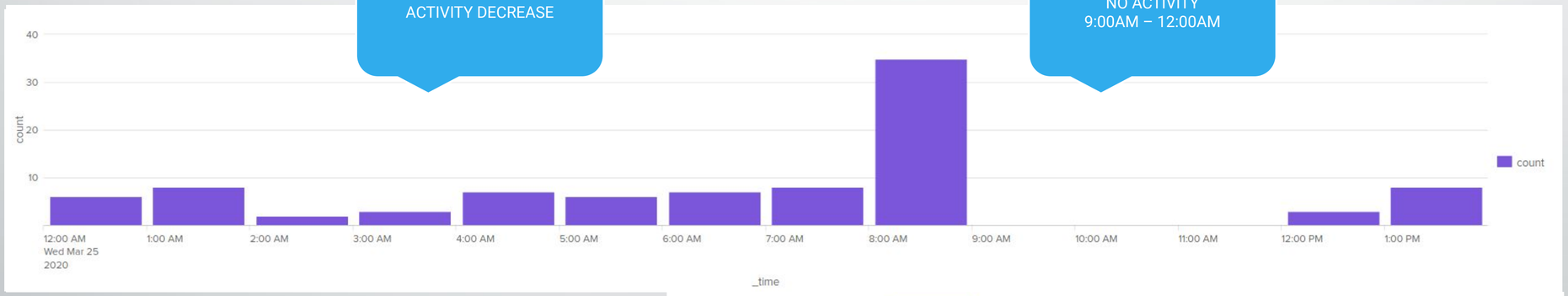


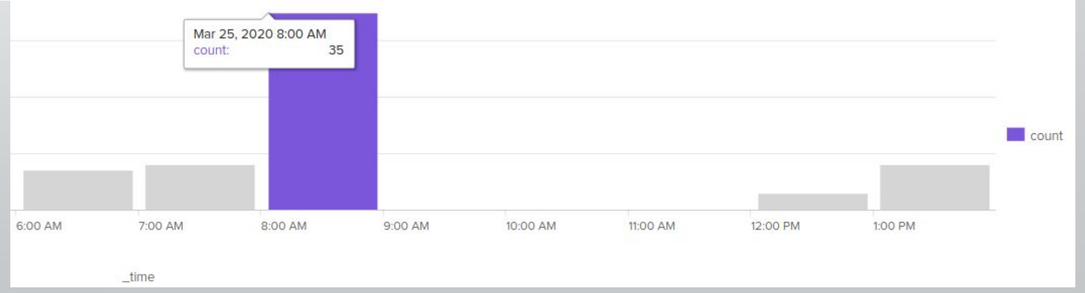
# Alerts—Windows (Failed Activities)

## Regular Alerts



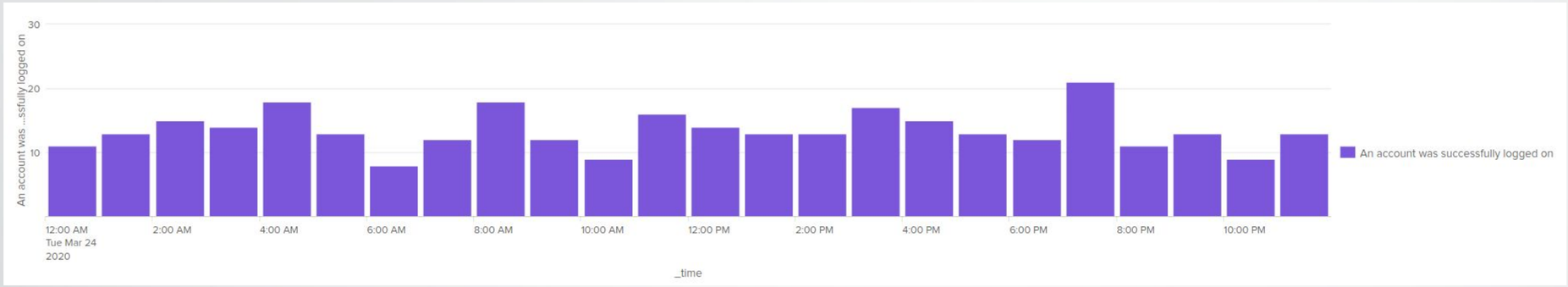

## Attack Alerts



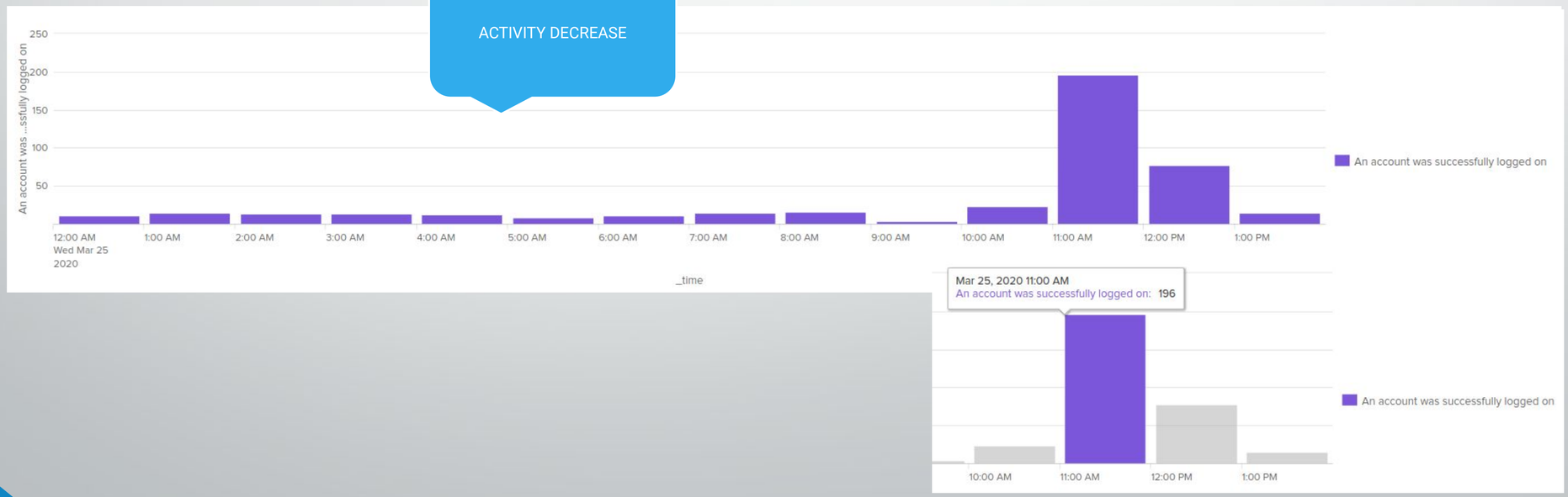



# Alerts—Windows (Successful Logins)

## Regular Alerts



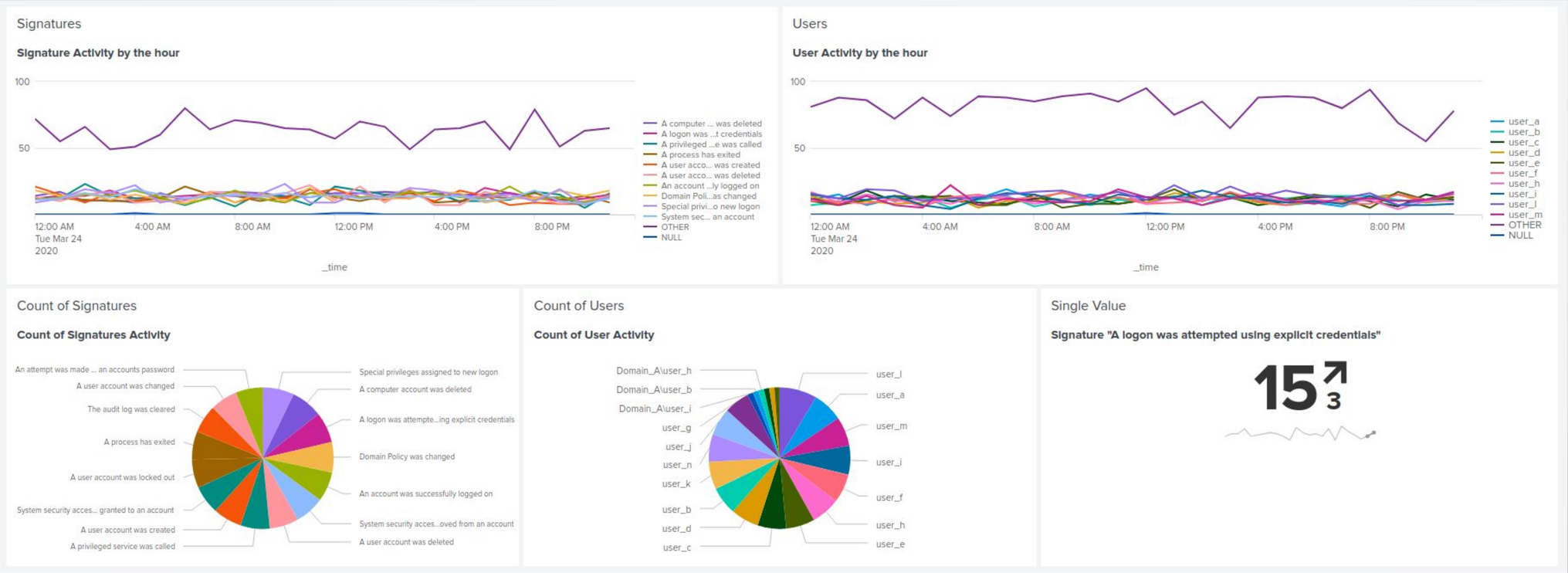

## Attack Alerts



# Windows Dashboards

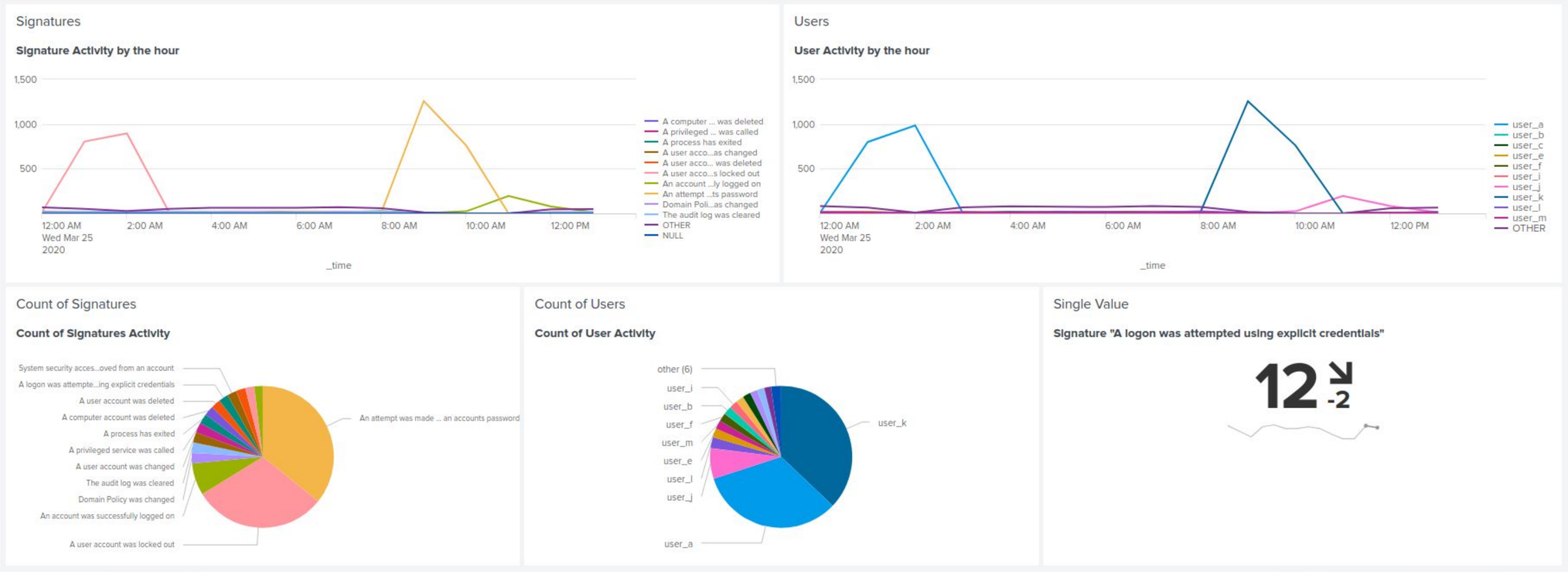
# Regular Dashboards—Windows

## Windows Server Monitoring



# Attack Dashboards—Windows

## Windows Server Monitoring Attack!



# Windows Attack Analysis

# Attack Report Summary—Windows

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

- ✔ Analysis of the attack logs indicates a spike in high **severity levels**, signaling heightened concerns regarding system integrity and security. This surge in high severity events implies a potential significant threat to the system's stability and functionality.

- ✔ Conversely, there has been a decline in the occurrence of **failed activities** within the attack logs, potentially indicating successful unauthorized access or activities.

- ✔ The correlation between increased **successful activities** and diminished **failure activities** rates suggests a potential security breach. These observations underscore the critical imperative for ongoing monitoring and the implementation of robust security measures to safeguard against such threats.

# Attack Alert Summary—Windows

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

- ✔ The alert for **failed activity** was initiated at 08:00 on March 3, 2020, triggered by a significant surge in failed activities. The quantity of failed activities recorded during this period markedly exceeded that of any other hour, signaling a potential security vulnerability.

- ✔ Similarly, the alert for **successful logins** was activated, affirming that the volume of successful logins remained within anticipated parameters on March 25, 2020, totaling 196 instances.

- ✔ Conversely, the alert for **deleted accounts** remained inactive, indicating that the number of deletions remained consistent with expected norms. Overall, the alert thresholds demonstrate accurate alignment, effectively reflecting the operational dynamics within the system.

- ✔ The thresholds for each alert were successfully established, however, continuous monitoring is imperative to ensure safety and to determine if any subsequent modifications are necessary.

# Attack Dashboard Summary—Windows

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

- ✔ The findings from the **Line chart** were corroborated by the **Pie chart** for signatures, notably indicating elevated counts for **"A user was locked out"** and **"An attempt was made to reset account password".**

- ✔ Similarly, the **Pie chart** for users reinforced the conclusions drawn from the **Line chart**, highlighting **user_a** and **user_k** for their substantial counts and significant proportions.

- ✔ Furthermore, the **Single Value chart** for the signature **"A logon was attempted using explicit credentials"** exhibited a decline in activity.

# Apache Logs

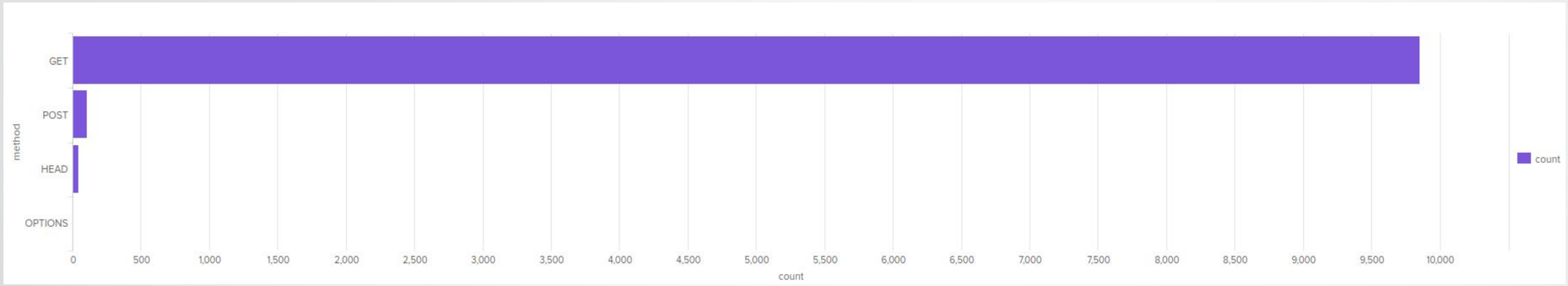
# Reports—Apache

- Designed the following reports:

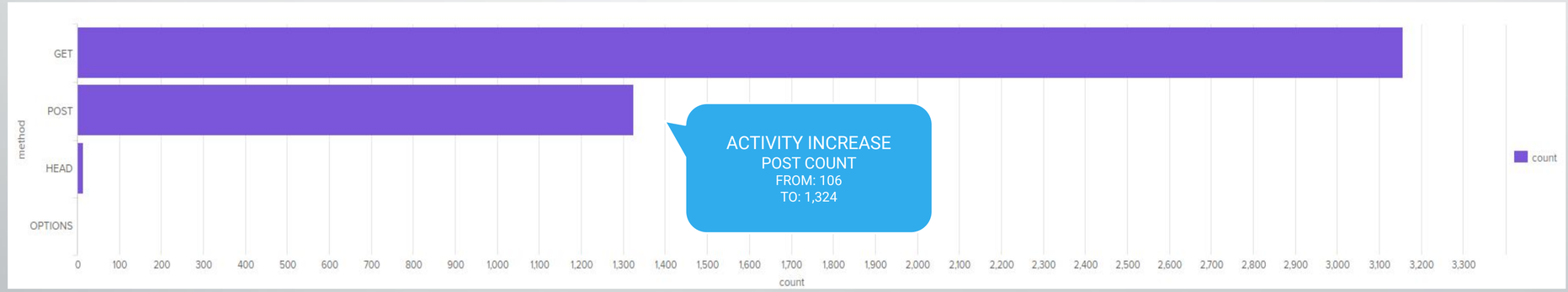
| Report Name | Report Description |
| --- | --- |
| **Apache Report HTTP Method** | A report that shows a table of the different HTTP methods (GET, POST, HEAD, etc.) |
| **Apache Report HTTP Response** | A report that shows the count of each HTTP response code. |
| **Apache Report Referer Domain** | A report that shows the top 10 domains that refer to VSI's website. |

# Report—Apache (HTTP Method)

## Regular Report

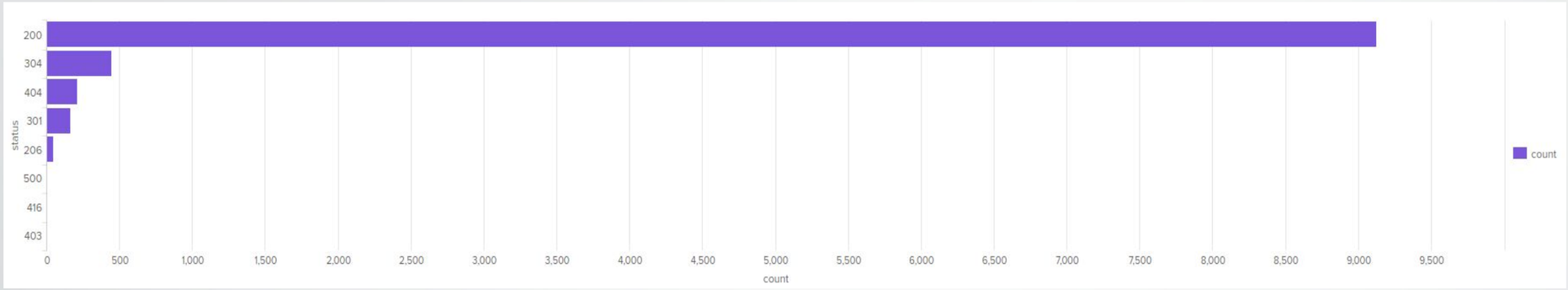



## Attack Report

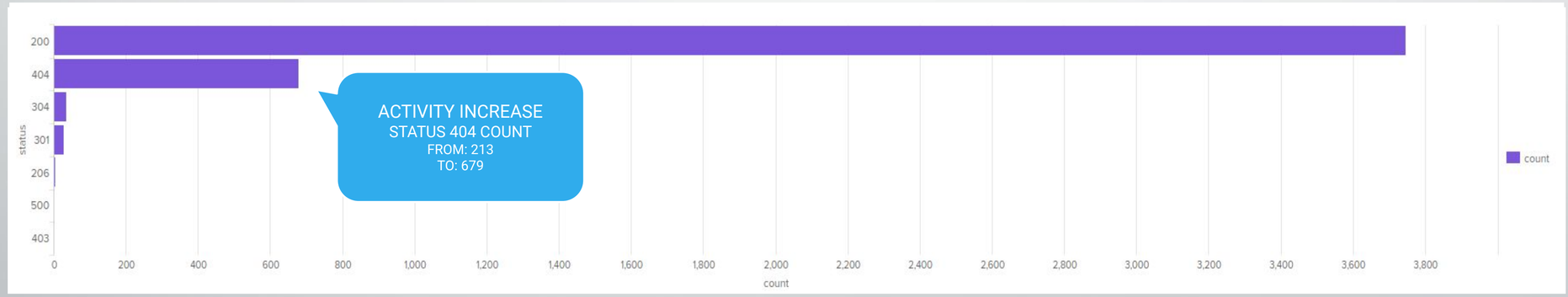


# Report—Apache (HTTP Response)

## Regular Report




## Attack Report



# Report—Apache (Referer Domain)

## TOP 10 Referer Domains

| referer_domain | count | percent |
|---|---|---|
| http://www.semicomplete.com | 3038 | 51.256960 |
| http://semicomplete.com | 2001 | 33.760756 |
| http://www.google.com | 123 | 2.075249 |
| https://www.google.com | 105 | 1.771554 |
| http://stackoverflow.com | 34 | 0.573646 |
| http://www.google.fr | 31 | 0.523030 |
| http://s-chassis.co.nz | 29 | 0.489286 |
| http://logstash.net | 28 | 0.472414 |
| http://www.google.es | 25 | 0.421799 |
| https://www.google.co.uk | 23 | 0.388055 |

# Alerts—Apache

- Designed the following Alerts:

| Alerts Name & Condition | Alerts Description |
| --- | --- |
| **Apache Alert HTTP POST Method**<br>Baseline: >15<br>Threshold: 1 Hour | Alert that's triggered when the threshold has been reached for the hourly count of the HTTP POST method. |
| **Apache Alert Hourly Activity NonUSA**<br>Baseline: >110<br>Threshold: 1 Hour | Alert that's triggered when the threshold has been reached for hourly activity from any country besides the United States. |

# Alerts—Apache

- **Justification**

## Apache Alert  HTTP POST Method

**Baseline: >15**
Provides a baseline for normal usage of the HTTP POST method, enabling the detection of abnormal spikes that may indicate attempts to exploit web application vulnerabilities or perform unauthorized actions.

**Threshold:  1 Hour**
Surpassing the threshold for HTTP POST method usage might indicate attempts to exploit web application vulnerabilities, such as injection attacks or data exfiltration attempts. Timely detection is crucial to prevent potential compromise of sensitive data, mitigate the impact of web application vulnerabilities, and safeguard against unauthorized access to critical systems or resources.

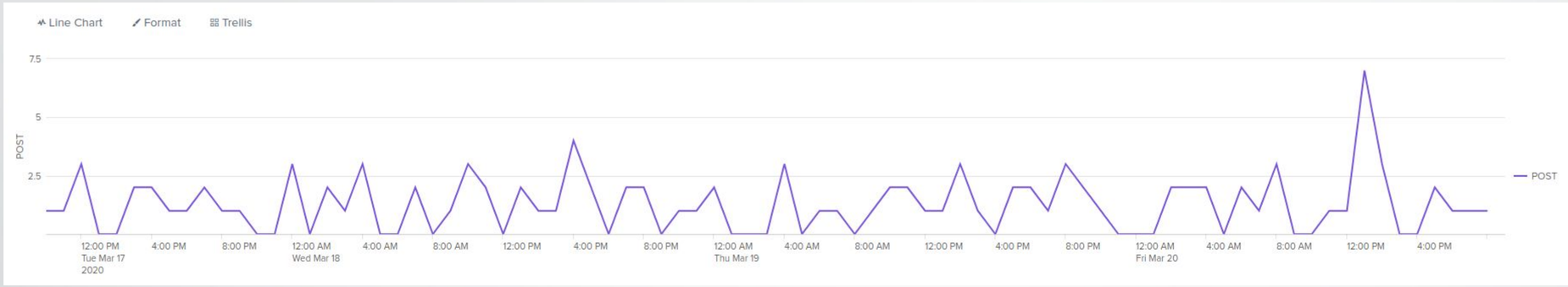
## Apache Alert Hourly Activity NonUSA

**Baseline: >110**
Establishes the typical volume of web traffic from non-US regions, serving as a basis for identifying deviations that may signal potential security threats or targeted attacks originating from international sources.

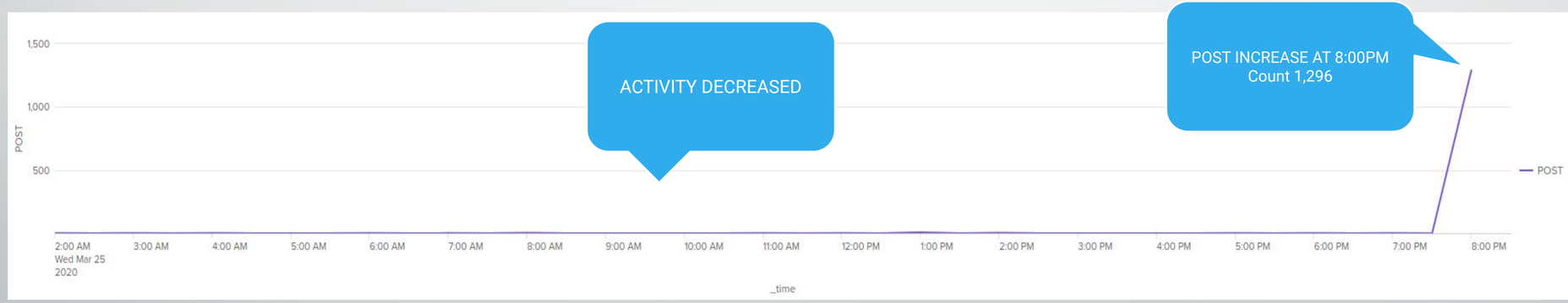
**Threshold: 1 Hour**
Exceeding the threshold for hourly activity from non-US regions could signal potential distributed denial-of-service (DDoS) attacks, brute-force attempts originating from foreign IP addresses, or targeted attacks from malicious actors located outside the USA. Timely detection enables proactive mitigation strategies to protect against service disruption, data breaches, and unauthorized access attempts originating from international sources.

# Alert—Apache (HTTP POST Method)

## Regular Report

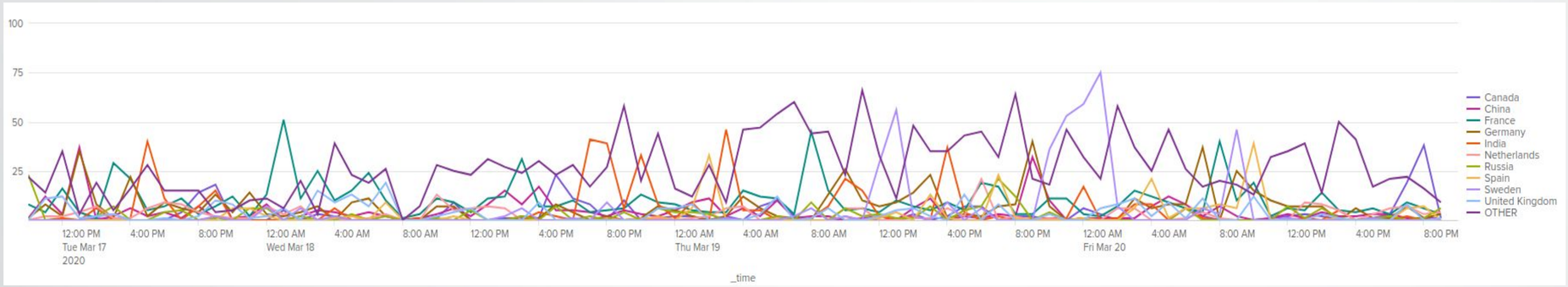



## Attack Report

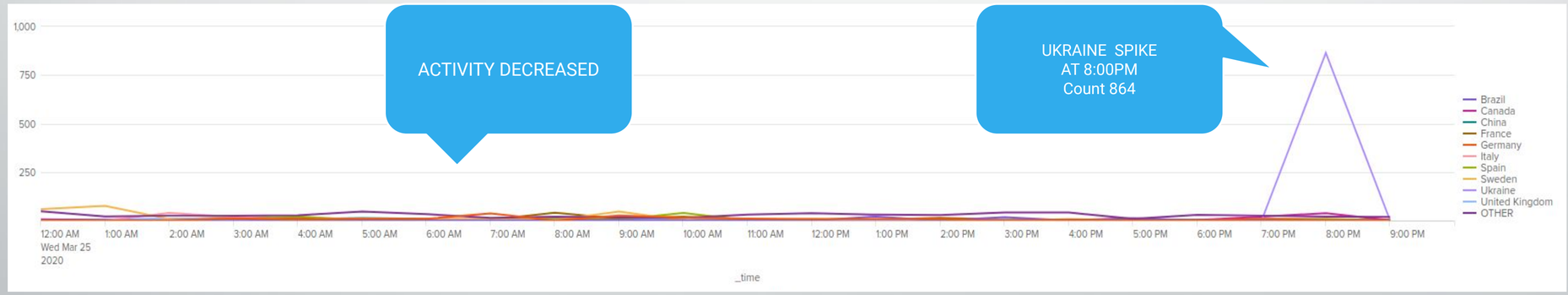


# Alert—Apache (HTTP POST Method)

## Regular Alert



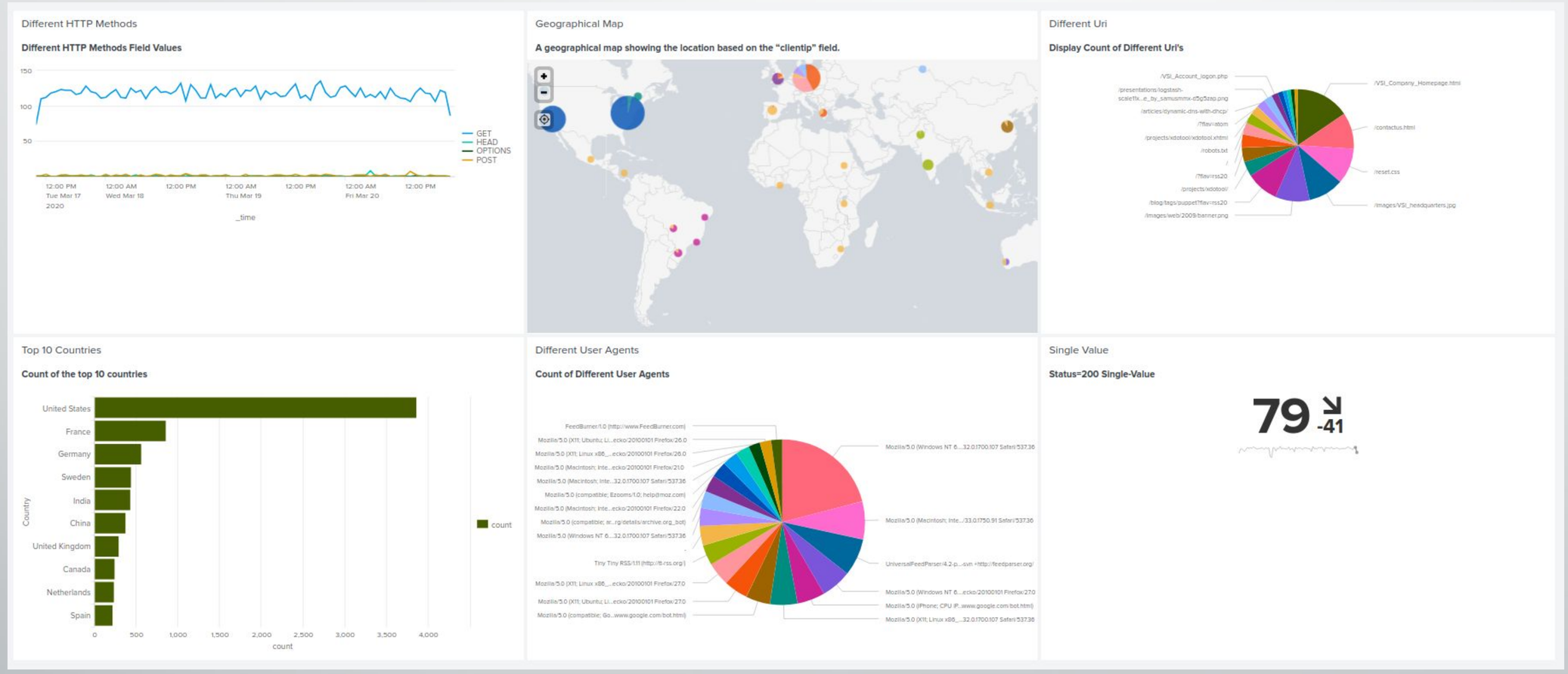

## Attack Alert



# Apache Dashboards

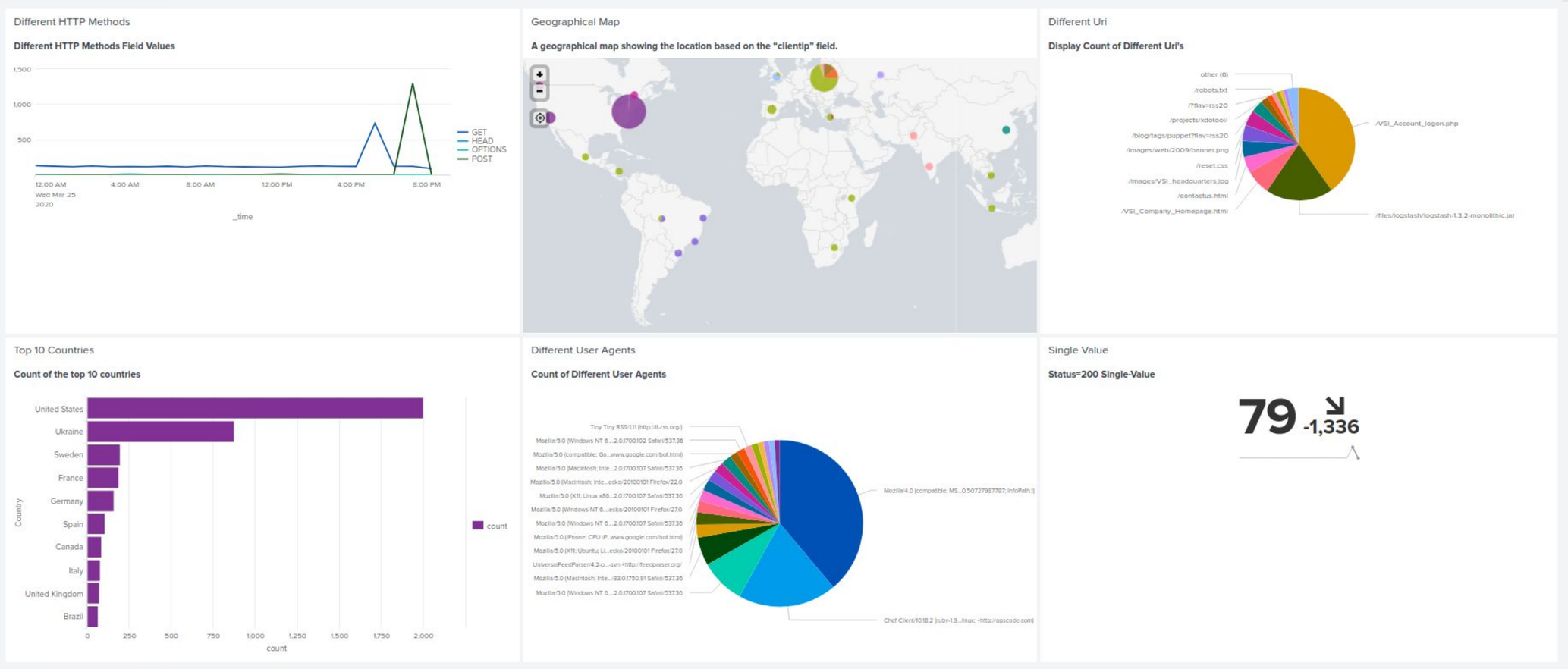
# Regular Dashboards—Apache

## Apache Web Server Monitoring



# Attack Dashboards—Apache

## Apache Web Server Monitoring Attack



# Apache Attack Analysis

# Attack Report Summary—Apache

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

- ✔ Suspicious changes associated with HTTP methods, particularly in relation to POST requests Increase.

- ✔ HTTP Response for 200 has around 8% decrease in events. As for the HTTP Response for 404 has an increase around 13% in events.

# Attack Alert Summary—Apache

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

- ✔ Our analysis of the attack logs reveals a notable decrease in the number of HTTP POST events over several hours, followed by a sudden spike in occurrences later on. Based on our observations, we believe the thresholds are appropriately configured, although continuous monitoring remains imperative to promptly address any emerging patterns or anomalies.
- ✔ An increased spike of events from Ukraine. The count shows as 864 at 8:00PM. Upon analyzing the attack logs and reviewing our current alerts, our findings suggest that the existing thresholds are appropriate. However, we remain committed to ongoing monitoring of Apache events and may consider adjusting the threshold values in the future if deemed necessary.

# Attack Dashboard Summary—Apache

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

- ✔ Our analysis of the attack logs reveals notable volumes of activity originating primarily from the United States, specifically New York with 547 activities and Washington DC with 668 activities. Additionally, significant activity is observed in Ukraine, particularly in Kiev with 440 activities and Kharkiv with 432 activities. These findings underscore the importance of maintaining vigilant monitoring and potentially adjusting thresholds to effectively manage and respond to emerging patterns of activity.

- ✔ The analysis of the current attack reveals a combination of GET and POST methods, with the attack timeline indicating GET requests occurring from 5:00 PM to 7:00 PM, followed by POST requests from 7:00 PM to 9:00 PM. Notably, the top method count during the attack corresponds to POST requests, totaling 1,296, surpassing GET requests which amounted to 729.

- ✔ The analysis of the current situation reveals that the URIs most affected are "/VSI/_Account_logon.php" with 1323 accesses and "/files/logstash-1.3.2-monolithic.jar" with 638 accesses. Given the high traffic on these URIs, the attacker could potentially be engaging in Brute Force Attack, attempting multiple logins by guessing username and password combinations on the "/VSI/_Account_logon.php" page. Additionally, the elevated activity may suggest a Denial of Service (DoS) Attack, aimed at inundating server resources on any page, potentially leading to server unavailability. Moreover, there's a risk of SQL Injection wherein malicious SQL statements are injected into entry fields, exploiting potential vulnerabilities if the login code isn't properly secured.

# Summary and Future Mitigations

# Project 3 Summary

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

  Upon reviewing the recent security incident, several key findings have emerged. Firstly, there has been a concerning increase in high severity events, suggesting the possibility of a serious attack taking place. Interestingly, this was coupled with a noticeable decrease in failed activities, implying potential unauthorized access. Our analysis also uncovered suspicious signatures, notably indicating attempts to reset account passwords and instances of user account lockouts. Notably, users 'user_a' and 'user_k' displayed unusually high levels of activity, warranting further investigation. Moreover, there was a significant uptick in both GET and POST requests, indicating heightened activity within the system. Additionally, changes in referrer domains were observed, hinting at a potential shift in traffic sources. Lastly, the rise in 404 (Not Found) HTTP responses raises concerns about attempts to access non-existent resources, potentially indicative of probing or reconnaissance efforts. These findings underscore the need for a comprehensive review of our security measures and prompt action to mitigate any potential risks to our systems and data.

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

  To safeguard VSI against potential future threats, it is imperative to establish a comprehensive security framework comprising continuous monitoring and stringent protocols. This entails implementing robust security measures and maintaining a proactive stance in adapting alert thresholds to reflect evolving threat landscapes. Regular updates to the repository of suspicious signatures and user profiles are essential to stay ahead of emerging attack vectors. Furthermore, vigilant monitoring of HTTP requests and response codes for anomalous patterns, along with tracking referrer domains and traffic origins, is crucial for identifying and mitigating potential threats. Equally important is the provision of comprehensive cybersecurity training to employees, empowering them with the knowledge and skills to recognize and respond effectively to security incidents. By adopting these measures, VSI can fortify its defenses and mitigate the risks posed by future cyber threats.

.