Defensive Security Project

Amany Seleem, Damanjeet Jassal,
Léa Di Federico, Nelson Ortiz, John Mallon

Table of Contents

This document contains the following resources:

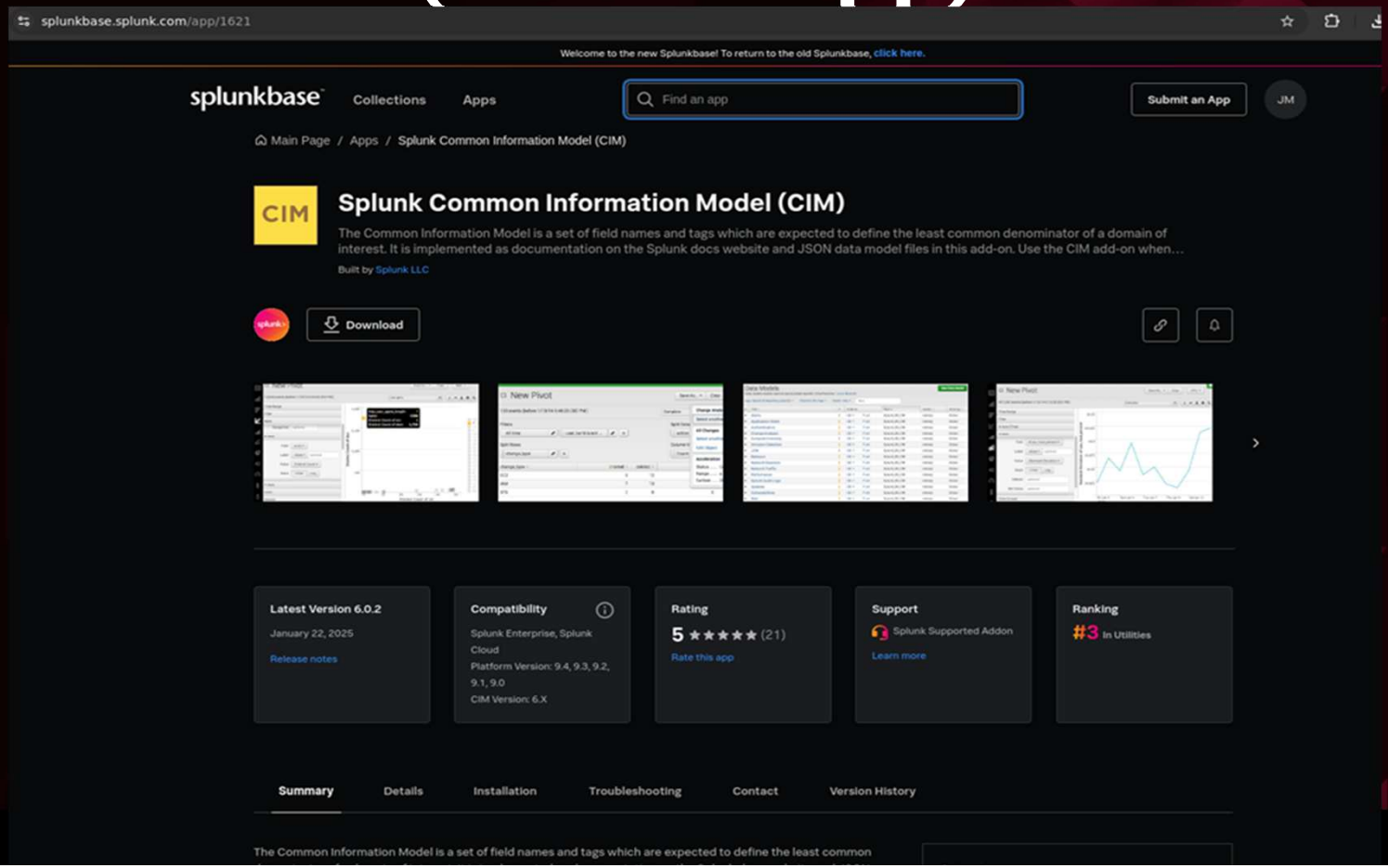
Monitoring Environment

Scenario

Playing the role of SOC analyst at a small company called Virtual Space Industries (VSI), which designs virtual-reality programs for businesses.

- VSI has heard rumors that a competitor, JobeCorp, may launch cyberattacks to disrupt VSI's business.
- As SOC analysts, we are tasked with using Splunk to monitor against potential attacks on the systems and applications.
- The VSI products that we have been tasked with monitoring include:
  - An administrative webpage: https://vsi-corporation.azurewebsites.net/
  - An Apache web server, which hosts this webpage
  - A Windows operating system, which runs many of VSI's back-end operations

Splunk Common Information Model (add-on app)



Splunk Common Information Model (CIM)

Key Features

Data Models: preconfigured data models

Normalization: helps normalize data from multiple source types

Search-time Schema: “schema-on-the-fly,” defining relationships in data

Performance options: indexes can be constrained to improve performance

Splunk Common Information Model (CIM)

Usage and Benefits

Data Consistency: helps break down log files into fields and event category tags

App Compatibility: many Splunk apps rely on CIM-compliant data for dashboards and reporting tools

Improved Analysis: includes tools for analysis, validation, and alerting

No Additional Indexing: a free add-on that does not perform additional indexing → no affect on licensing

Splunk Common Information Model (CIM)

Why use the CIM?
VSI could receive network traffic logs from various devices which uses different field names for similar data, for example Cisco routers, Juniper firewalls, and Palo Alto Networks appliances.

The Splunk CIM Add-On normalizes these fields to a common field name, for example src_ip. A security analyst is now able to search for all traffic from a specific IP address across all devices as follows:

```
| datamodel Network_Traffic search | where src_ip="192.168.1.100"
```

This search works across all device types, allowing the analyst to easily work with the data to create reports, dashboards, and alerts which improves efficiency and consistency.

Splunk Common Information Model (CIM)

How about in the event of an attack?

In the event of an attack, the CIM and Attack Analyzer work together to provide a powerful defense and analysis mechanism:

real-time detection	standardized field naming
automated analysis	enhanced detection capabilities
comprehensive threat analysis	rapid response

In addition, with contextual insights, contextual information is provided about the threat, helping analysts understand the nature and potential impact of the attack quickly.
Through the use of the CIM and Attack Analyzer during an attack, security teams can benefit from faster, more accurate threat detection and analysis, leading to more effective incident response and mitigation.

Logs Analyzed

1 Windows Logs

The Windows log contains important information on Windows events, including

application
security
system
forwarded
setup

2 Apache Logs

Apache is a Web Application Server and the logs contain

crucial information about web server activities, primarily divided into two types

1- Access Logs that record details of every HTTP request

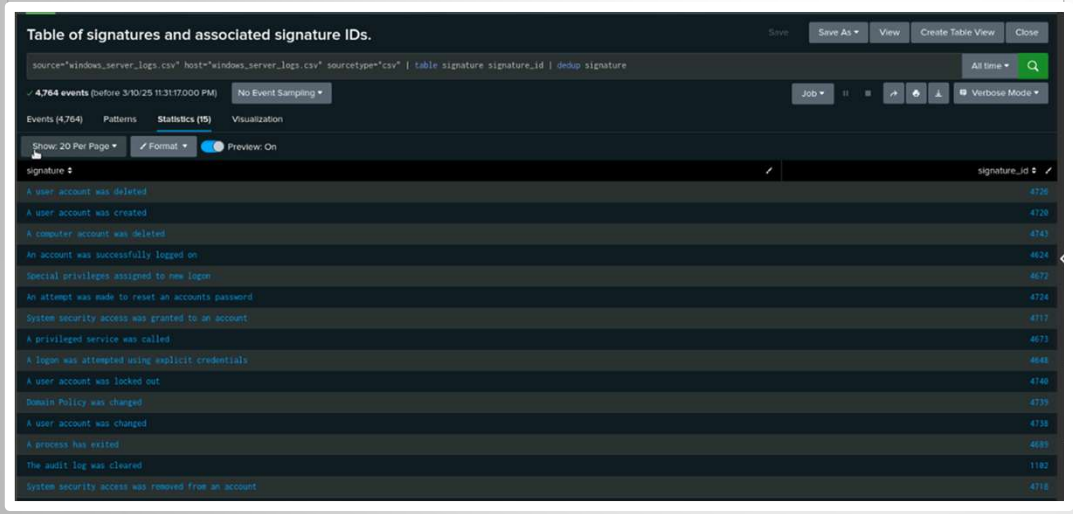
2- Error Logs contain information by the web server while processing requests. Error logs use a LogLevel directive to indicate the severity of an error

Windows Logs

Reports—Windows

Designed the following reports:

Report Name	Report Description
Table of signatures and associated signature IDs	A report featuring a table of signatures along with their associated signature IDs. This will allow VSI to generate reports that display the ID numbers, corresponding to specific signatures related to Windows activity.



Reports—Windows

Designed the following reports:

Report Name	Report Description
Severity levels including count and percentage	This will enable VSI to quickly assess the severity levels of the Windows logs being reviewed.

Reports—Windows

Designed the following reports:

Report Name	Report Description
A comparison between the success and failure of Windows activities.	A report analyzing the success and failure rates of Windows tasks. This will help VSI identify if there is an unusual number of failed activities on their server, potentially indicating suspicious behavior.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
VSI of Suspicious Activity	An alert that is triggered once the specified threshold has been reached.	6	12

JUSTIFICATION: The average is 6, with a maximum of 10 failures. A threshold of 12 would be reasonable to minimize false positives and reduce alert fatigue.

Alerts—Windows

Designed the following alerts:

Alert Name	Alert Description	Alert Baseline	Alert Threshold
An account was successfully logged on	An alert to trigger once the defined threshold for this count has been reached.	13	23

JUSTIFICATION: The average is 13, with a maximum of 21 successful logins. A threshold of 23 would be reasonable, and any number exceeding 23 should be considered suspicious.

Alerts—Windows

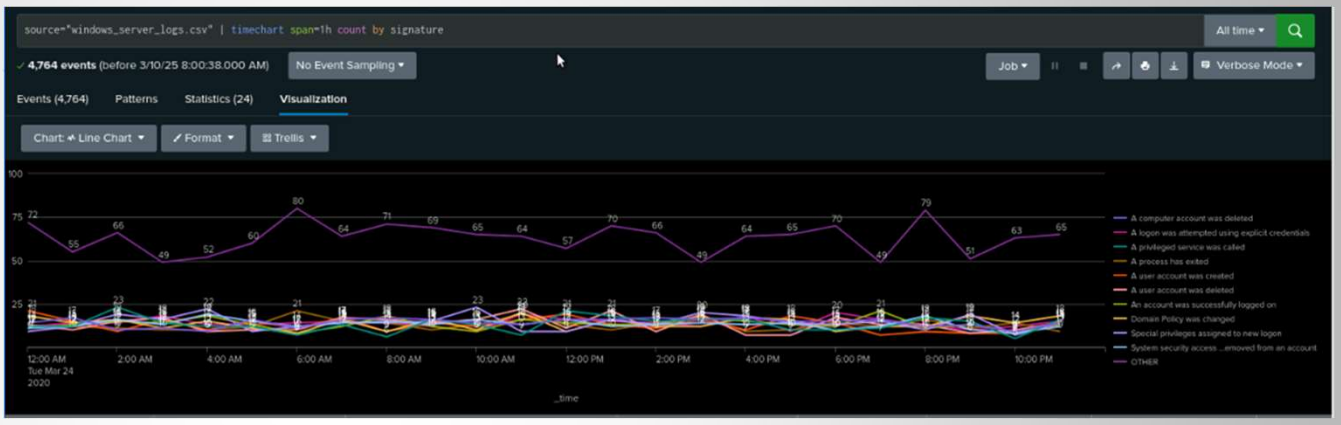
Designed the following alerts:

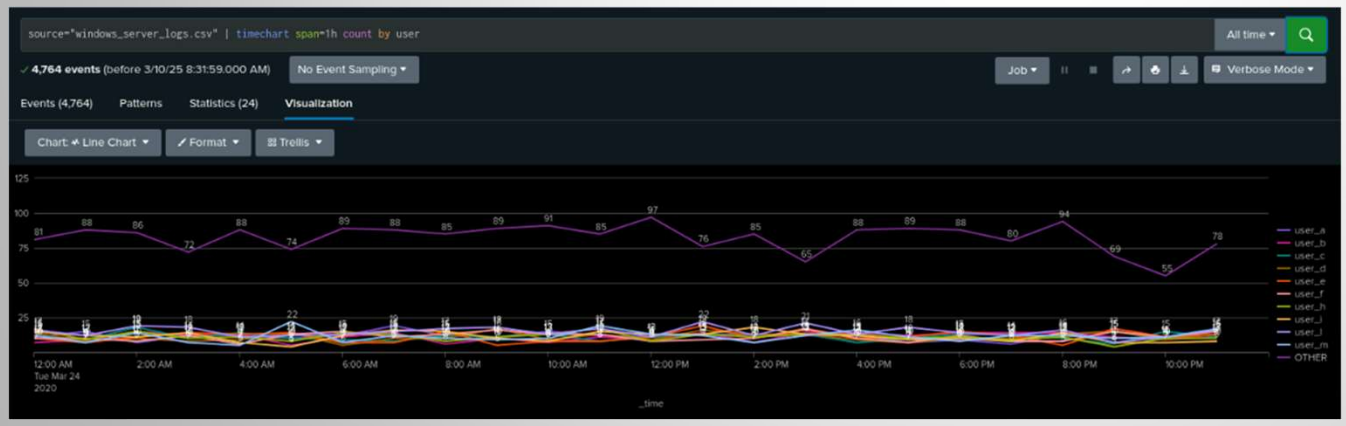
Alert Name	Alert Description	Alert Baseline	Alert Threshold
"A user account was deleted." Alert.	The alert based on the corresponding signature ID, as the signature name sometimes changes when the Windows system updates.	13	23

JUSTIFICATION: The maximum number of user accounts deleted was 22, with an average of 13. A threshold of 23 would be appropriate to allow for some flexibility while helping to detect any unusual spikes in activity without causing unnecessary alerts.

Dashboards—Windows

Dashboard Analysis for Time Chart of Signatures

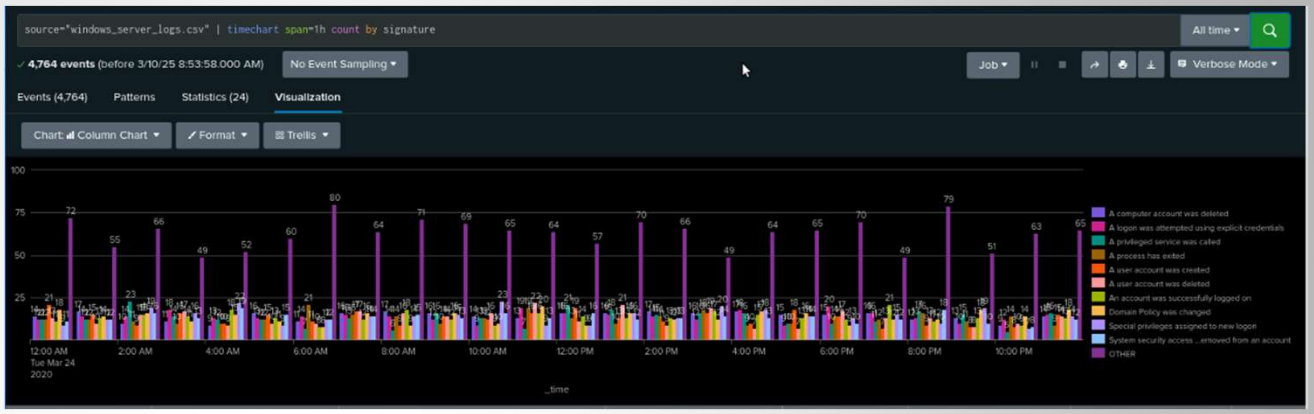


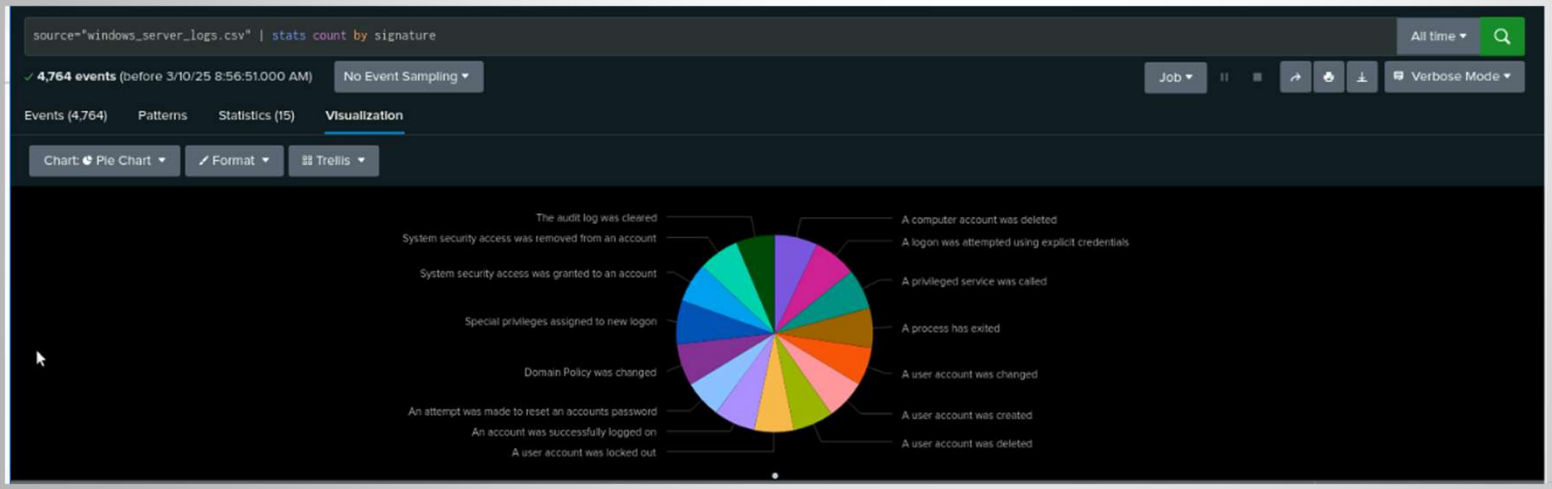


Dashboard Analysis for Users

Dashboards—Windows

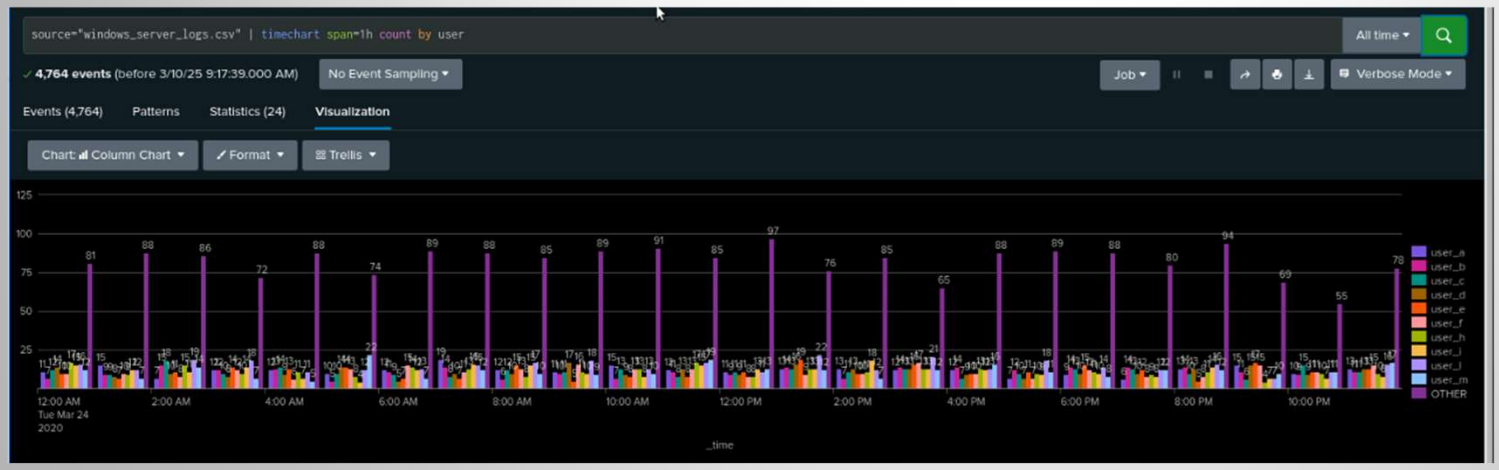
Dashboard Analysis for Signatures with Bar, Graph, and Pie Charts





Dashboards—Windows

Dashboard Analysis for Users with Bar, Graph, and Pie Charts



Apache Logs

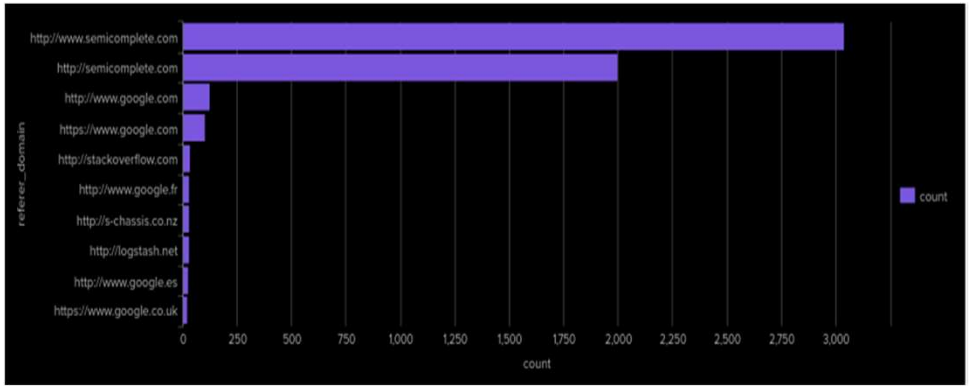
Reports—Apache

Designed the following reports:

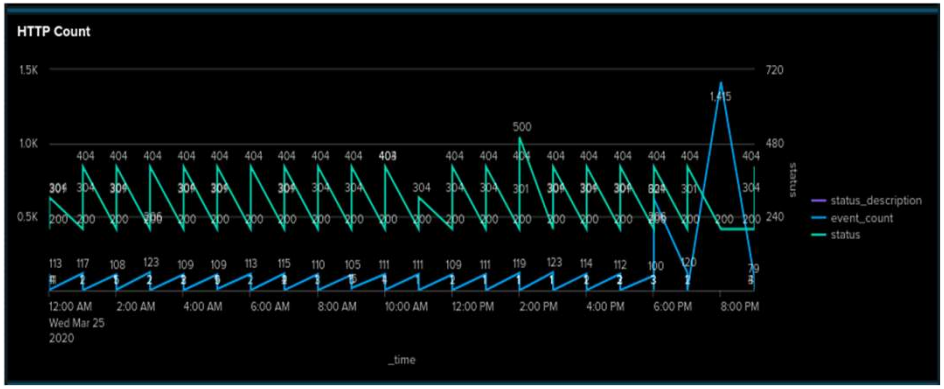
Report Name	Report Description
APACHE Domain	Identifies the top external domains that refer traffic to VSI's web server.
APACHE HTTP Count	Tracks the number of HTTP response code to detect potential attack patterns
APACHE Method	Shows the breakdown of different HTTP methods (GET, POST, HEAD)
APACHE URI	Identifies the most frequently accessed pages and URI's on the VSI's web server.

Images of Reports—Apache

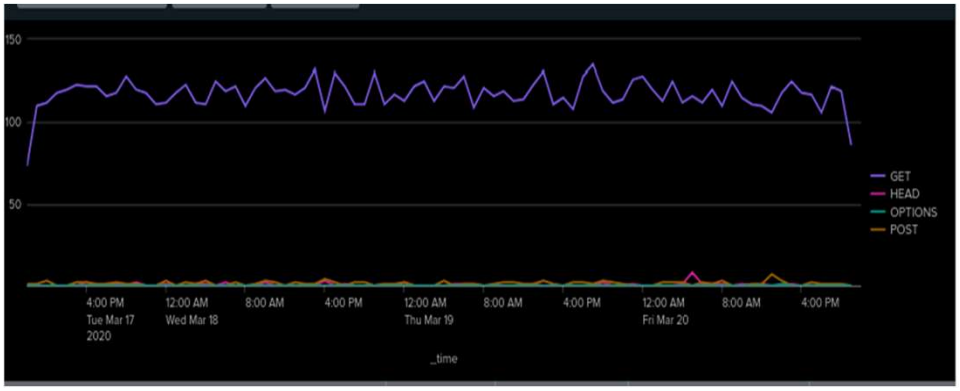
Domains



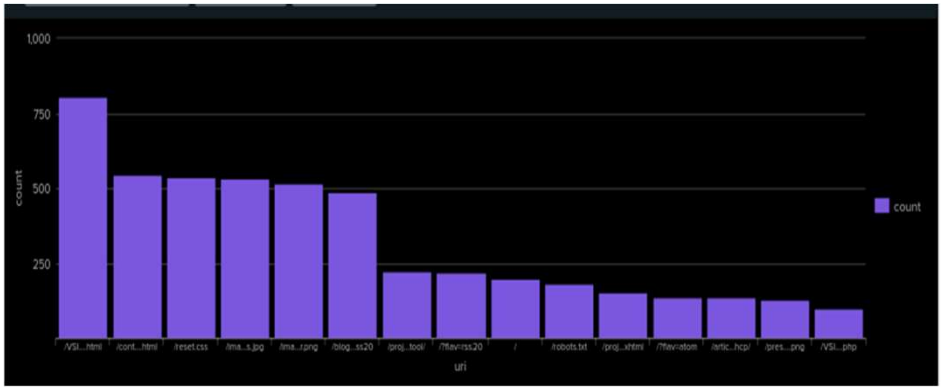
HTTP Response Count



HTTP METHOD

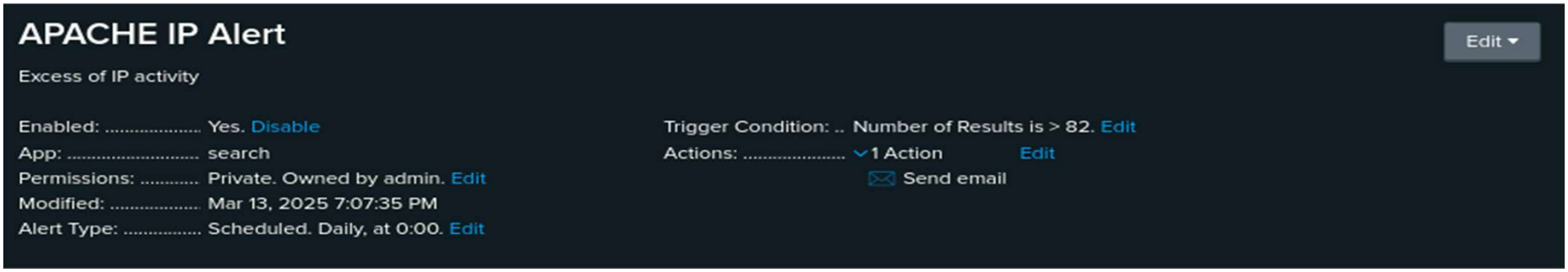


URI's



Alerts—Apache

Alert Name	Alert Description	Alert Baseline	Alert Threshold
APACHE_IP Alert	This alert monitors the amount of traffic coming from non-US IP addresses. A potential attack may be underway.	73	More than 82, results in an alert



JUSTIFICATION: The baselines were calculated through averaging which gave a footing when choosing a threshold. Meaning that any number significantly higher than the average will be flagged.

Alerts—Apache

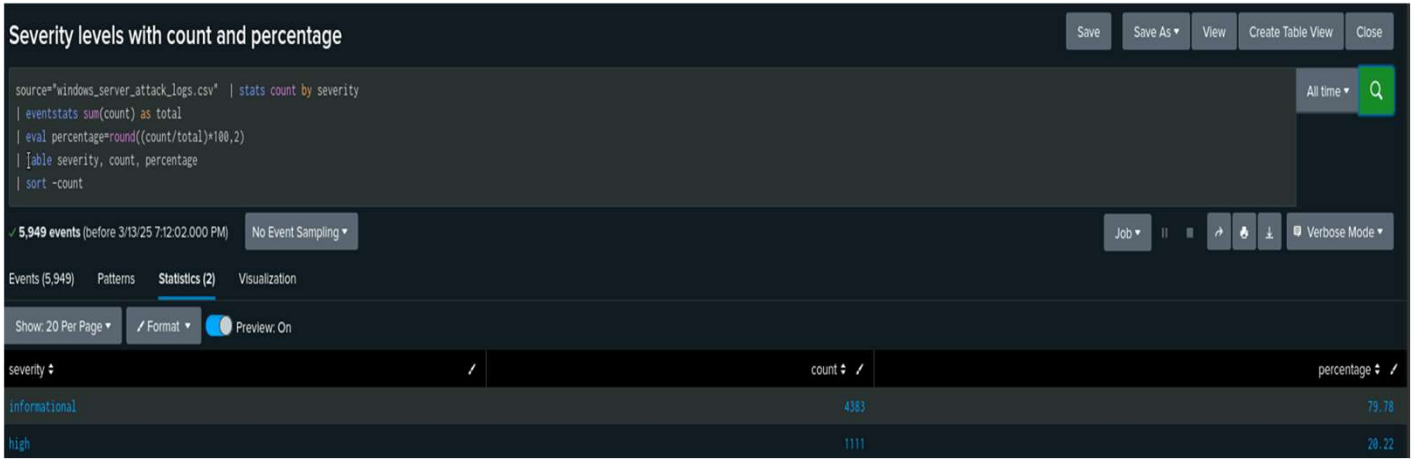
Alert Name	Alert Description	Alert Baseline	Alert Threshold
APACHE_POST Alert	This alert tracks HTTP POST requests which are usually form submissions, logins and file uploads. An excess in this may signal an attack	2	More than 3, results in an alert.

JUSTIFICATION: The baselines were calculated through averaging which gave a footing when choosing a threshold. Meaning that any number significantly higher than the average will be flagged.

Dashboards—Apache

Attack Analysis

Attack Summary—Windows Reports

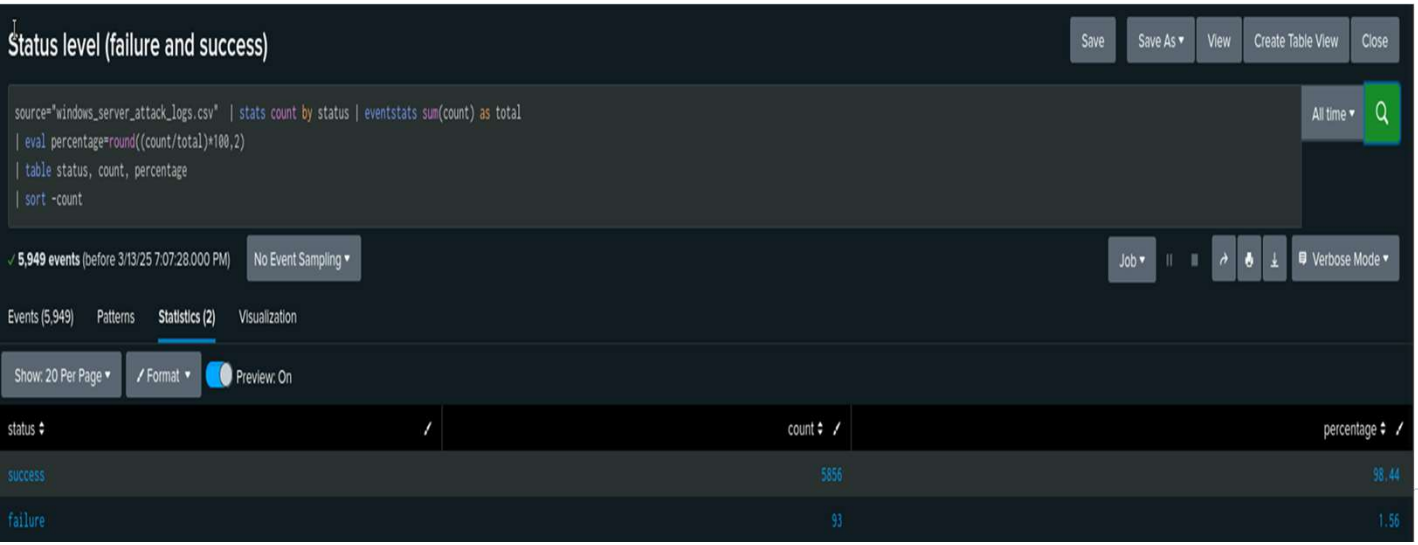


Severity:

High severity count

Initial count: 329 (7%)→ 1111 (20%)

Indicates →
- attackers are gaining admin level access
- possibly transferring sensitive data
- may have ran malicious payloads.



Failed Activities (Status):

Count for successes increased

4622 → 5856

Indicates →
- attackers exploited a vulnerability possibly through brute force attacks
- attempts to login succeeded

Check IP addresses, if many successful logins or failed attempts from same IP → credential surfing

Attack Summary—Windows Failed Activities Alert

High Failed Windows Activity Alert

Save | Save As | View | Create Table View | Close

```
source="windows_server_attack_logs.csv"  status="failure"
| bin _time span=1h
| stats count as failures by _time
| eventstats avg(failures) as baseline, stdev(failures) as std_dev
| eval threshold = baseline + (2 * std_dev)
| table _time, failures, baseline, threshold
| sort -_time_
```

All time

✓ 93 events (before 3/13/25 7:34:31.000 PM) | No Event Sampling | Job | Verbose Mode

Events (93) | Patterns | Statistics (11) | Visualization

Show: 20 Per Page | Format | Preview: On

_time	failures	baseline	threshold
2020-03-25 00:00	6	8.454545454545455	26.595408418883977
2020-03-25 01:00	8	8.454545454545455	26.595408418883977
2020-03-25 02:00	2	8.454545454545455	26.595408418883977
2020-03-25 03:00	3	8.454545454545455	26.595408418883977
2020-03-25 04:00	7	8.454545454545455	26.595408418883977
2020-03-25 05:00	6	8.454545454545455	26.595408418883977
2020-03-25 06:00	7	8.454545454545455	26.595408418883977
2020-03-25 07:00	8	8.454545454545455	26.595408418883977
2020-03-25 08:00	35	8.454545454545455	26.595408418883977
2020-03-25 12:00	3	8.454545454545455	26.595408418883977
2020-03-25 13:00	8	8.454545454545455	26.595408418883977

Alert for Windows failed activities:

Windows Logs:
Baseline → 5.9
Std deviation → 2.5
Threshold → 12

Attack logs:
Baseline → 8.5
35 failed attempts at 8AM, 03/25/2020

HUGE RED FLAG!!

Threshold was good and would trigger. No changes required.

Attack Summary—Windows Successful Logins Alert

High Login Activity Alert

```
source="windows_server_attack_logs.csv"  signature_id="4624"
| bin _time span=1h
| stats count as logins by _time
| eventstats avg(logins) as baseline, stdev(logins) as std_dev
| eval threshold = baseline + (2 * std_dev)
```

✓ **140 events** (before 3/13/25 7:45:14.000 PM) No Event Sampling

Events (140) Patterns **Statistics (12)** Visualization

Show: 20 Per Page Format Preview: On

_time	logins	baseline
2020-03-25 00:00	11	11.666666666666666
2020-03-25 01:00	15	11.666666666666666
2020-03-25 02:00	14	11.666666666666666
2020-03-25 03:00	14	11.666666666666666
2020-03-25 04:00	12	11.666666666666666
2020-03-25 05:00	9	11.666666666666666
2020-03-25 06:00	11	11.666666666666666
2020-03-25 07:00	15	11.666666666666666
2020-03-25 08:00	16	11.666666666666666
2020-03-25 09:00	4	11.666666666666666
2020-03-25 12:00	4	11.666666666666666
2020-03-25 13:00	15	11.666666666666666

Baseline: Decreased from 13.5 → 11.7

- Logins were within normal activity
- Indicates that once attackers were in the system, did not need to login many times.

Threshold was set to 23 but would not have mattered as maximum number of logins were 16 during the attack.

We would not change the threshold, as once the attackers had the credentials, they were able to login easily.

Instead, the alert that triggered when failed logins was 35 should have been taken very seriously and that warning would indicate an attack.

Attack Summary—Windows Account Deletion

Unusual account deletions in the hour

Save | Save As | View | Create Table View | Close

```
source="windows_server_attack_logs.csv"  signature_id="4726" | bin _time span=1h
| stats count as deletions by _time
| eventstats avg(deletions) as baseline, stdev(deletions) as std_dev
```

All time

✓ 131 events (before 3/13/25 8:03:32.000 PM) | No Event Sampling | Job | Verbose Mode

Events (131) | Patterns | Statistics (13) | Visualization

Show: 20 Per Page | Format | Preview: On

_time	deletions	baseline	std_dev
2020-03-25 00:00	14	10.076923076923077	4.786465962508917
2020-03-25 01:00	7	10.076923076923077	4.786465962508917
2020-03-25 02:00	5	10.076923076923077	4.786465962508917
2020-03-25 03:00	9	10.076923076923077	4.786465962508917
2020-03-25 04:00	14	10.076923076923077	4.786465962508917
2020-03-25 05:00	17	10.076923076923077	4.786465962508917
2020-03-25 06:00	13	10.076923076923077	4.786465962508917
2020-03-25 07:00	11	10.076923076923077	4.786465962508917
2020-03-25 08:00	11	10.076923076923077	4.786465962508917
2020-03-25 09:00	3	10.076923076923077	4.786465962508917
2020-03-25 11:00	1	10.076923076923077	4.786465962508917
2020-03-25 12:00	13	10.076923076923077	4.786465962508917
2020-03-25 13:00	13	10.076923076923077	4.786465962508917

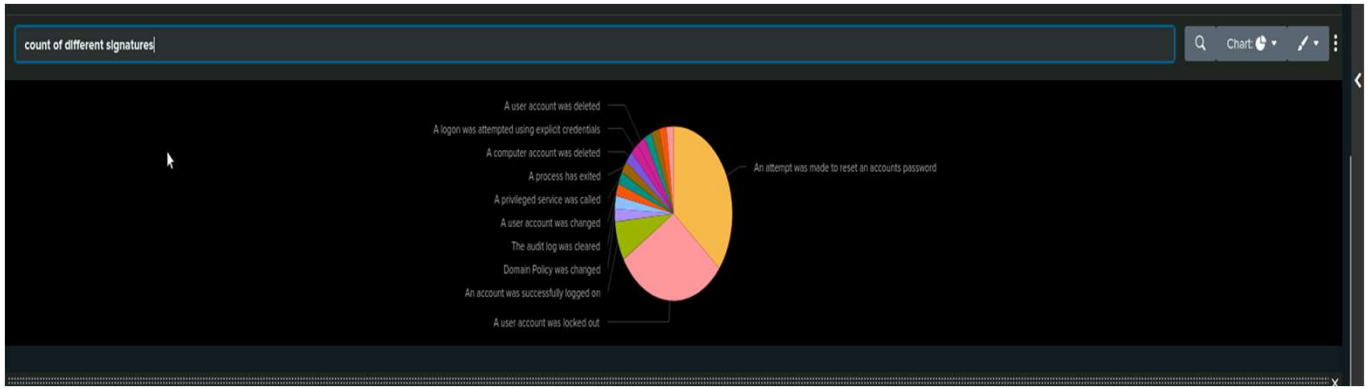
Baseline → dropped from 13 to 11

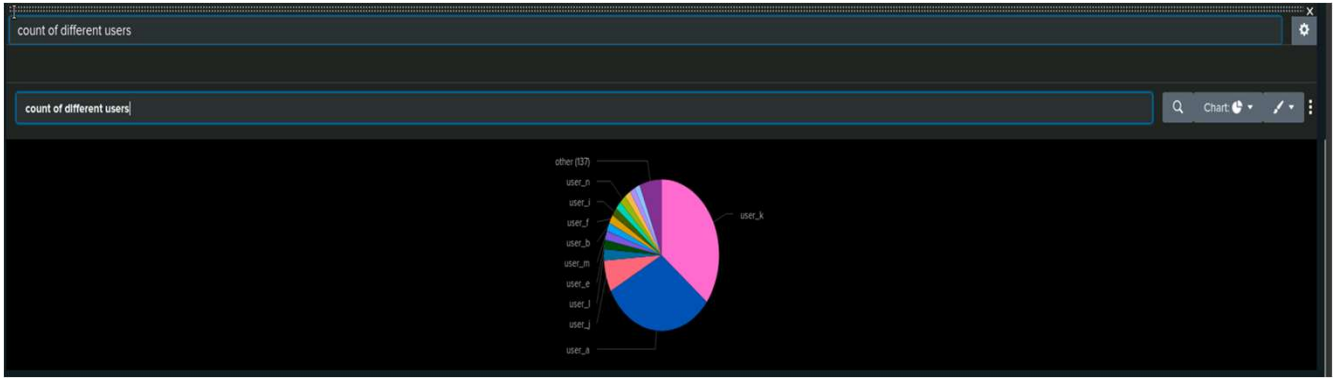
Threshold of unusual account deletions set to 23.

Activity was within normal parameters.

Threshold would not be changed as this would cause alert fatigue from normal operations.

Attack Summary—Windows Dashboard





The peak count for the different signatures was 896 accounts being locked out, and 1258 attempts to reset a password.

Indicates a brute force attack

Two very active users during the attack:

Users A and K.

Indicate their accounts were used to access data, credentials compromised.

Peak logins for both users: 984 for user A and 1256 for user K.

User J had 398 logins.

Occurred between 12-3AM and 8-11AM.

Windows Attack Logs - Summary

Malicious activity occurred

- Accounts were compromised – possibly through brute force attacks / credential surfing / password spraying
- 2-3 users accounts were compromised, possibly more.

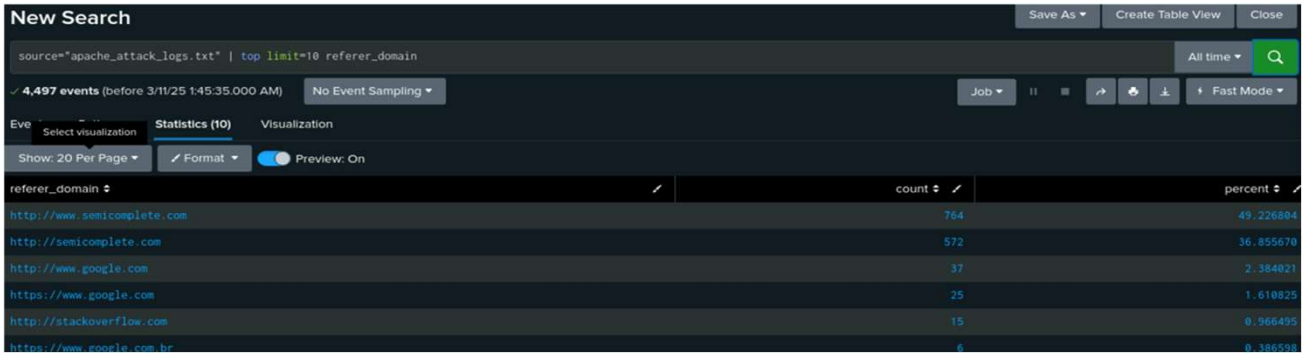
Many accounts were locked out – indicating failed login attempts

Password resets for accounts were attempted – indicates failed logins or changing password to lock users out of accounts.

Attack Summary—Apache Reports

1. HTTP Methods VSI's Website

2. Top 10 Referrer Domains of



GET method:
9851 → 3157

POST method:
106 → 1324

Possible Meanings

Decrease in GET method:
→ normal browsing was reduced.

Significant **increase in POST** method:
→ Potential Brute-Force or SQL injection attack, and/or unauthorized login attempts.

Decrease in Referrer domain traffic:
→ less visits by legitimate users during the attack

Overall decrease in referrer domain traffic.
Example: www.semicomplete.com dropped from 3038 to 764

Attack Summary - Apache Reports cont'd

3. HTTP Response Codes

status	count
200	3746
206	5
301	29
304	36
403	1
404	679
500	1

- **Significant drop** in 200 (OK) response code: 9126 → 3746
- **Increase** in 404 (Error) response code: 213 → 679
- **Large decrease** in 304 (Not Modified) response code: 445 → 36
- **Decrease** in 301 (Redirect) response code: 164 → 29
- **Disappearence** of 416 (Range Not Satisfiable) response code: 2 → 0

Possible Meanings:

Drop in 200:
→ Attack disrupted normal operations

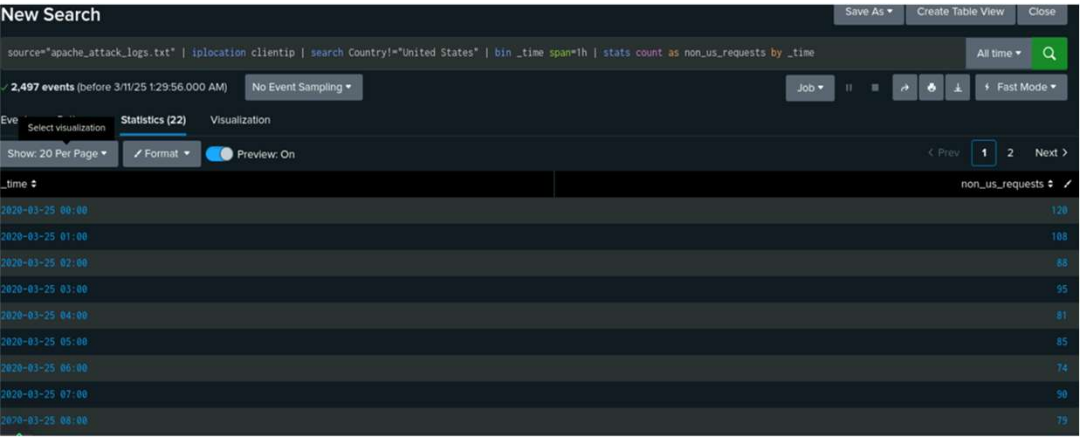
Increase in 404:
→ Attempts to gather information about VSI's corporation / website (Web Reconnaissance)

Drop in 304/ 416 Gone:
→ legitimate users not returning to site during the attack

Drop in 301:
→ attackers avoid regular navigation paths and directly targeting endpoints

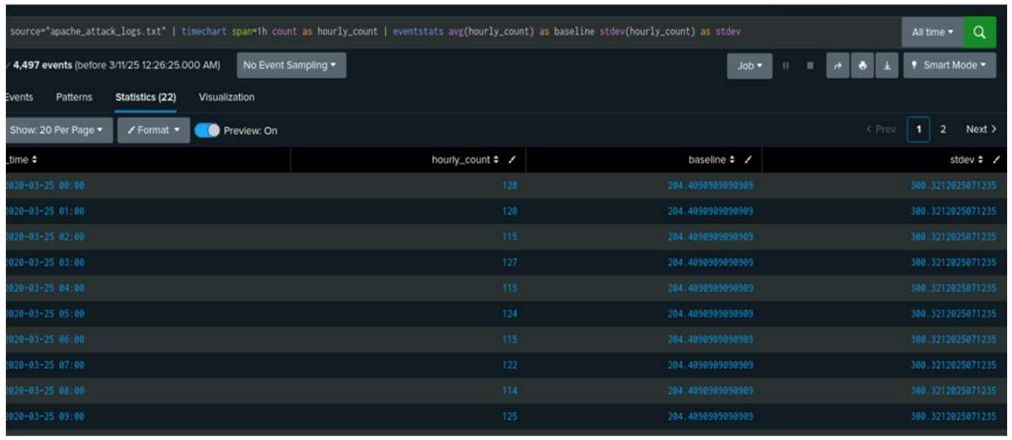
Attack Summary—Apache Alerts

1. Hourly Count for Non-US Requests



- Highest volume of non-U.S. requests : **120**
  - At 00:00 on March 25, 2020
- **Hours of major attack activity**:
  - Midnight to 3:00am (Ranging 120 to 95)
  - 7:00am to 10:00am (Ranging 79 to 107)
- Threshold of 82 was efficient
  - Flagged the majority
  - Missed a couple high values, such as 79

2. Hourly Count for HTTP POST Method



- Huge increase of hourly HTTP POST method count
  - Normal log range: 0 - 3
  - Attack log range: 114 - 128
- Threshold of > 3 was too low
  - It helped flag minor anomalies, but can easily cause alert fatigue
  - A threshold of 6 or 7 would have strictly indicated an attack

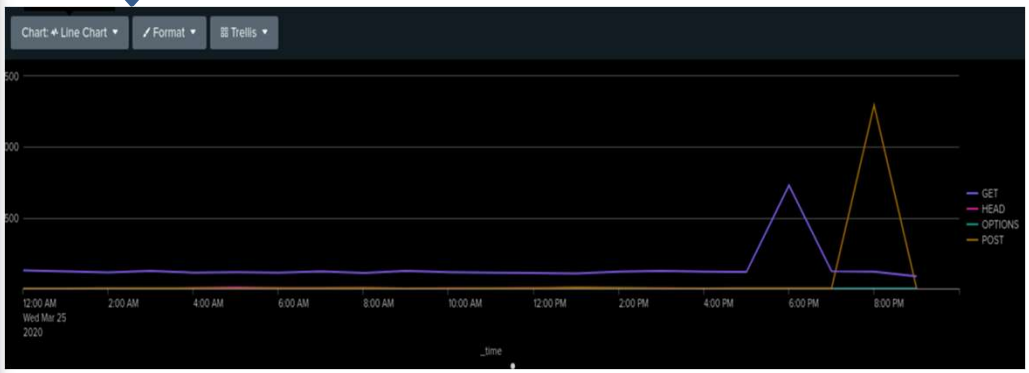
Attack Summary—Apache Dashboard Visuals

1. HTTP Methods

1 Normal Log

- GET method:
  - Ranges 110 to 128/h
- POST method:
  - Max value of 7/h

2 Attack Log

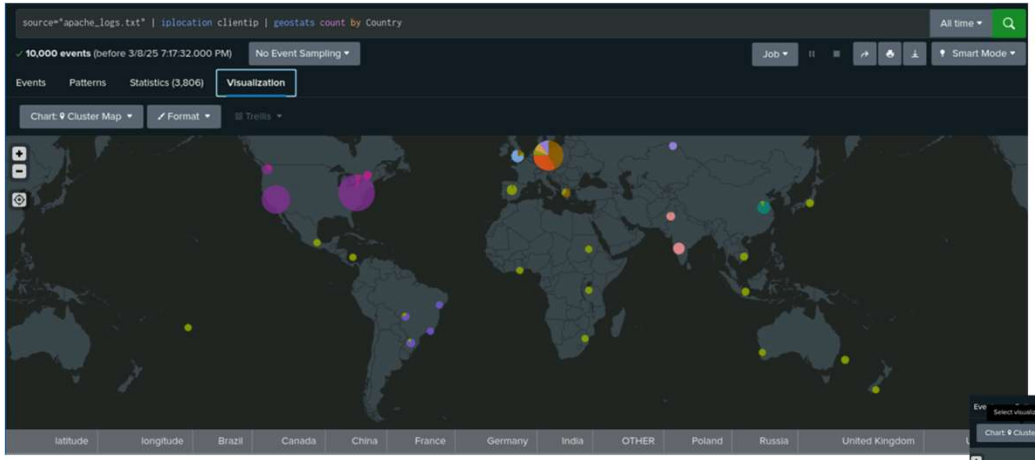


- GET method:
  - Jumps to 729 at 6:00pm
- POST method:
  - Skyrockets to 1296 at 8:00pm

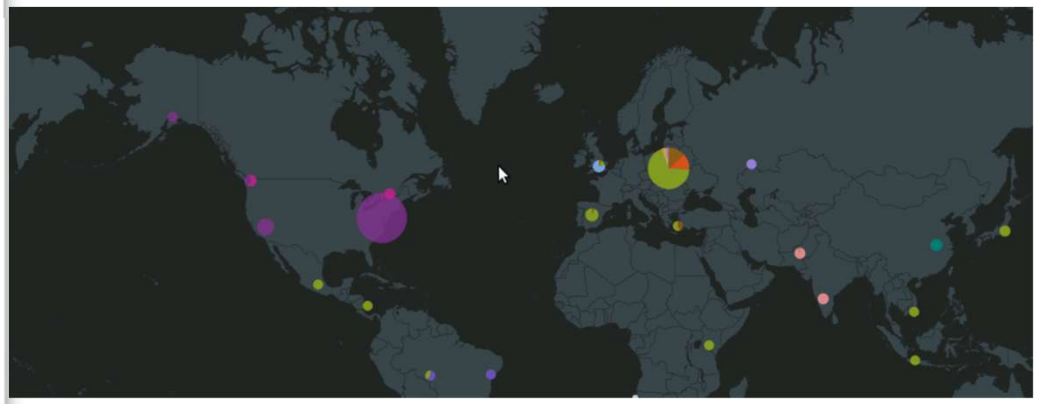
Attack Summary—Apache Dashboard Visuals

1. Clustermap of IP Locations

1 Normal Log



2 Attack Log

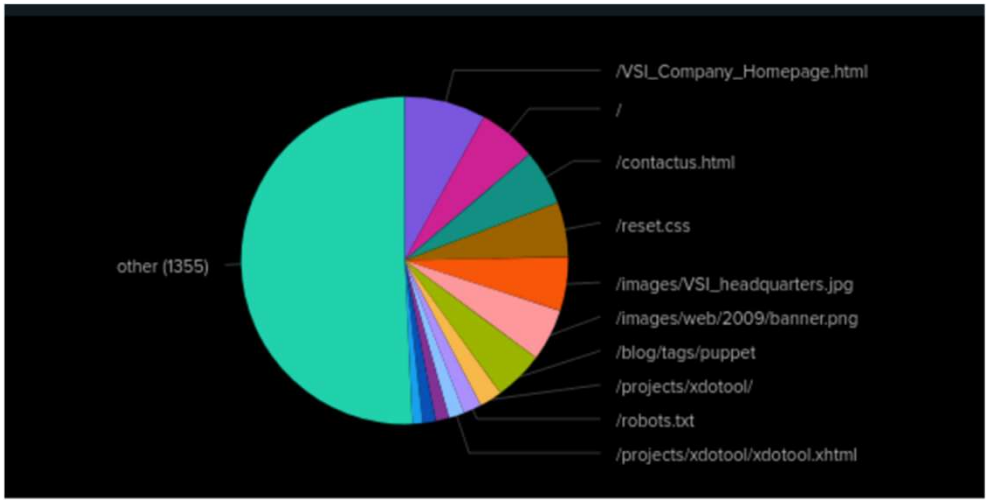


Location of new city activity: Dnipropetrovsk, Ukraine

Attack Summary—Apache Dashboard Visuals

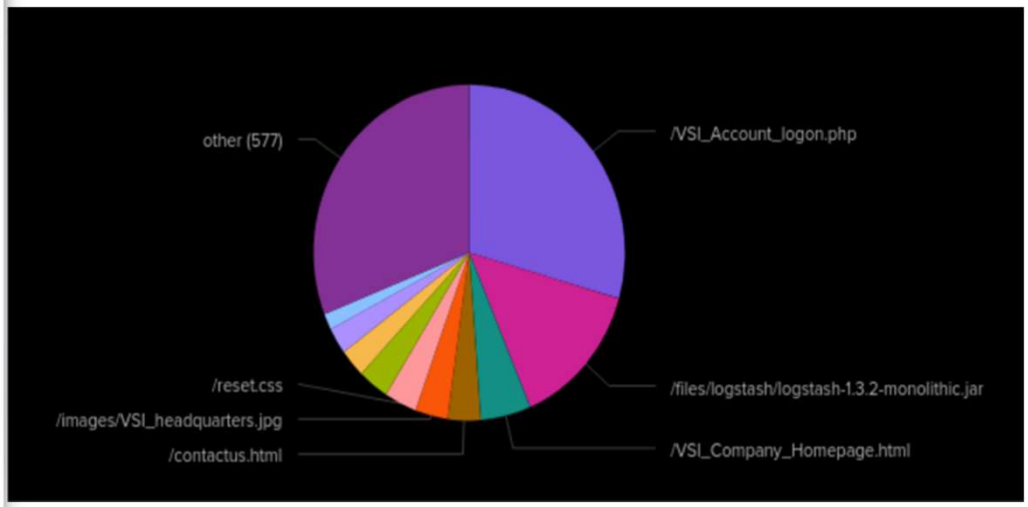
3. URI Path

1 Normal Log



/VSI_Account_logon.php: **count of 101**

2 Attack Log



/VSI_Account_logon.php: **count of 1323**

Indicating… Unauthorized login to the system (i.e. Brute-Force Attack, SQL Injection, exploiting login system)

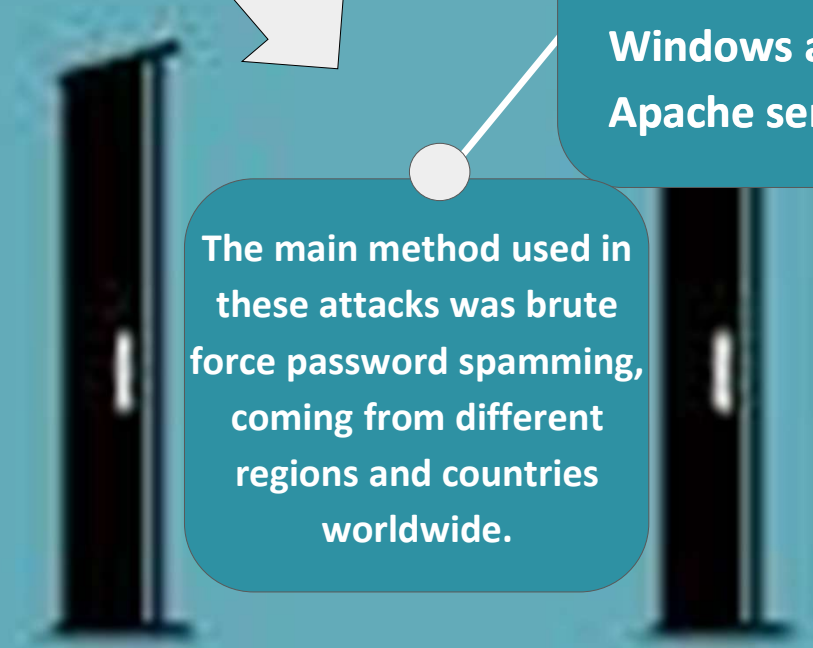
Apache Attack Logs - Summary

- Malicious activity did occur
  - Unauthorized login attempts - some being successful
    - Possible Brute-Force attack
    - Possible SQL Injection attacks
  - less legitimate users interacting with the site during attack
  - Attackers directly targeting endpoints
  - New city with suspicious activity in Ukraine

Summary and Future Mitigations

Windows and Apache Servers attack Summary

TYPICALLY, THE DATA FROM THE ATTACK THAT TOOK PLACE ON MARCH 25, 2020:



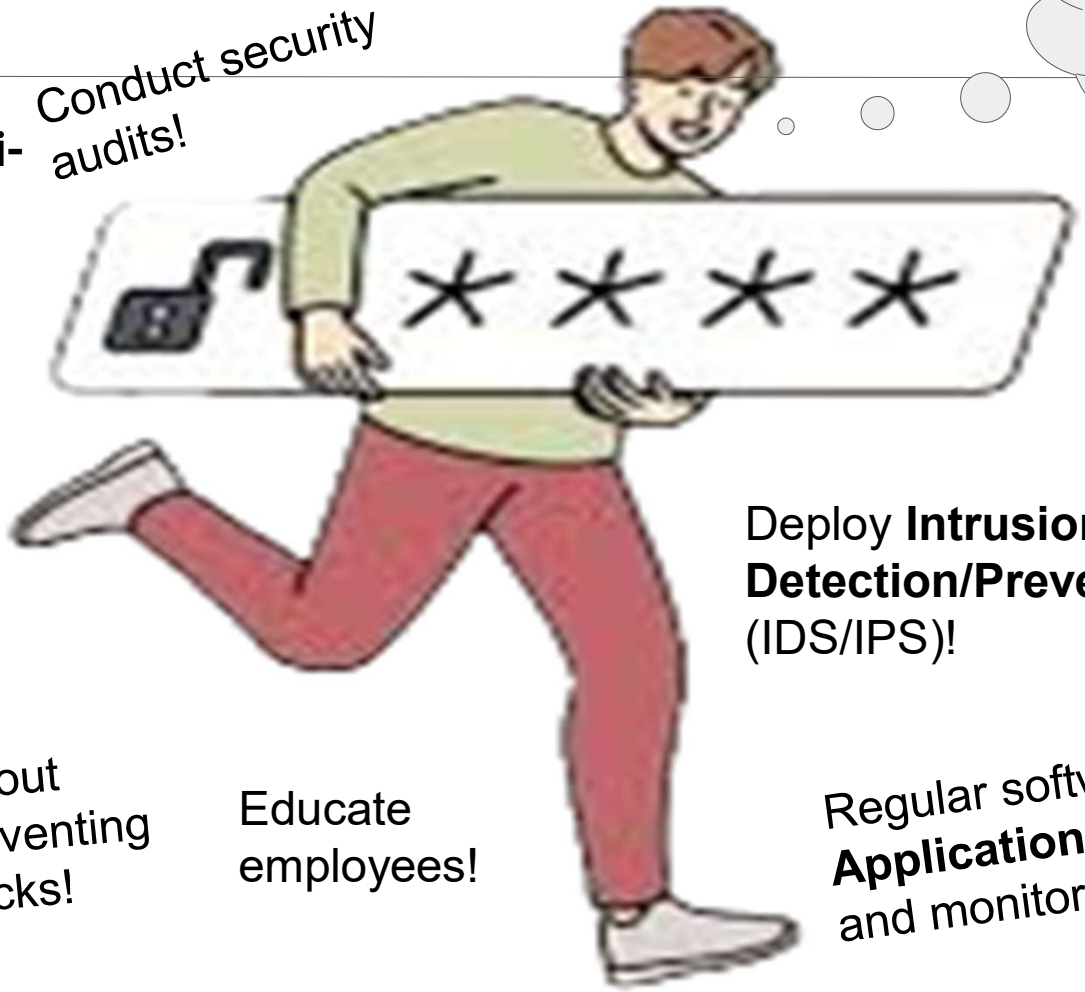
VSI faced multiple attacks on their Windows and Apache servers.

The main method used in these attacks was brute force password spamming, coming from different regions and countries worldwide.

Recommended mitigations

Conduct security audits!

Implement **Multi-Factor Authentication** (MFA) for all users!



IP rate limiting!

Geo-blocking!

Enforce strong password policies!

Deploy **Intrusion Detection/Prevention Systems** (IDS/IPS)!

Use account lockout mechanisms, preventing Brute-Force Attacks!

Educate employees!

Regular software patching, **Web Application Firewalls** (WAF), and monitoring logs!

QUESTIONS