

Splunk 2: Defend Your SOC (Attack Detection)

Scenario



VSI recently experienced several cyberattacks, likely from their adversary JobeCorp. Fortunately, your SOC team had set up several monitoring solutions to help VSI quickly identify what was attacked. These monitoring solutions will also help VSI create mitigation strategies to protect the organization.

Windows Server Logs



Reports:

Report Analysis for Severity

Before the Attack

| Severity | | | Save | Save As ▾ | View | Create Table View | Close |
|---|--|--|----------|-----------|------|-------------------|---|
| source="windows_server_logs.csv" top severity | | | | | | All time ▾ |  |
| ✓ 23,820 events (before 6/16/22 1:33:15.000 AM) No Event Sampling ▾ | | | Job ▾ | | ■ | ↗ | 📄 ⬇️ ⚙️ Smart Mode ▾ |
| Events Patterns Statistics (2) Visualization | | | | | | | |
| 100 Per Page ▾  Format Preview ▾ | | | | | | | |
| severity ⬇️ | | | count ⬇️ | | | | |
| informational | | | 22175 | 93.09 % | | | |
| high | | | 1645 | 6.91 % | | | |

Current

| Severity | | | Save | Save As ▾ | View | Create Table View | Close |
|---|--|--|----------|-----------|------|-------------------|---|
| source="windows_server_attack_logs.csv" top severity | | | | | | All time ▾ |  |
| ✓ 17,847 events (before 6/16/22 1:33:24.000 AM) No Event Sampling ▾ | | | Job ▾ | | ■ | ↗ | 📄 ⬇️ ⚙️ Smart Mode ▾ |
| Events Patterns Statistics (2) Visualization | | | | | | | |
| 100 Per Page ▾  Format Preview ▾ | | | | | | | |
| severity ⬇️ | | | count ⬇️ | | | | |
| informational | | | 13149 | 79.78 % | | | |
| high | | | 3333 | 20.22 % | | | |

Observations: The high severity increase more than double

Report Analysis for Failed Activities

Before the Attack

source="windows_server_logs.csv" | top status

All time

✓ 28,584 events (before 6/16/22 1:46:19.000 AM) No Event Sampling

Job

||

Smart Mode

Events

Patterns

Statistics (2)

Visualization

100 Per Page

Format

Preview

| status | count | percent |
|---------|-------|---------|
| success | 27732 | 97.02 % |
| failure | 852 | 2.98 % |

Current

source="windows_server_attack_logs.csv" | top status

All time

✓ 17,847 events (before 6/16/22 1:49:43.000 AM) No Event Sampling

Job

Smart Mode

Events

Patterns

Statistics (2)

Visualization

100 Per Page

Format

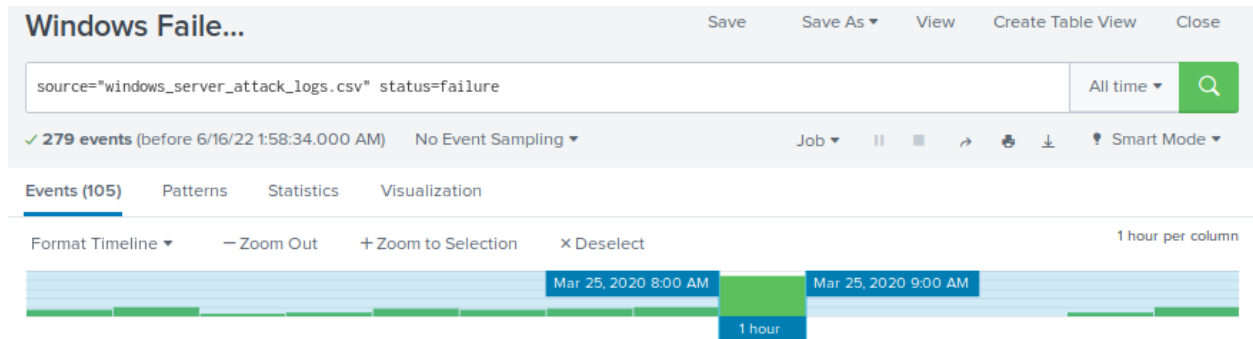
Preview

| status | count | percent |
|---------|-------|---------|
| success | 17568 | 98.44 % |
| failure | 279 | 1.56 % |

Observations: The failure activities decreased

Alerts:

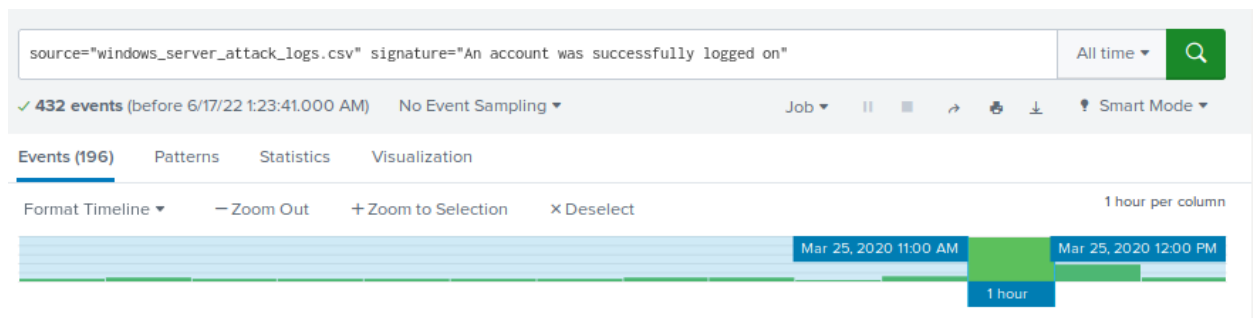
Alert Analysis for Failed Windows Activity



Observations:

The alert triggers on Wednesday 25 March. 2020 at 8 AM as the threshold of 25 events is triggered. 35 events were detected during that hour. The alert was triggered only at that hour, so no changes are required.

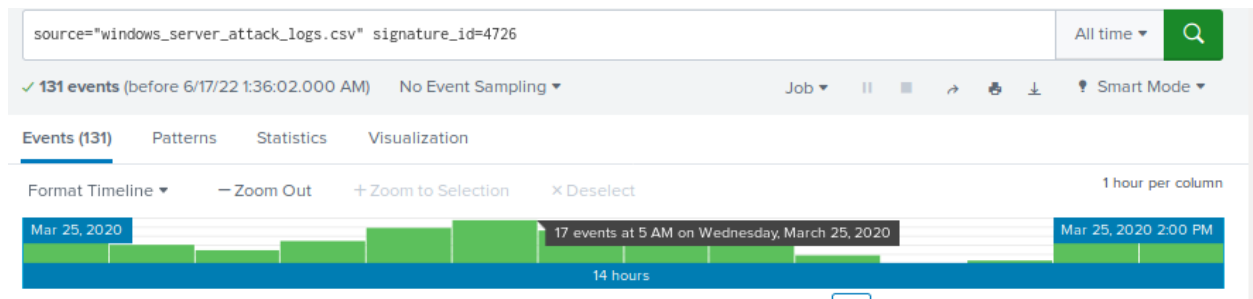
Alert Analysis for Successful Logged on



Observations:

The alert triggered on Wednesday 25 March. 2020 at 11 AM and 12 AM. 196 and 77 events were detected respectively. The 35 threshold does not need changes as it triggered only at the time of the attack.

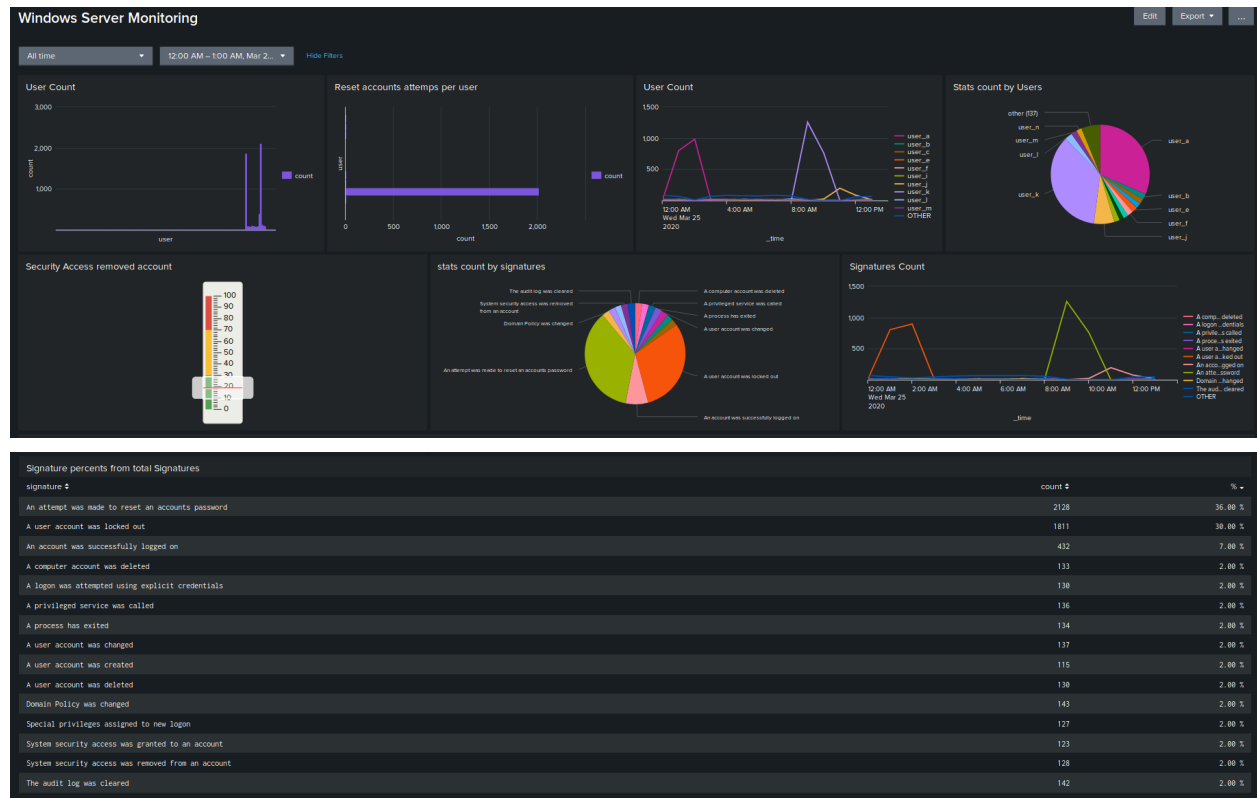
Alert Analysis for Deleted Accounts



Observations:

No alerts were triggered as the hour with a higher number of events of 17 does not reach the threshold of 25.

Dashboard:



Observations:

There is a substantial increase in the Signatures of attempts to reset passwords (1258) from 08h00 to 11h00, and account locked out (896) from 00h00 to 03h00. User "k" and "a" has a peak on activity per hour

User "a" activity began at 00h00 at extend to 03h00 with a peak of 894 events similar to the number of signatures of locked out (896)

Meanwhile user "k" activity ranges from 08h00 to 11h00 with a peak of 1256 closer to the 1258 attempts to reset passwords during the same period of time

Apache Web Server Logs

Reports:

Report HTTP methods

Before the Attack

| source="apache_logs.txt" top limit=20 method | | All time | 🔍 |
|--|-------|----------|---|
| ✓ 10,000 events (before 6/17/22 11:33:49.000 PM) No Event Sampling | | Job | ⏏ |
| Events Patterns Statistics (4) Visualization | | | |
| 20 Per Page Format Preview | | | |
| method | count | percent | |
| GET | 9851 | 98.51 % | |
| POST | 106 | 1.06 % | |
| HEAD | 42 | 0.42 % | |
| OPTIONS | 1 | 0.01 % | |

Current

| source="apache_attack_logs.txt" top limit=20 method | | All time | 🔍 |
|---|-------|----------|---|
| ✓ 4,497 events (before 6/17/22 10:49:15.000 PM) No Event Sampling | | Job | ⏏ |
| Events Patterns Statistics (4) Visualization | | | |
| 20 Per Page Format Preview | | | |
| method | count | percent | |
| GET | 3157 | 70.20 % | |
| POST | 1324 | 29.44 % | |
| HEAD | 15 | 0.33 % | |
| OPTIONS | 1 | 0.02 % | |

Observations: The Post Method has increased. This method is use to send data.

Report Analysis for Referrer Domains

Before the Attack

| source="apache_logs.txt" top limit=10 referer_domain | | All time | 🔍 |
|--|----------|-----------------|-----------------------------|
| ✓ 10,000 events (before 6/17/22 11:34:58.000 PM) No Event Sampling | | Job | ⏸️ 📊 ➡️ 🗑️ ⬇️ ⚙️ Smart Mode |
| Events | Patterns | Statistics (10) | Visualization |
| 20 Per Page | Format | Preview | |
| referer_domain | count | percent | |
| http://www.semicomplete.com | 3038 | 51.26 % | |
| http://semicomplete.com | 2001 | 33.76 % | |
| http://www.google.com | 123 | 2.08 % | |
| https://www.google.com | 105 | 1.77 % | |
| http://stackoverflow.com | 34 | 0.57 % | |
| http://www.google.fr | 31 | 0.52 % | |
| http://s-chassis.co.nz | 29 | 0.49 % | |
| http://logstash.net | 28 | 0.47 % | |
| http://www.google.es | 25 | 0.42 % | |
| https://www.google.co.uk | 23 | 0.39 % | |

Current

| New Search | | Save As | Create Table View | Close |
|---|----------|-----------------|-----------------------------|-------|
| source="apache_attack_logs.txt" top limit=10 referer_domain | | All time | 🔍 | |
| ✓ 4,497 events (before 6/17/22 10:55:15.000 PM) No Event Sampling | | Job | ⏸️ 📊 ➡️ 🗑️ ⬇️ ⚙️ Smart Mode | |
| Events | Patterns | Statistics (10) | Visualization | |
| 20 Per Page | Format | Preview | | |
| referer_domain | count | percent | | |
| http://www.semicomplete.com | 764 | 49.23 % | | |
| http://semicomplete.com | 572 | 36.86 % | | |
| http://www.google.com | 37 | 2.38 % | | |
| https://www.google.com | 25 | 1.61 % | | |
| http://stackoverflow.com | 15 | 0.97 % | | |
| https://www.google.com.br | 6 | 0.39 % | | |
| https://www.google.co.uk | 6 | 0.39 % | | |
| http://tuxradar.com | 6 | 0.39 % | | |
| http://logstash.net | 6 | 0.39 % | | |
| http://www.google.de | 5 | 0.32 % | | |

Observations: There is a substantial decrease on th events

Report Analysis for HTTP Response Codes

Before the Attack

source="apache_logs.txt" | top status

✓ 10,000 events (before 6/17/22 11:35:33.000 PM) No Event Sampling

Events Patterns **Statistics (8)** Visualization

20 Per Page Format Preview

| status | count | percent |
|--------|-------|---------|
| 200 | 9126 | 91.26 % |
| 304 | 445 | 4.45 % |
| 404 | 213 | 2.13 % |
| 301 | 164 | 1.64 % |
| 206 | 45 | 0.45 % |
| 500 | 3 | 0.03 % |
| 416 | 2 | 0.02 % |
| 403 | 2 | 0.02 % |

Current

New Search

source="apache_attack_logs.txt" | top status

✓ 4,497 events (before 6/17/22 11:01:42.000 PM) No Event Sampling

Events Patterns **Statistics (7)** Visualization

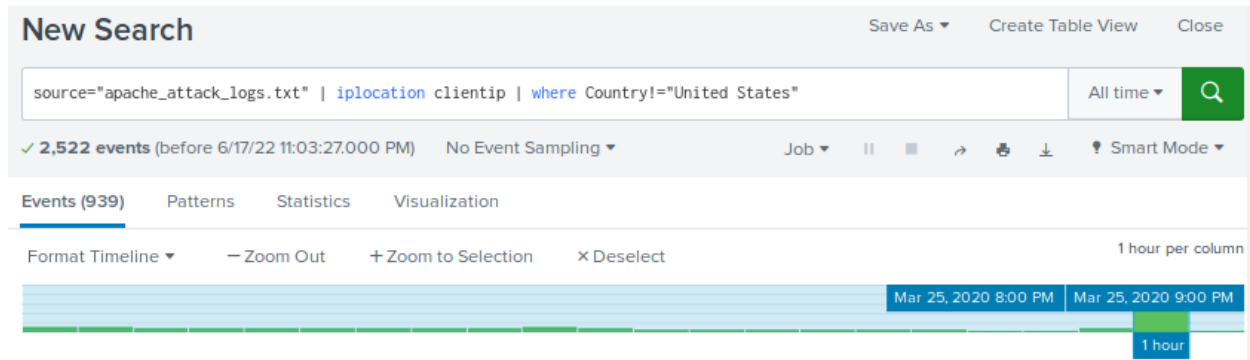
20 Per Page Format Preview

| status | count | percent |
|--------|-------|---------|
| 200 | 3746 | 83.30 % |
| 404 | 679 | 15.10 % |
| 304 | 36 | 0.80 % |
| 301 | 29 | 0.64 % |
| 206 | 5 | 0.11 % |
| 500 | 1 | 0.02 % |
| 403 | 1 | 0.02 % |

Observations: There is a significance increase of the 404 code

Alerts:

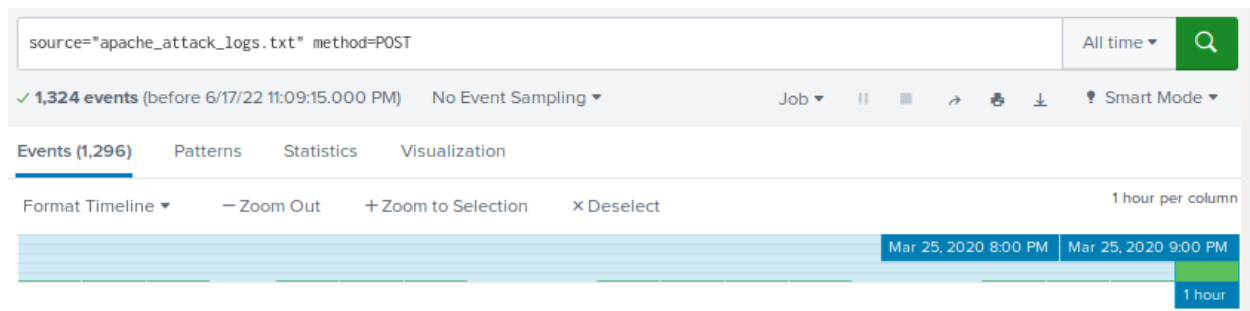
Alert Analysis for International Activity



Observations:

There is a suspicious volume of international activity. There are 939 events at 20h00. This event triggered the alert of 120. The threshold does not need change as the threshold has not trigger any other hour.

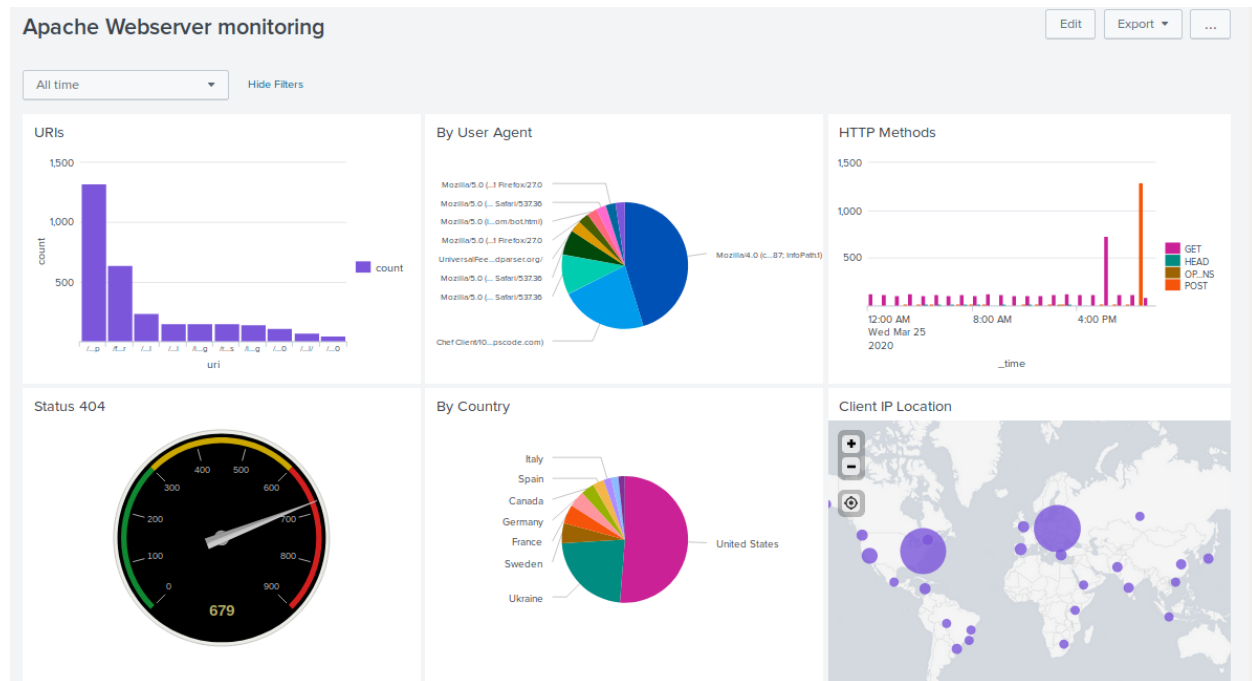
Alert Analysis for HTTP POST Activity



Observations:

There is a peak of 1296 events of Http POST the March 25 2020 at 20h00. Only at this moment the threshold was triggered generating an alert, so no change is needed for this.

Dashboard:



Observations:

There are two types of attack. The GET method attack occurs from 17h00 to 19h00 and the POST method attack occurs from 19h00 to 21h00. The peak count of the top method was 1296.

It detected a higher volume of activity coming from the city of Kiev, Ukraine with a peak of 439 events.

The dashboard shows an URI peak for account_logon.php. We could imply that this was a back-end attack like a local inclusion.