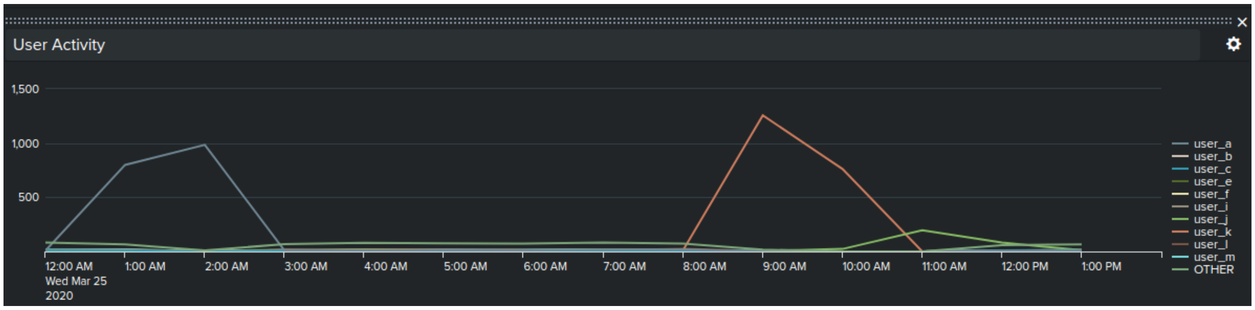
Part 1: Windows Server Attack

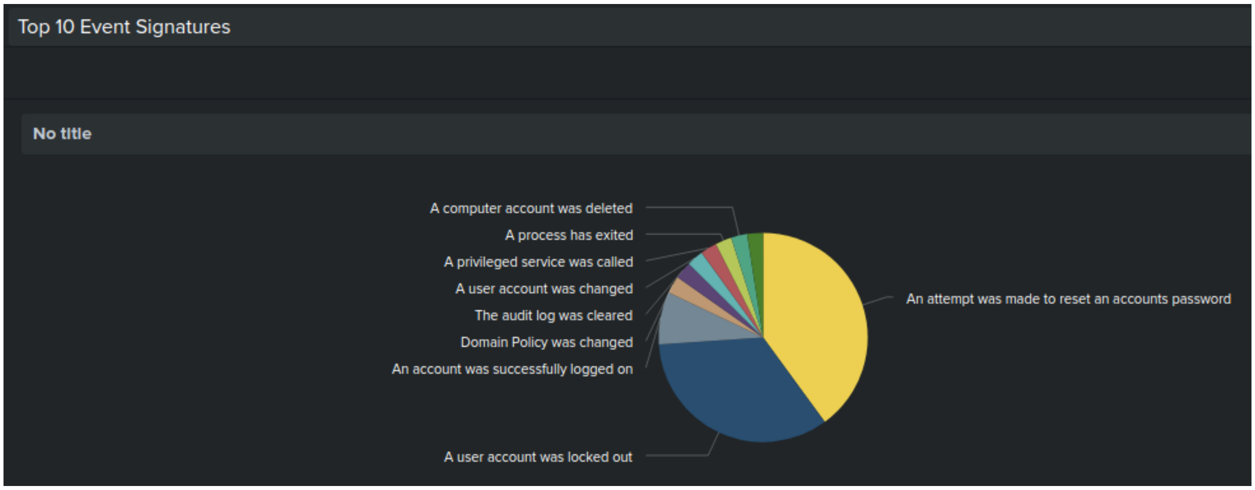
Note: This is a public-facing windows server that VSI employees access.

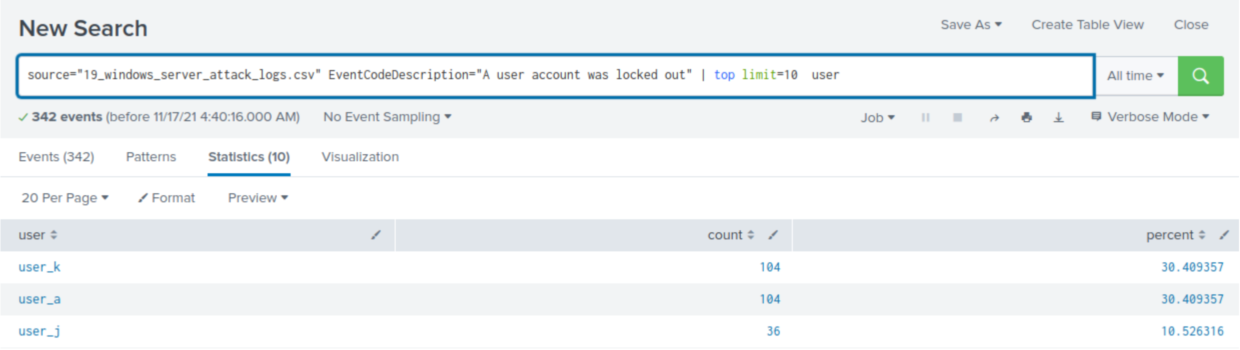
Question 1

- Several users were impacted during the attack on March 25th.
- Based on the attack signatures, what mitigations would you recommend to protect each user account? Provide global mitigations that the whole company can use and individual mitigations that are specific to each user.



user_a between 12-3am
user_k between 8-11am

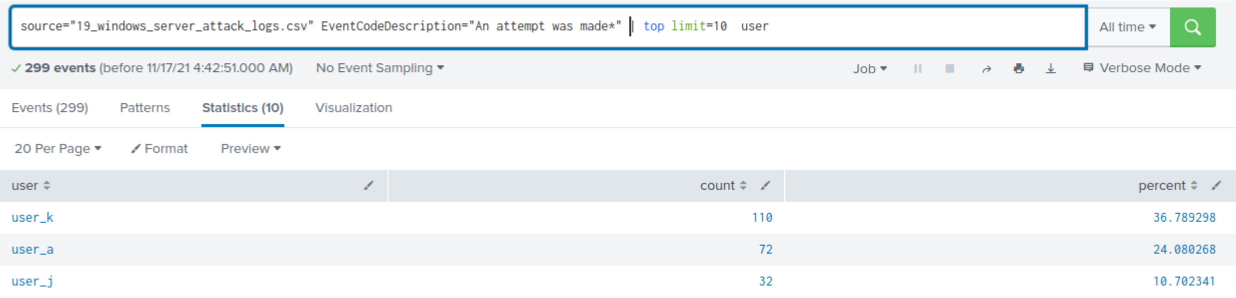




```
source="19_windows_server_attack_logs.csv" EventCodeDescription="A user account was locked out" | top limit=10  user
```

✓ 342 events (before 11/17/21 4:40:16.000 AM) No Event Sampling ▾

user	count	percent
user_k	104	30.409357
user_a	104	30.409357
user_j	36	10.526316



```
source="19_windows_server_attack_logs.csv" EventCodeDescription="An attempt was made*" | top limit=10  user
```

✓ 299 events (before 11/17/21 4:42:51.000 AM) No Event Sampling

user	count	percent
user_k	110	36.789298
user_a	72	24.080268
user_j	32	10.702341

Review account lockout settings. Progressively increase lockout times for failed logins. Reject logins from IP ranges not normally associated with VSI employees.

Question 2

- VSI has insider information that JobeCorp attempted to target users by sending "Bad Logins" to lock out every user.
- What sort of mitigation could you use to protect against this?

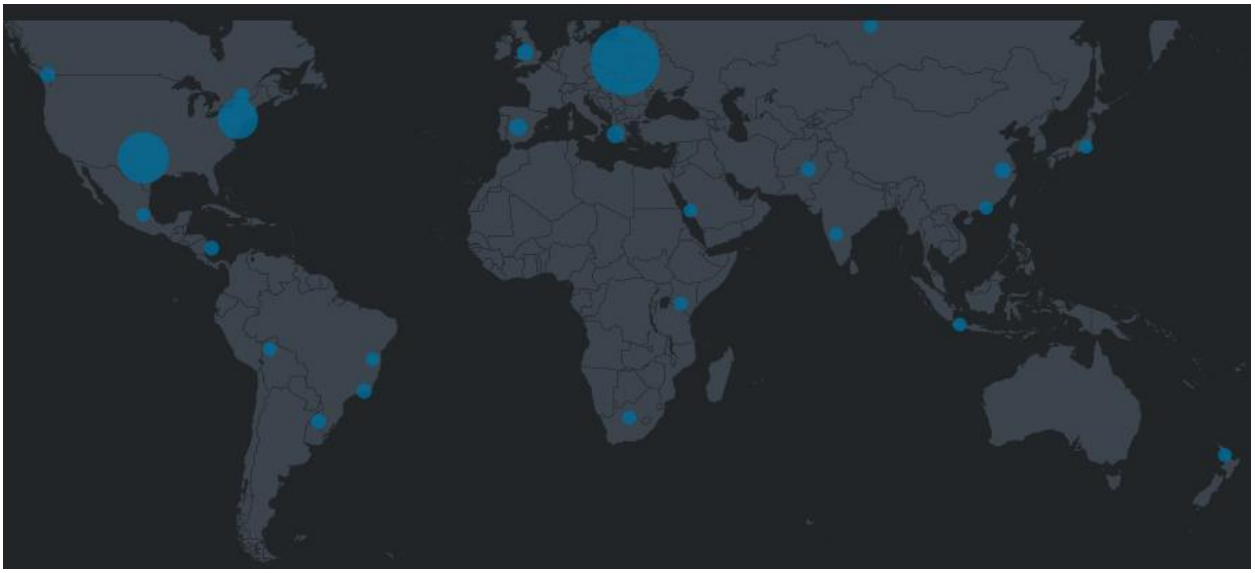
  If this server is for VSI employees, it should not be on the public facing internet. Either place it in a DMZ or on their intranet accessible via a VPN. Block logins from outside of their usual geographic IP areas / ranges. Employ multi-factor or two step authentication of logins (especially if they are from unusual IP addresses for VSI's employees).

Part 2: Apache Webserver Attack:

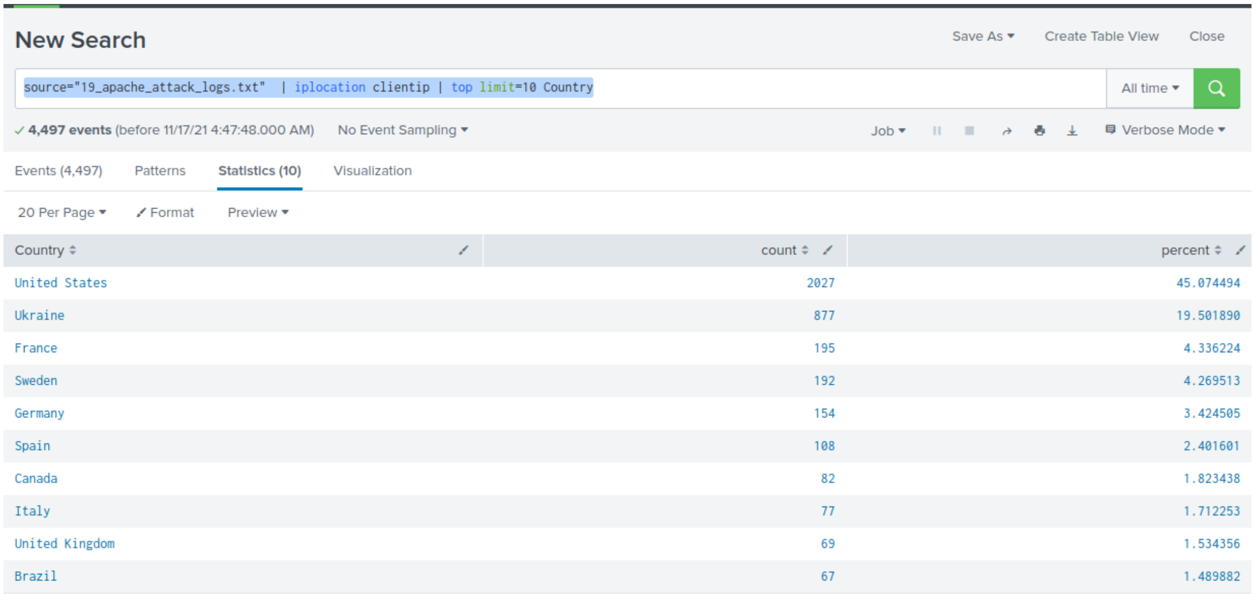
Question 1

- Based on the geographic map, recommend a firewall rule that the networking team should implement.
- Provide a "plain english" description of the rule.
  - For example: "Block all incoming HTTP traffic where the source IP comes from the city of Los Angeles."
- Provide a screen shot of the geographic map that justifies why you created this rule.

Geographic map



```
source="19_apache_attack_logs.txt" | iplocation clientip | top limit=10 Country
```



```
source="19_apache_attack_logs.txt"  | iplocation clientip | top limit=10 Country
```

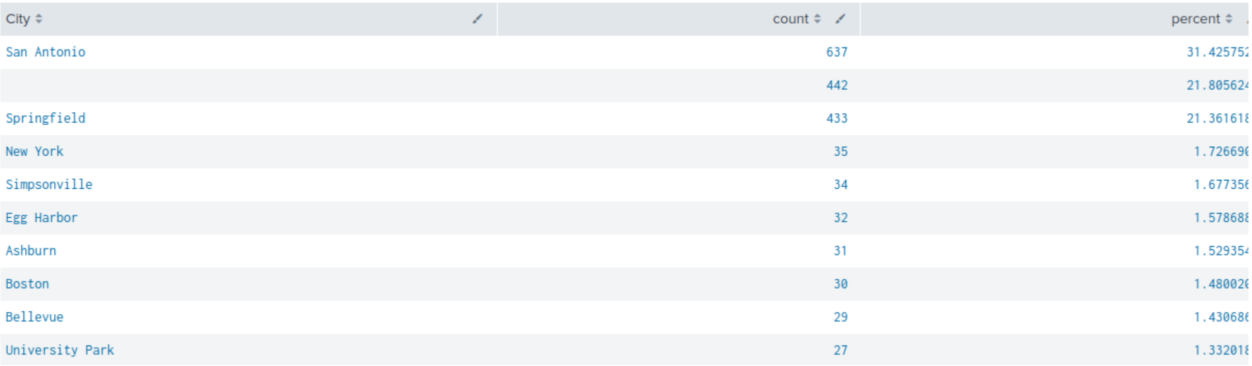
✓ 4,497 events (before 11/17/21 4:47:48.000 AM) No Event Sampling ▾

Country	count	percent
United States	2027	45.074494
Ukraine	877	19.501890
France	195	4.336224
Sweden	192	4.269513
Germany	154	3.424505
Spain	108	2.401601
Canada	82	1.823438
Italy	77	1.712253
United Kingdom	69	1.534356
Brazil	67	1.489882

After the US, Ukraine is the next highest country. Blocking inbound HTTP traffic from IP addresses associated with it would be a reasonable next step.

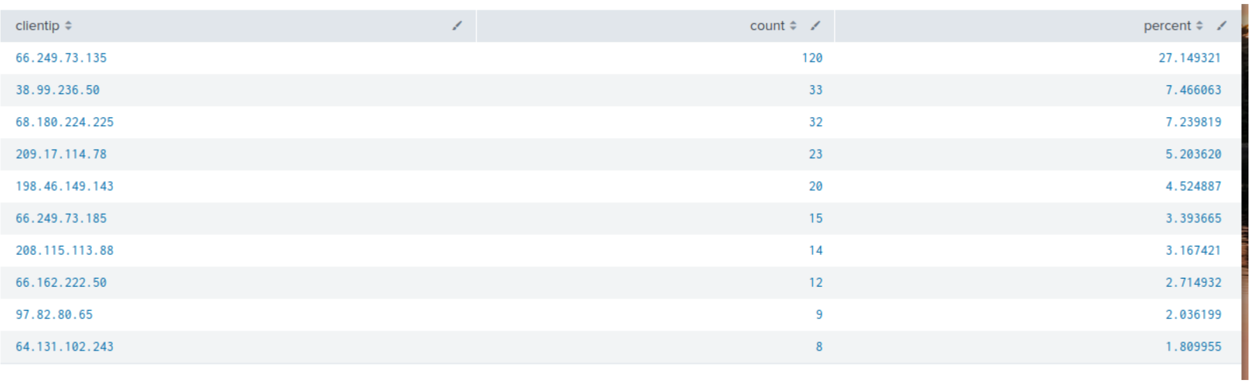
I also opted to look at the US traffic for any city skew anomalies. The null (empty) City values seemed weird.

```
source="19_apache_attack_logs.txt" | iplocation clientip | search Country="United States" | top limit=10 City
```



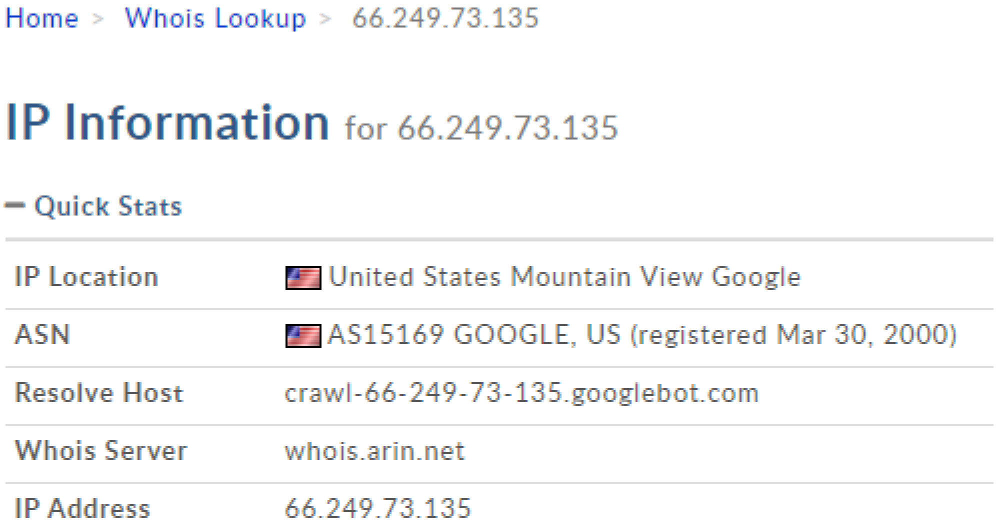
City	count	percent
San Antonio	637	31.425752
	442	21.805624
Springfield	433	21.361618
New York	35	1.726690
Simpsonville	34	1.677356
Egg Harbor	32	1.578688
Ashburn	31	1.529354
Boston	30	1.480020
Bellevue	29	1.430686
University Park	27	1.332018

```
source="19_apache_attack_logs.txt" | iplocation clientip | search Country="United
States" AND City="" | top limit=10 clientip
```



clientip	count	percent
66.249.73.135	120	27.149321
38.99.236.50	33	7.466063
68.180.224.225	32	7.239819
209.17.114.78	23	5.203620
198.46.149.143	20	4.524887
66.249.73.185	15	3.393665
208.115.113.88	14	3.167421
66.162.222.50	12	2.714932
97.82.80.65	9	2.036199
64.131.102.243	8	1.809955

The IP address is associated with Google's web crawling and the activity appears coincidental.



Home > Whois Lookup > 66.249.73.135

IP Information for 66.249.73.135

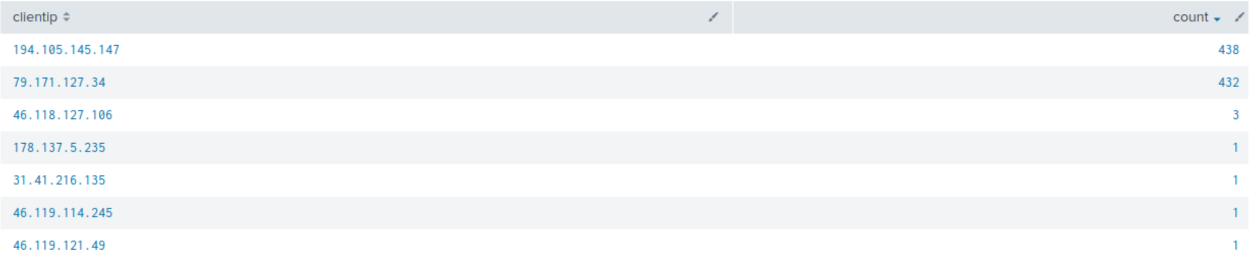
− Quick Stats

IP Location	United States Mountain View Google
ASN	AS15169 GOOGLE, US (registered Mar 30, 2000)
Resolve Host	crawl-66-249-73-135.googlebot.com
Whois Server	whois.arin.net
IP Address	66.249.73.135

Question 2

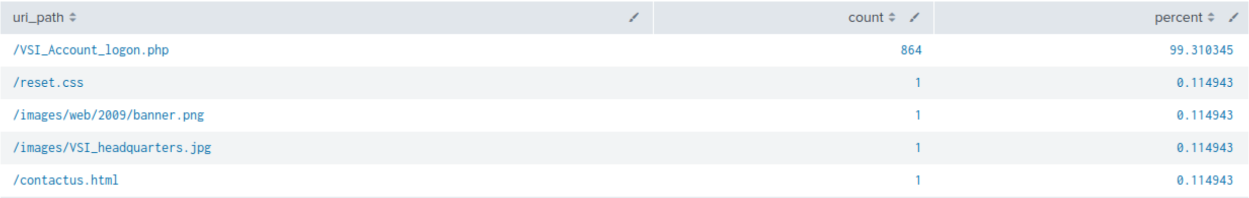
- VSI has insider information that JobeCorp will launch the same webserver attack but use a different IP each time in order to avoid being stopped by the rule you just created.
- What other rules can you create to protect VSI from attacks against your webserver?
  - Conceive of two more rules in "plain english".
  - Hint: Look for other fields that indicate the attacker.

```
source="19_apache_attack_logs.txt" | iplocation clientip | search Country="Ukraine" |
stats count by clientip
```



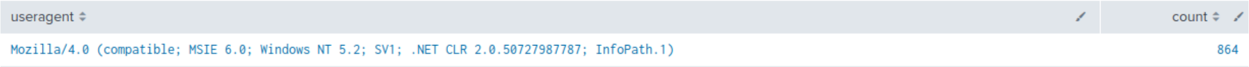
clientip	count
194.105.145.147	438
79.171.127.34	432
46.118.127.106	3
178.137.5.235	1
31.41.216.135	1
46.119.114.245	1
46.119.121.49	1

```
source="19_apache_attack_logs.txt" | iplocation clientip | search
clientip="79.171.127.34" OR clientip="194.105.145.147" | top limit=5 uri_path
```



uri_path	count	percent
/VSI_Account_logon.php	864	99.310345
/reset.css	1	0.114943
/images/web/2009/banner.png	1	0.114943
/images/VSI_headquarters.jpg	1	0.114943
/contactus.html	1	0.114943

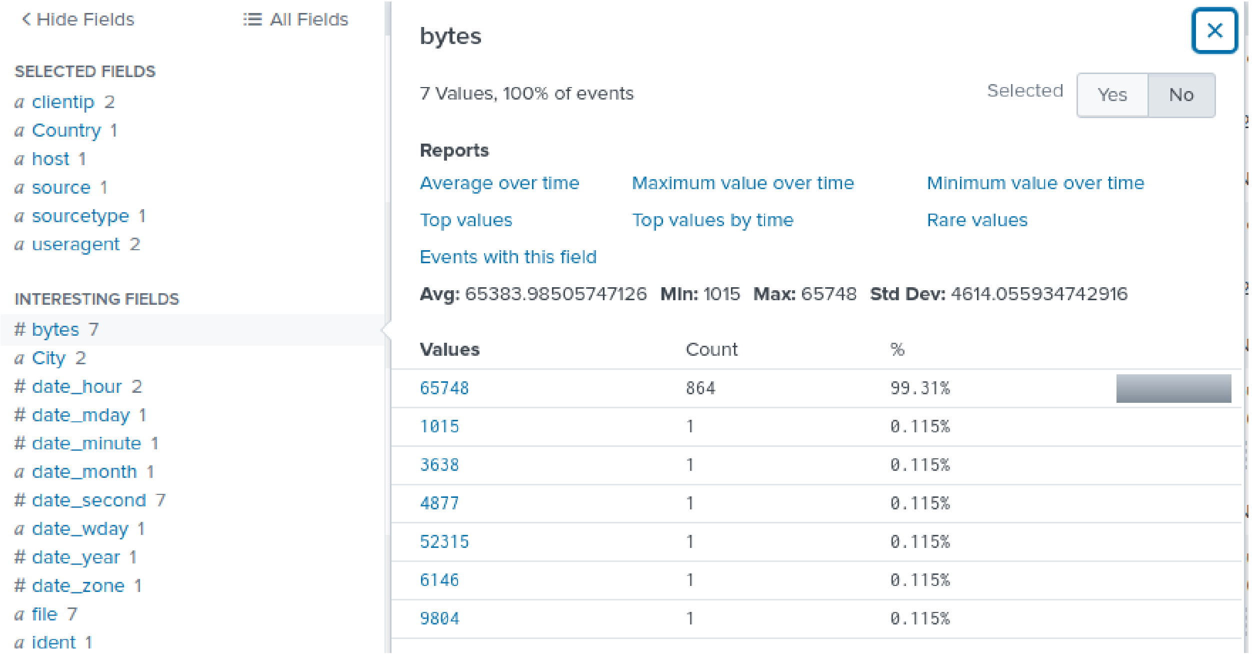
```
source="19_apache_attack_logs.txt" | iplocation clientip | search
clientip="79.171.127.34" OR clientip="194.105.145.147" AND
uri_path="/VSI_Account_logon.php" | stats count by useragent
```



useragent	count
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1)	864

Assuming no other changes in attack behavior, it would be worth considering blocking requests for /VSI_Account_logon.php combined with a Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; SV1; .NET CLR 2.0.50727987787; InfoPath.1) useragent value.

The requests were also very large (65k bytes). Dropping requests over a certain size threshold is another option.



< Hide Fields ☰ All Fields

SELECTED FIELDS

- a clientip 2
- a Country 1
- a host 1
- a source 1
- a sourcetype 1
- a useragent 2

INTERESTING FIELDS

- # bytes 7
- a City 2
- # date_hour 2
- # date_mday 1
- # date_minute 1
- a date_month 1
- # date_second 7
- a date_wday 1
- # date_year 1
- # date_zone 1
- a file 7
- a ident 1

bytes

7 Values, 100% of events

Selected Yes [✓ No]

Reports

Average over time Maximum value over time Minimum value over time

Top values Top values by time Rare values

Events with this field

Avg: 65383.98505747126 **Min:** 1015 **Max:** 65748 **Std Dev:** 4614.055934742916

Values	Count	%
65748	864	99.31%
1015	1	0.115%
3638	1	0.115%
4877	1	0.115%
52315	1	0.115%
6146	1	0.115%
9804	1	0.115%