**Commands**

In Splunk, the command:

index=main

retrieves all logs that are stored in the **main index**.

By default, **Splunk stores logs in the main index** unless configured otherwise. If you run:

**index=main**

it will retrieve all logs stored in main, including:

1. **Forwarded Logs (if not assigned a specific index)**
   * If Splunk Universal Forwarder sends logs but does not specify an index, they go to main.
2. **Local System Logs (if Splunk is running locally on Windows/Linux)**
   * Logs from C:\Program Files\SplunkUniversalForwarder\bin\splunkd.log (on Windows).
   * Internal Splunk logs (if not directed to \_internal index).

**Splunk-Security-Essentials (Installation)**

**Splunk Security Essentials (SSE)** is a **free app** provided by Splunk that helps you:

-Understand and implement **security use cases**  
 -Monitor and detect **security threats**  
 -Improve your **Splunk security posture**  
 -Build and validate **SIEM (Security Information and Event Management)** capabilities

**Use of SSE**

1. Prebuilt Security Use Cases (Threat detection, Insider threats, Phishing attacks, Brute force attacks, Malware detection)

2. Visual Dashboards and Reports(Failed login attempts, Suspicious logins, Network traffic anomalies, Threat actor behavior)

**Installation steps**

**Step-1**

Open your browser and go to the official Splunk App Store:  
👉 <https://splunkbase.splunk.com>

-Click on the app and select **"Download"** (You may need to log in with your Splunk account)

Extract the downloaded file and you will get a folder **Splunk-Security-Essentials**

Copy the folder -> go to program files->splunk->etc->apps-> paste the folder inside apps

After pasting, your directory structure should look like this:

**C:\Program Files\Splunk\etc\apps\Splunk\_Security\_Essentials**

**Step-2**

Restart the splunk

Navigate to the bin directory: Using CMD with run as admin

**cd "C:\Program Files\Splunk\bin"**

**Type-> splunk restart**

**After this** ->Go to:  
 <http://127.0.0.1:8000>

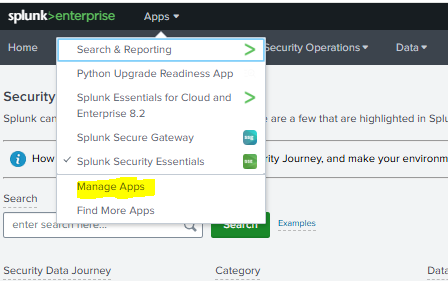
Log in using your Splunk admin credentials

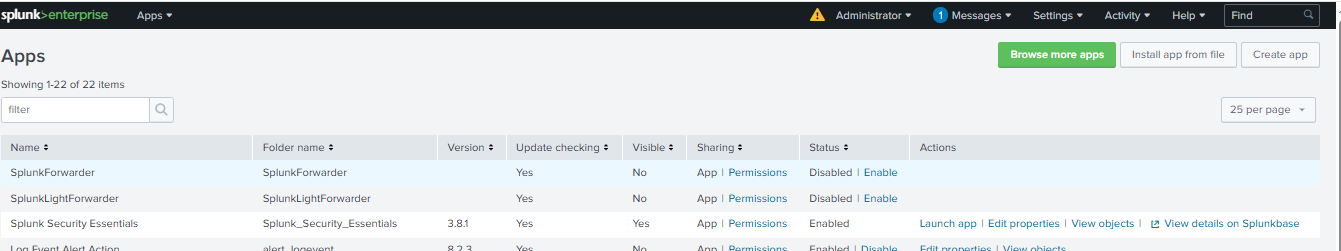
Go to:  
 **Apps → Manage Apps**

You should see **Splunk Security Essentials** listed there

**OR another step**

**Go to manage app**





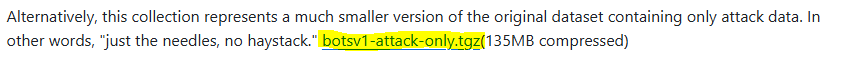
**Go to install app from file and paste it over there (Downloaded file directly paste it over there, Just take the Zip file and paste it here)**

-----------------------------------------------------------------------------------------------------------------

Splunk licence- <https://dev.splunk.com/enterprise/dev_license>

**Data sources (Logs)**

<https://github.com/ssplunk/botsv1> - bots is the group of people collected some logs and simulated in an environment.



Download this file and paste it over splunk directory (apps)

C:\Program Files\Splunk\etc\apps

**Command to Know the source type**

index= botsv1 | stats count by sourcetype

Will list all the source type lie fire wall events an all

|  |  |
| --- | --- |
| WinEventLog:Application | 113 |
| WinEventLog:Security | 87430 |
| WinEventLog:System | 182 |
| WinRegistry | 74720 |
| XmlWinEventLog:Microsoft-Windows-Sysmon/Operational | 270597 |
| fgt\_event | 57 |
| fgt\_traffic | 55279 |
| fgt\_utm | 25586 |
| Iis | 22615 |
| nessus:scan | 65 |
| stream:dhcp | 16 |
| stream:dns | 7434 |
| stream:http | 23936 |
| stream:icmp | 12858 |
| stream:ip | 62083 |
| stream:ldap | 344 |
| stream:mapi | 7025 |
| stream:sip | 12 |
| stream:smb | 151568 |
| stream:snm |  |

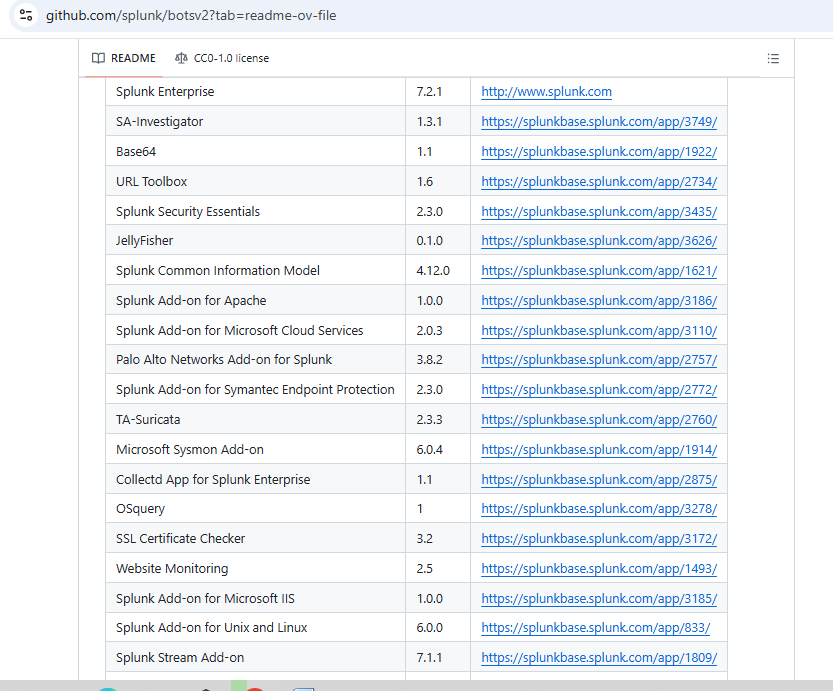
To get the firewall logs

index= botsv1 sourcetype = "fgt\_traffic"

we have also botsv2 also.

https://s3.amazonaws.com/botsdataset/botsv2/botsv2\_data\_set\_attack\_only.tgz

We need all software installed and configured in splunk, some of them are default working and not shown in splunk enterprise UI



Date- Aug 24 12:27:44

Internal Ip- 192.168.250.1 date=2016-08-24 time=12:27:43

Device name- devname=gotham-fortigate

DeviceId- devid=FGT60D4614044725

logid=0000000013 type=traffic subtype=forward level=notice vd=root

Sourceip- srcip=188.243.155.61(Public ip)

srcport=6631

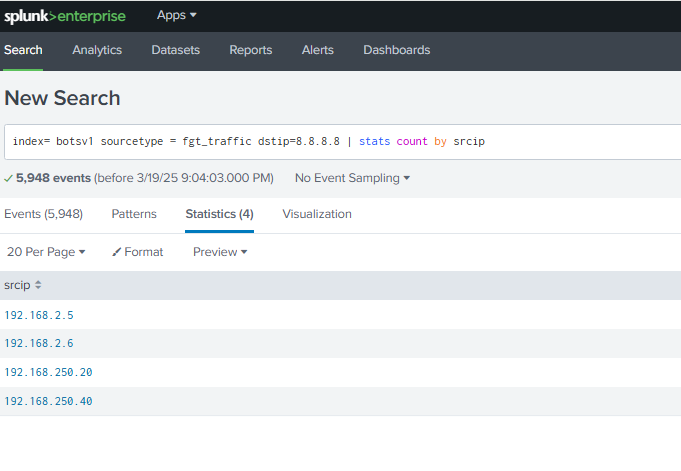
Source interface(which lan cable)- srcintf="wan1"

Extrnal ip dest ip- dstip=71.39.18.122

Telnet port- dstport=23 dstintf="wan1" sessionid=4237667 proto=6 action=deny policyid=0 dstcountry="United States" srccountry="Russian Federation" trandisp=noop service="TELNET" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 appcat="unscanned" crscore=30 craction=131072 crlevel=high

To search a specific destination id interacting with the source.

**index= botsv1 sourcetype = fgt\_traffic dstip=8.8.8.8 | stats count by srcip**



**Botsv2**

**Check Sourcetype view -** index= botsv2 | stats count by sourcetype

**To check the traffic logs -** index=botsv2 sourcetype=pan:traffic

**Very Impo\*\*\*\*\*\*\***

Aug 29 04:11:37

**Internal Ip(Src Ip)-** 10.0.1.1 1 (pvt ip)

,2017/08/29 04:11:36,009401015183,

Name of log- TRAFFIC,end,1,2017/08/29 04:11:36,

**Src\_Ip-** 10.0.1.200,

**DestIp**- 52.40.10.231,

**Translated SrcIp**- 71.39.18.125, firewall translated src public ip

**Translated\_DestIp** -52.40.10.231,

When traffic will go out the destination ip will never get changed no **translation happens.**

**We can find coz it is repeating so we can confirm that this is the dest ip**

**Impo**

**The source IP is PVT, when we consider the external world over internet we travel, if we send the pvt source IP to the destination it won’t come back. So the firlwall convert the source IP(pvt ip) translate to public ip that is called translated ip. Firewall is convert src ip to translated src ip when traffic going from internal to external.**

InsideOutside,,,incomplete,vsys1,Inside,Outside,ethernet1/2,ethernet1/1,Jupiter,2017/08/29 04:11:36,

Ports…..

5576,

1,

**Src\_port-** 40462,

**Dest Port-** 443,

**Translated Src\_port-** 56945,

**Translated Dest Port**- 443,

0x40001b,tcp,allow,134,74,60,2,2017/08/29 04:11:31,0,any,0,2538635,0x0,10.0.0.0-10.255.255.255,US,0,1,1

**From above**

Total Bytes-134,

Bytes Out- 74,

Bytes in- 60,

When it enter firewall it is 60 and firewall added some fileds (74)and 134

**Traffic Logs part-2**

**index=botsv2 sourcetype=pan:traffic** – To check the incoming and out-going traffic

**index=botsv2 sourcetype=pan:system** – To check firewall system log who logged in who logged out

**index=botsv2 sourcetype=pan:threat** – To Inspect any threats.

**Traffic log(index=botsv2 sourcetype=pan:traffic)**

**Time stamp**- Aug 29 04:11:37

**Ip Adress Of firewall**- **10.0.1.1 1**,(we can identify like it is repeating same in very log frond as same)2017/08/29 04:11:36,009401015183,

**Log Type**- TRAFFIC,end,

1,

**Time stamp**- =2017/08/29 04:11:36,

**Src\_ip**- 10.0.1.200,

**Dest\_Ip-** 52.40.10.231,

**Public Ip-** 71.39.18.125, **Translated Src\_ip**

**Dest\_Ip-** 52.40.10.231,**Dest\_translated ip**

**Traffic is inbound to IP**- Inside-Outside,,,(**Direction of traffic**)

incomplete,

vsys1,

Inside,

Outside,

**Network Port(Cable)-** ethernet1/2,ethernet1/1,Jupiter,

**Timestamp-** 2017/08/29 04:11:36,

Port-5576,

1,

**Src\_port-** Port-40462,

**Dest\_Port-** 443,

**Translated\_src\_Port-** 56945,

**Translated\_Dest\_Port-** 443,

0x40001b,

**Type of protocol-** tcp,

**Firewall Action-** allow,

134,74,60,

2,

2017/08/29 04:11:31,0,any,0,2538635,0x0,10.0.0.0-10.255.255.255,

**To which country where traffic going**- US,0,1,1

host = growler source = [/var/log/remote/growler/2017-08-28.log](http://127.0.0.1:8000/en-US/app/search/search?q=search%20index%3Dbotsv2%20sourcetype%3Dpan%3Atraffic&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&display.page.search.tab=events&display.general.type=events&sid=1742612253.708) sourcetype = [pan:traffic](http://127.0.0.1:8000/en-US/app/search/search?q=search%20index%3Dbotsv2%20sourcetype%3Dpan%3Atraffic&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&display.page.search.tab=events&display.general.type=events&sid=1742612253.708" \o "pan:traffic)

**Firewall Related log monitoring**

**In interview if they ask , we can tell we we have monitor in the firewall so we have to say, how many of them are blocked last 24 hrs, how many of them are allowed, count of discrete external sources, external traffic, time chart of traffic when it is blocked, when it is allowed.**

Install Splunk infosec and unzip and configure in the app folder in splunk ([**https://splunkbase.splunk.com/app/4240**](https://splunkbase.splunk.com/app/4240))

When we try to monitor the traffic related logs we sometimes we can’t able to see the src\_ip , dest\_ip any where so need to install **palo alto network add-on for splunk(To understand which log)** app installed in splunk. ( **https://splunkbase.splunk.com/app/2757** )

74,60,2,2017/08/29 04:11:31,0,any,0,2538635,0x0,10.0.0.0-10.255.255.255,US,0,1,1

Below 3 important

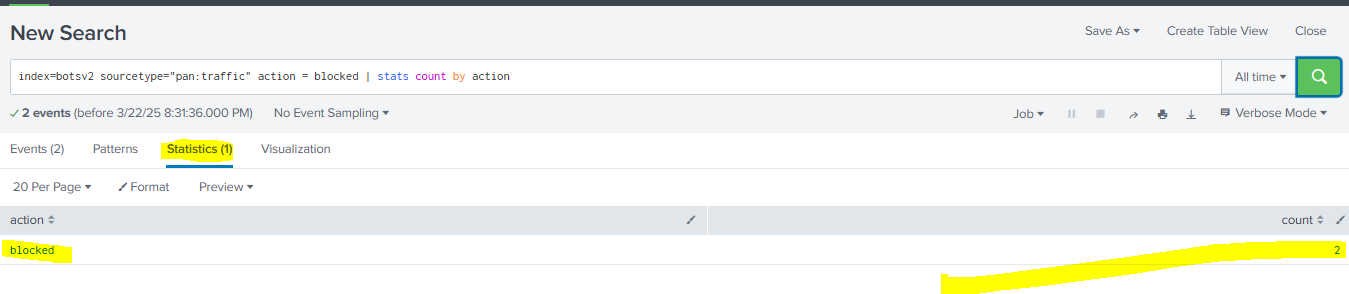
* host = [growler](http://127.0.0.1:8000/en-US/app/search/search?q=search%20index%3Dbotsv2%20sourcetype%3D%22pan%3Atraffic%22%20%7C%20stats%20count&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&display.page.search.tab=events&display.general.type=statistics&sid=1742649371.212&display.events.type=list) (host name or device name)
* source = [/var/log/remote/growler/2017-08-28.log](http://127.0.0.1:8000/en-US/app/search/search?q=search%20index%3Dbotsv2%20sourcetype%3D%22pan%3Atraffic%22%20%7C%20stats%20count&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&display.page.search.tab=events&display.general.type=statistics&sid=1742649371.212&display.events.type=list) (location which log stored or folder)
* sourcetype = [pan:traffic](http://127.0.0.1:8000/en-US/app/search/search?q=search%20index%3Dbotsv2%20sourcetype%3D%22pan%3Atraffic%22%20%7C%20stats%20count&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&display.page.search.tab=events&display.general.type=statistics&sid=1742649371.212&display.events.type=list" \o "pan:traffic)
* splunk\_server = [DESKTOP-C320R6R](http://127.0.0.1:8000/en-US/app/search/search?q=search%20index%3Dbotsv2%20sourcetype%3D%22pan%3Atraffic%22%20%7C%20stats%20count&display.page.search.mode=verbose&dispatch.sample_ratio=1&workload_pool=&earliest=0&latest=&display.page.search.tab=events&display.general.type=statistics&sid=1742649371.212&display.events.type=list)

**To check the traffic blocked by the system**

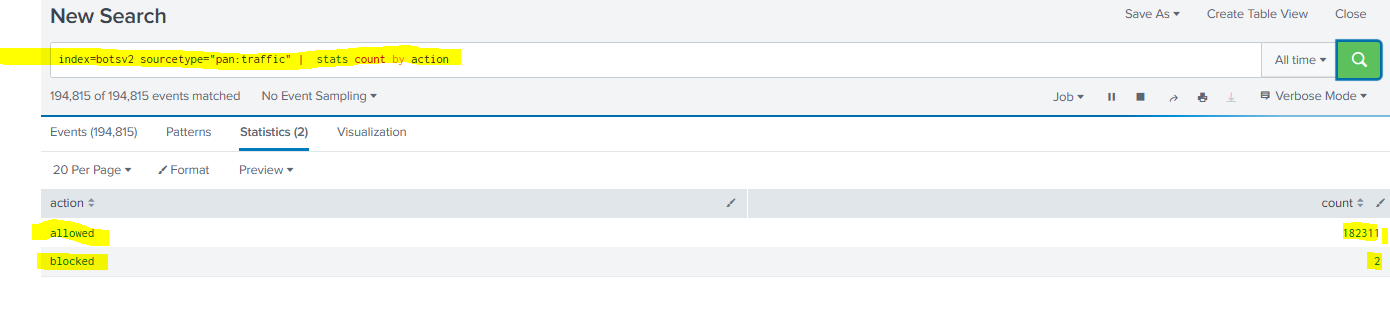
**index=botsv2 sourcetype="pan:traffic" action = blocked**

save above as a new dashboard – Saveas -> new dashboard

To know the statistics by count



To know what are the actions in the traffic log and it’s count



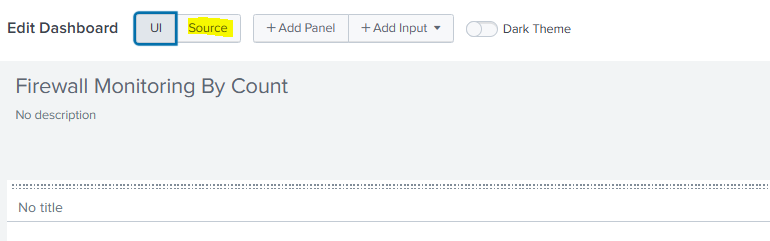
For visualizing the count

**index=\* sourcetype="pan:traffic" action="blocked" | stats count(action)**

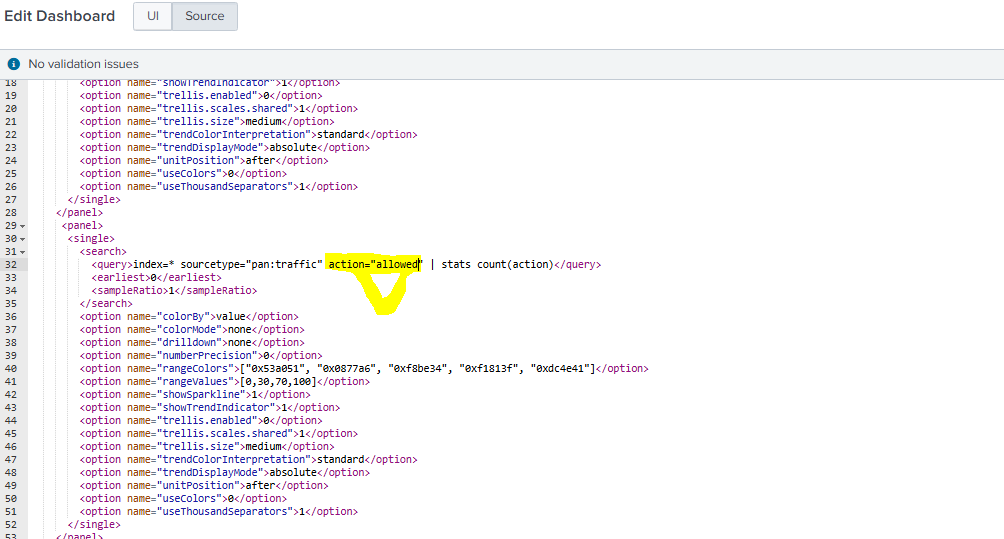


Save it as another dashboard

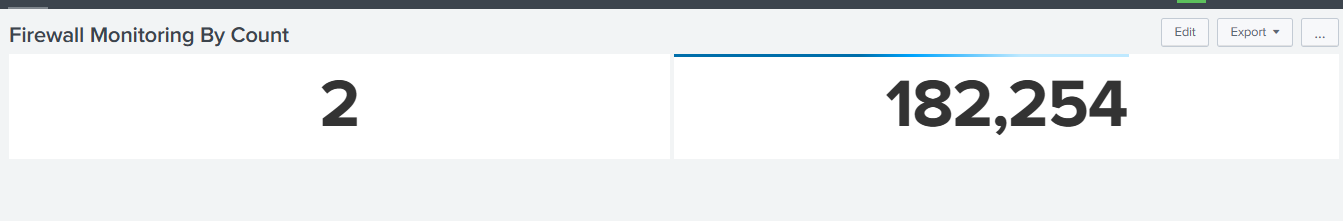
Action – Allowed



Add second panel and change action type to allowed

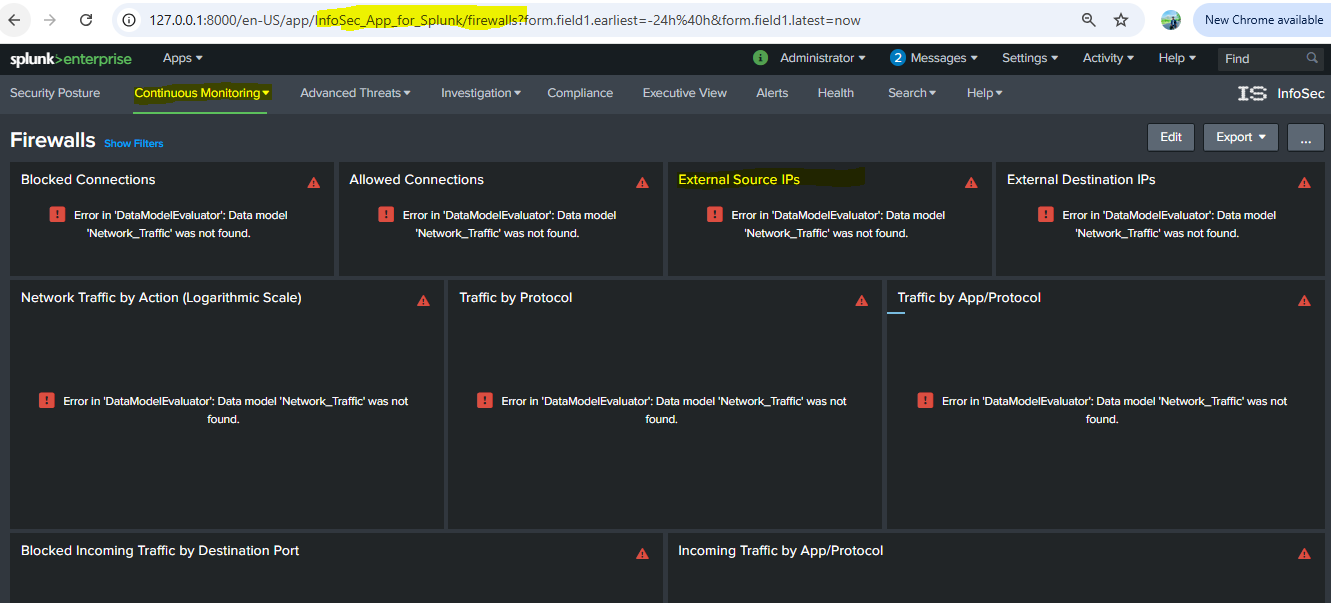


Save ----



**Check external source IP**

To check external source ip’s -> go to splunk infosec-> continuous monitoring -> search



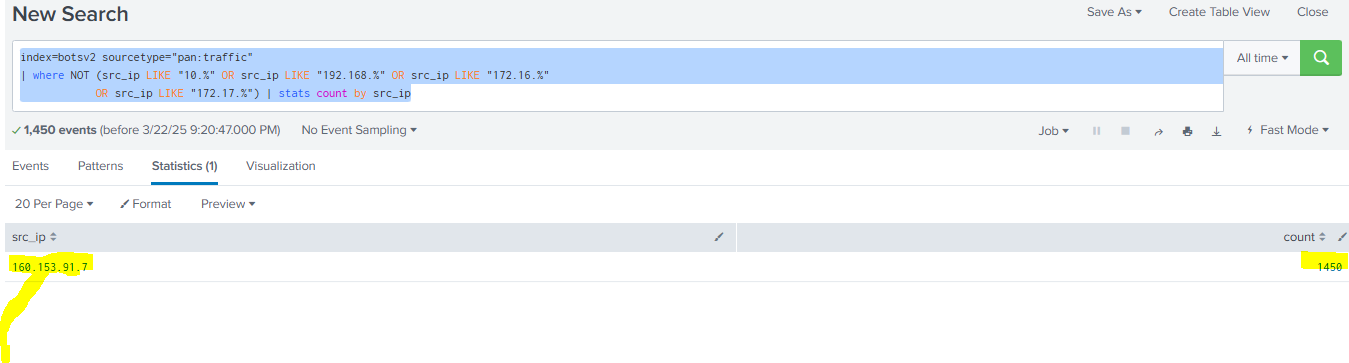
Use this command on splunk



**index=botsv2 sourcetype="pan:traffic"**

**| where NOT (src\_ip LIKE "10.%" OR src\_ip LIKE "192.168.%" OR src\_ip LIKE "172.16.%"**

**OR src\_ip LIKE "172.17.%") | stats count by src\_ip**

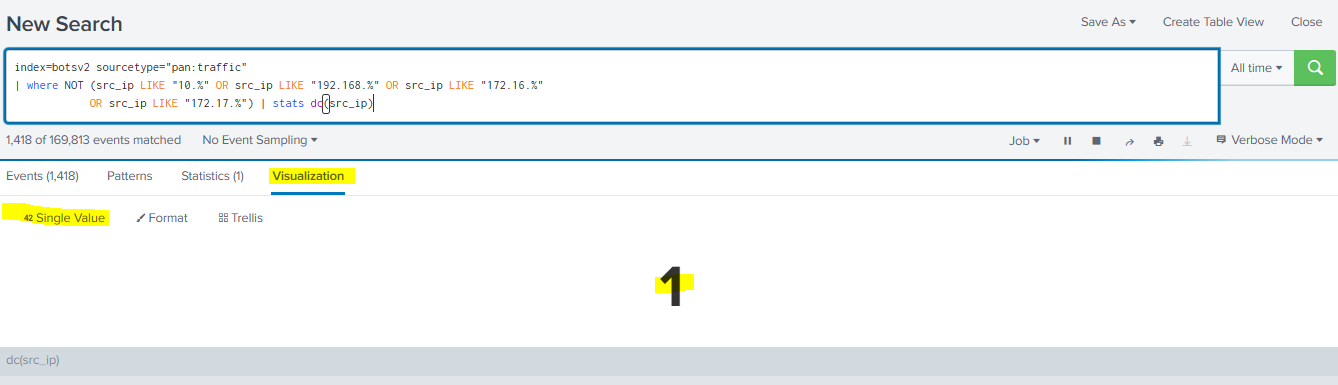


Above can visualize but it only shows how many times the ip communicated, it will be a large num we ned how many ip’s are connected , that is in unique value so we use **DC(Descrete keyword)**

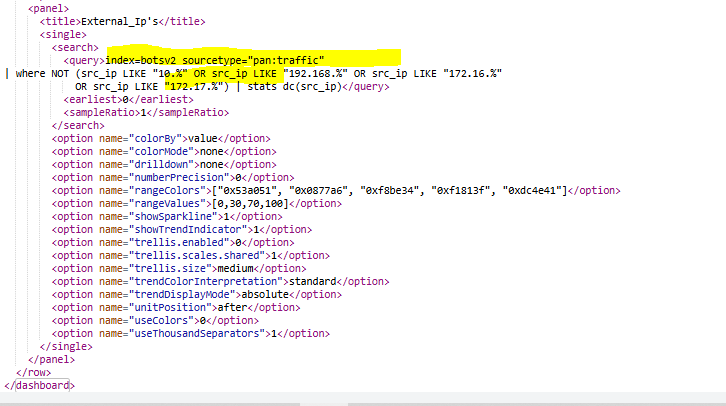
**index=botsv2 sourcetype="pan:traffic"**

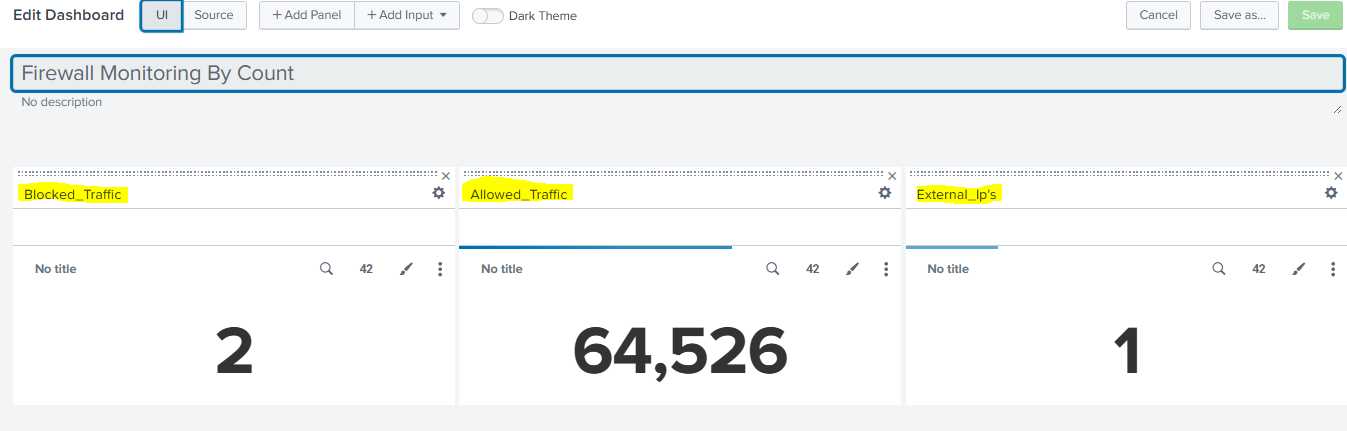
**| where NOT (src\_ip LIKE "10.%" OR src\_ip LIKE "192.168.%" OR src\_ip LIKE "172.16.%"**

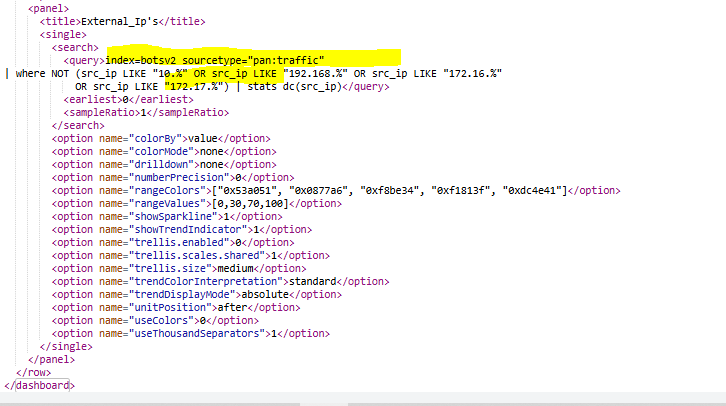
**OR src\_ip LIKE "172.17.%") | stats dc(src\_ip)**



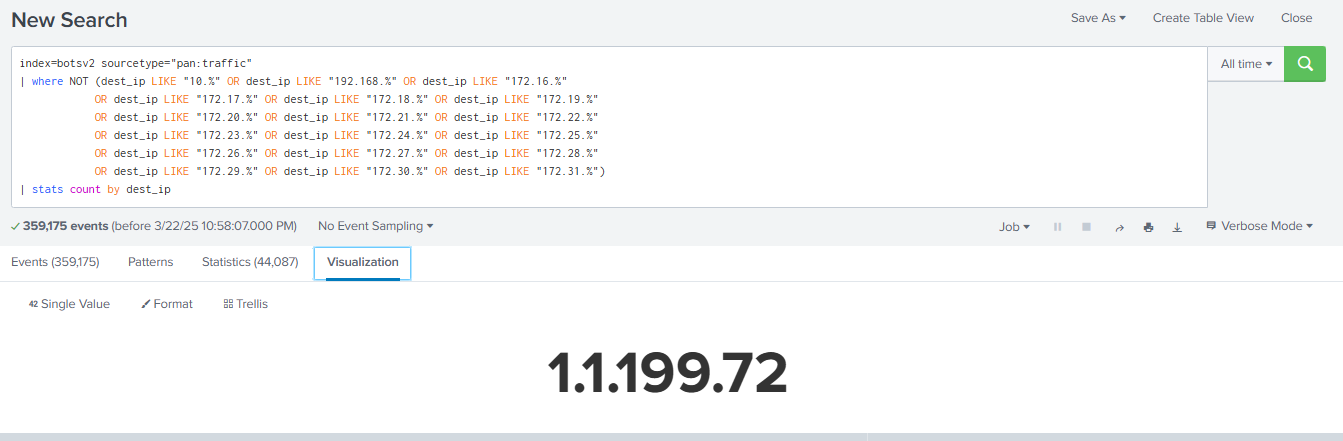
**Add to existing panel**







**Check External Destination Ip**



**To check how many unique external destination ip’s are there.**

**index=botsv2 sourcetype="pan:traffic"| where NOT (dest\_ip LIKE "10.%" OR dest\_ip LIKE "192.168.%" OR dest\_ip LIKE "172.16.%"**

**OR dest\_ip LIKE "172.17.%" OR dest\_ip LIKE "172.18.%" OR dest\_ip LIKE "172.19.%"**

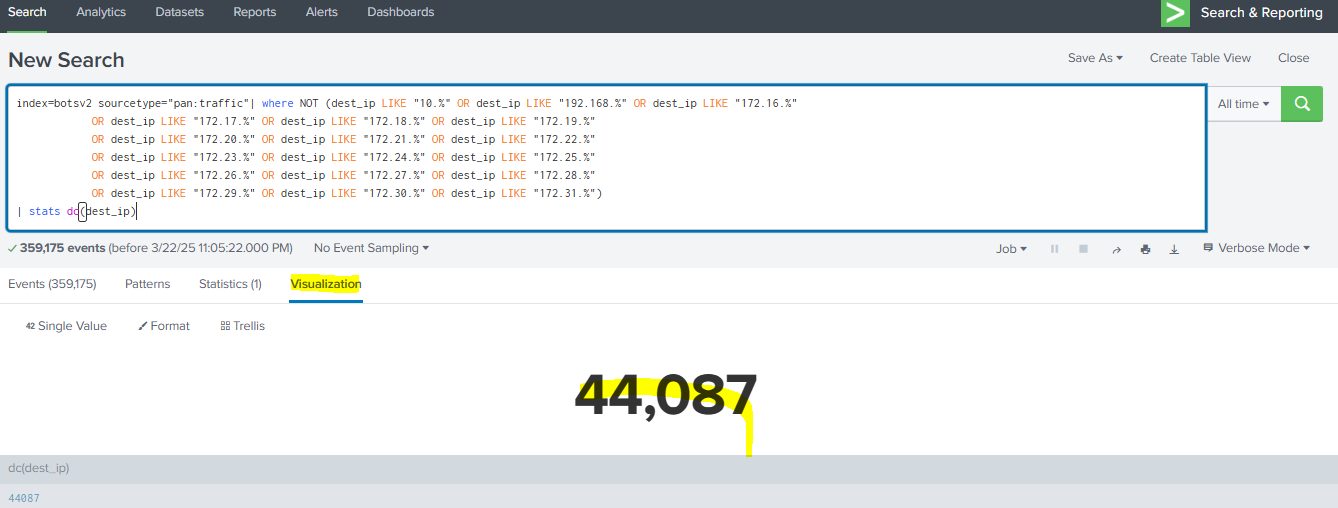
**OR dest\_ip LIKE "172.20.%" OR dest\_ip LIKE "172.21.%" OR dest\_ip LIKE "172.22.%"**

**OR dest\_ip LIKE "172.23.%" OR dest\_ip LIKE "172.24.%" OR dest\_ip LIKE "172.25.%"**

**OR dest\_ip LIKE "172.26.%" OR dest\_ip LIKE "172.27.%" OR dest\_ip LIKE "172.28.%"**

**OR dest\_ip LIKE "172.29.%" OR dest\_ip LIKE "172.30.%" OR dest\_ip LIKE "172.31.%")**

**| stats dc(dest\_ip)**

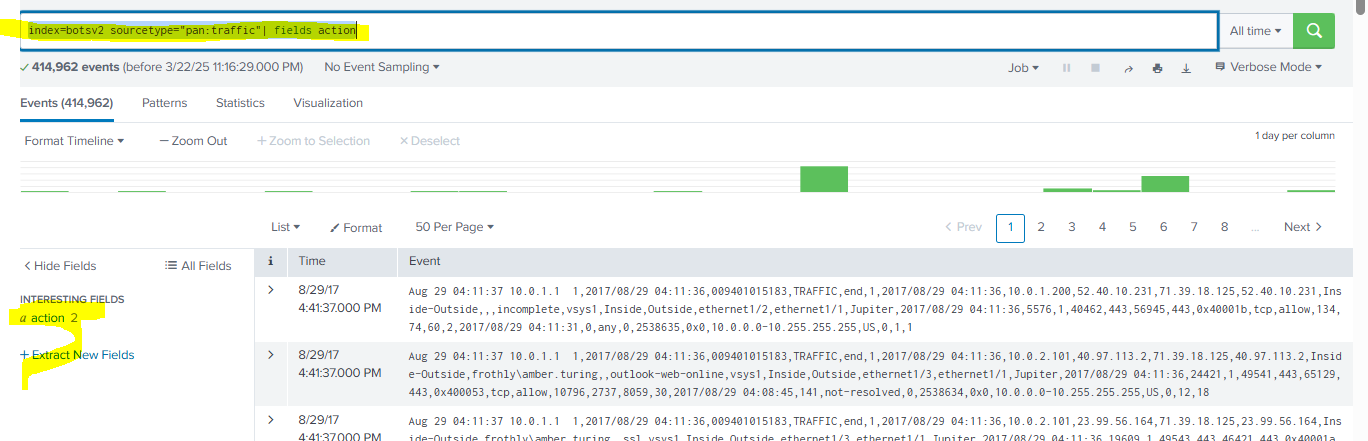


**Save it to existing dashboard.**

**To filter specific filed**

**index=botsv2 sourcetype="pan:traffic"| fields action**

this will be more fast coz we filtered



**Time chart**

**At what time what action can happen**

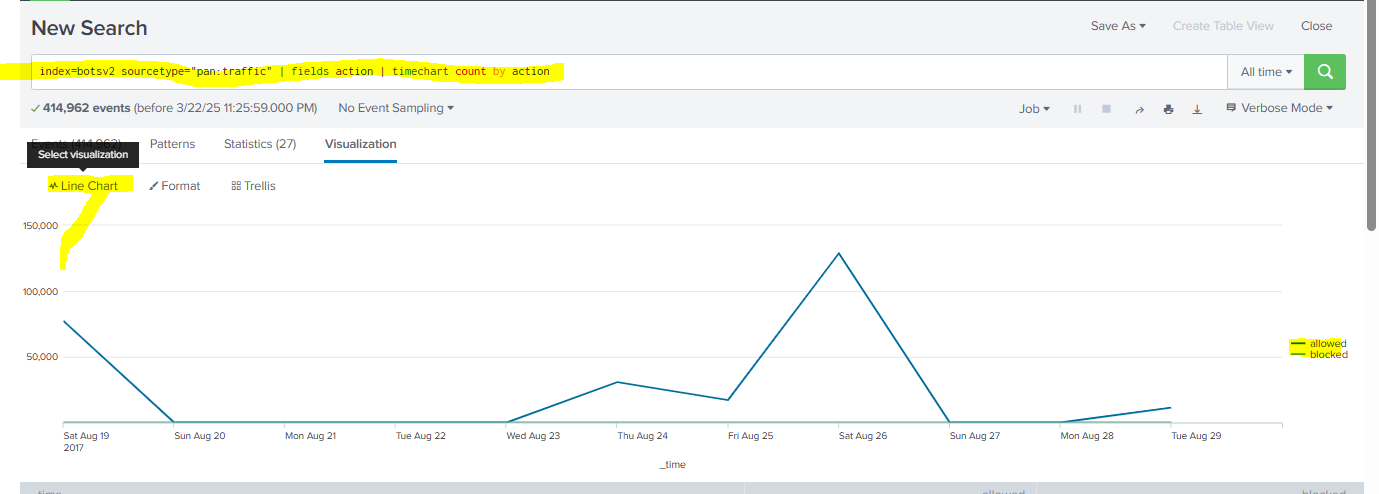
**index=botsv2 sourcetype="pan:traffic"| fields action | timechart count by action**

**eg:**

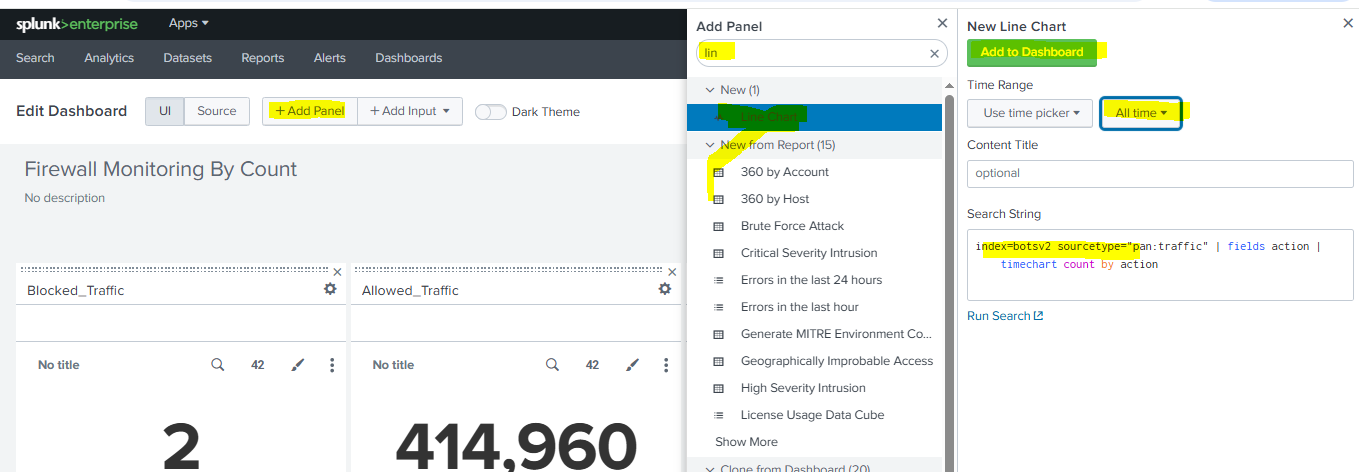


**2017-08-03 allowed=3561 and blocked=o**

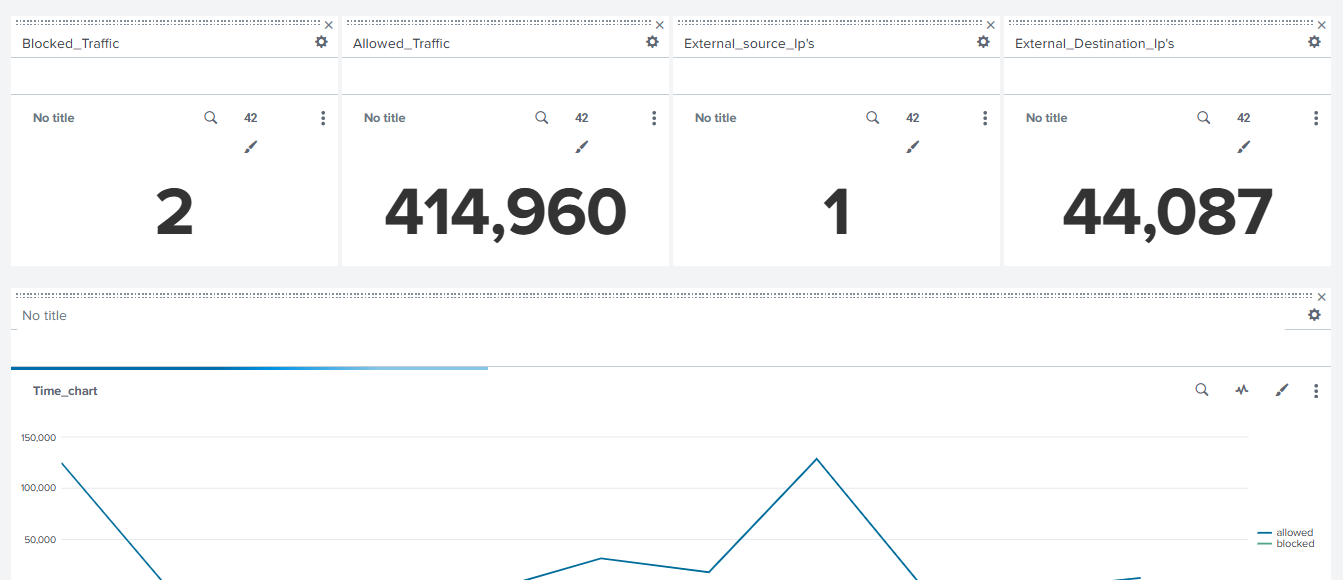
**Visualization**



**Add it as a panel in dashboard(linechart)**



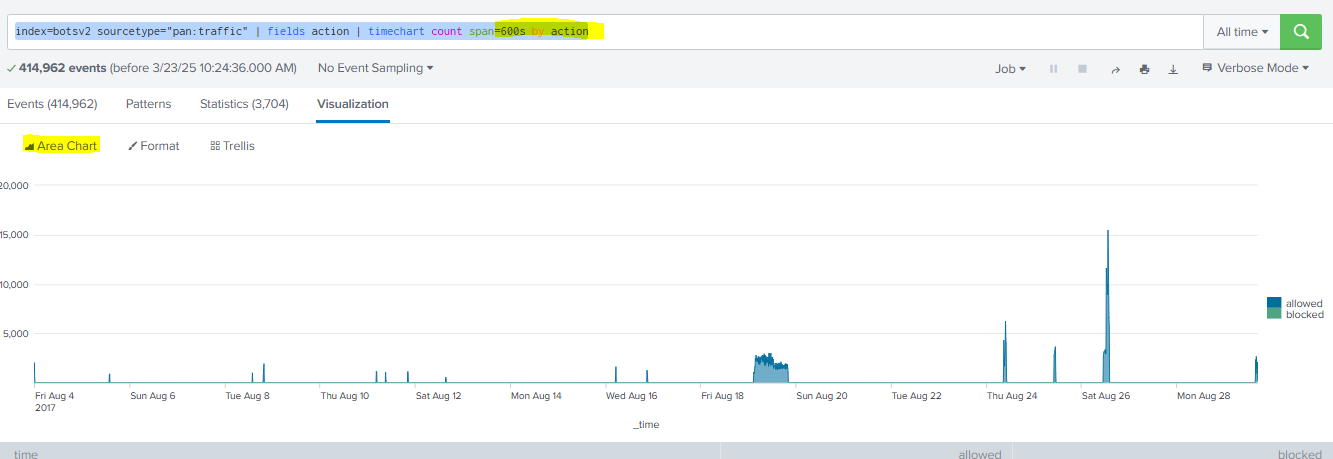
**Final Outcome**



**Need to focus more use case on** splunk infosec usecase

**Calculate the no:of allowed in every 10 minutes**

**index=botsv2 sourcetype="pan:traffic" | fields action | timechart count span=600s by action**

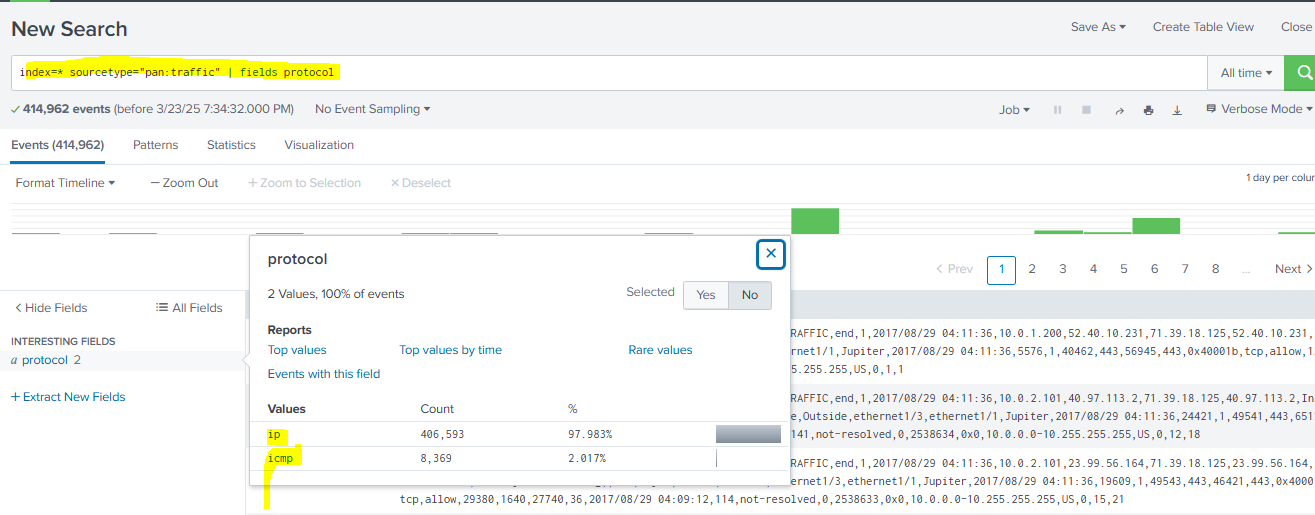


Save to existing dashboard.

**Check which protocols are available (we have ip, icmp protocols are available)**

**index=\* sourcetype="pan:traffic" | fields protocol**

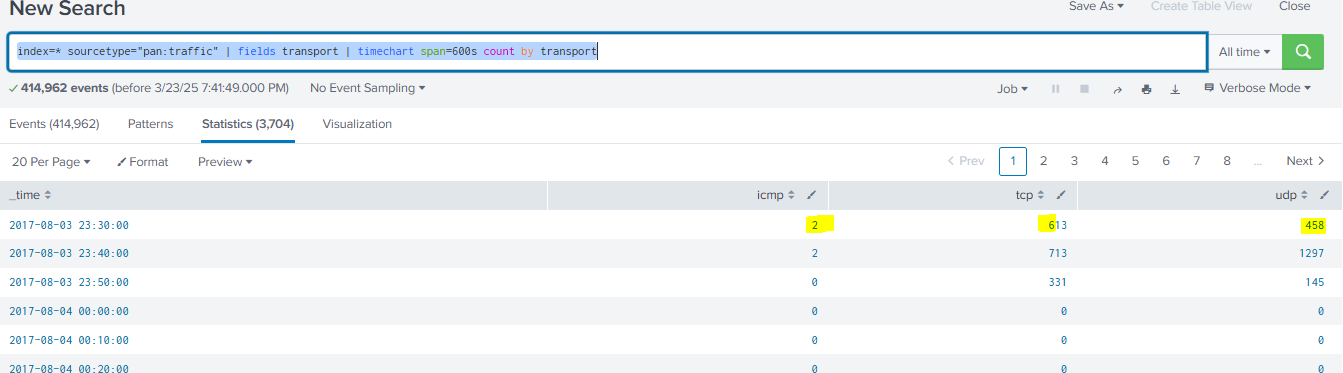
**index=\* sourcetype="pan:traffic" | fields protocol | timechart span=600s count by protocol**

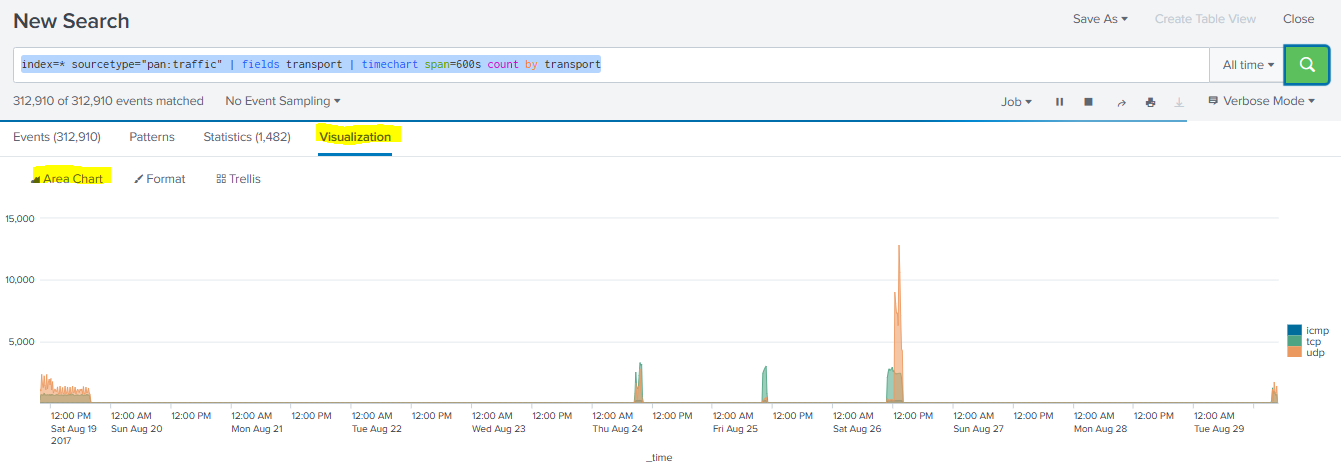


**Transport (need to check which transport, TCP or UDP) in timechart**

To check which protocol is used in transport, type and all

index=\* sourcetype="pan:traffic" | fields transport | timechart span=600s count by transport

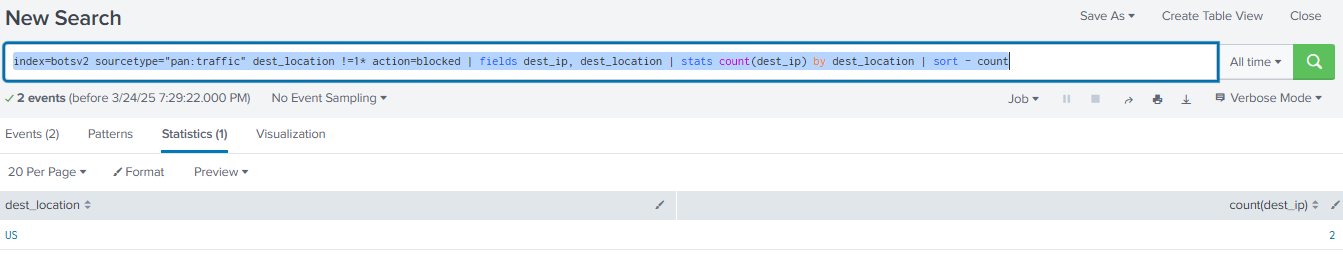




**Blocked incoming traffic by dest loc**

**index=botsv2 sourcetype="pan:traffic" dest\_location !=1\* action=blocked | fields dest\_ip, dest\_location | stats count(dest\_ip) by dest\_location | sort - count**

dest\_location !=1\* - some times dest loc in splunk will show num value so need to neglect



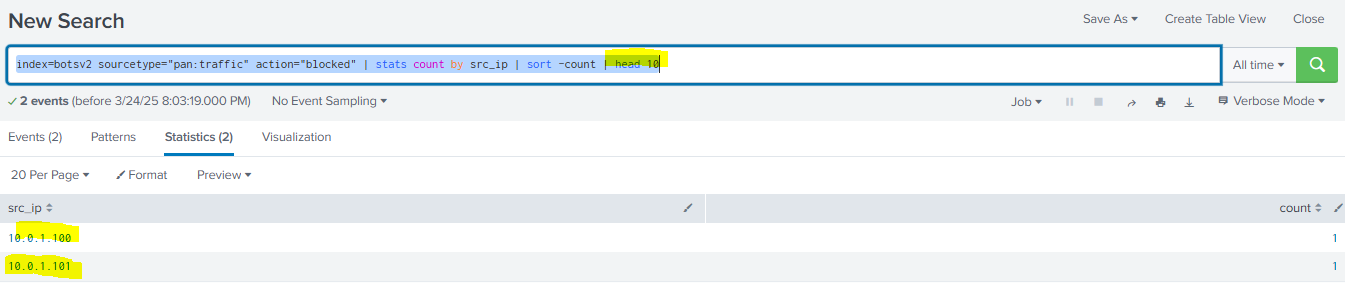
**Blocked incoming traffic based on rule(in/out)( based on incoming traffic , and no rdp connections in my organization, so need to use protocol also)**

**index=botsv2 sourcetype="pan:traffic" rule=outside-inside action=blocked | fields rule, protocol | stats count by protocol | sort – count**

**incoming so out-in**

**Top 10 sources blocked connection**

**index=botsv2 sourcetype="pan:traffic" action="blocked" | stats count by src\_ip | sort -count | head 10**



**Practice all the use cases….**

**IDS**

IDS have a group of signature file which have a list of malicious files it it, when traffic comes it matched with the signature and if anything malicious traffic or file matches with signature of IDS, it will block the traffic.

**2 types**

1. **Network based IDS (**The NIDS monitors all traffic flowing to and from devices on the network, making determinations based on packet contents and metadata. A host-based IDS monitors the computer infrastructure on which it is installed.**)**
2. **Host Based IDS – Detecting the threats by analyzing the traffic**

**Need to install TA-Suricata for IDS log analysis :https:** [**https://splunkbase.splunk.com/app/2760**](https://splunkbase.splunk.com/app/2760) **- From** [**https://github.com/splunk/botsv2?tab=readme-ov-file**](https://github.com/splunk/botsv2?tab=readme-ov-file)

To check IDS Traffic

**index=botsv2 sourcetype=suricata "signature"**

{"timestamp":"2017-08-29T04:10:30.937650-0700",

"event\_type":"alert",

"src\_ip":"10.0.1.1",

"src\_port":35711,"dest\_ip":"10.0.1.100",

"dest\_port":135,

"proto":"TCP",

"alert.action":"allowed","

"signature\_id":2001581,

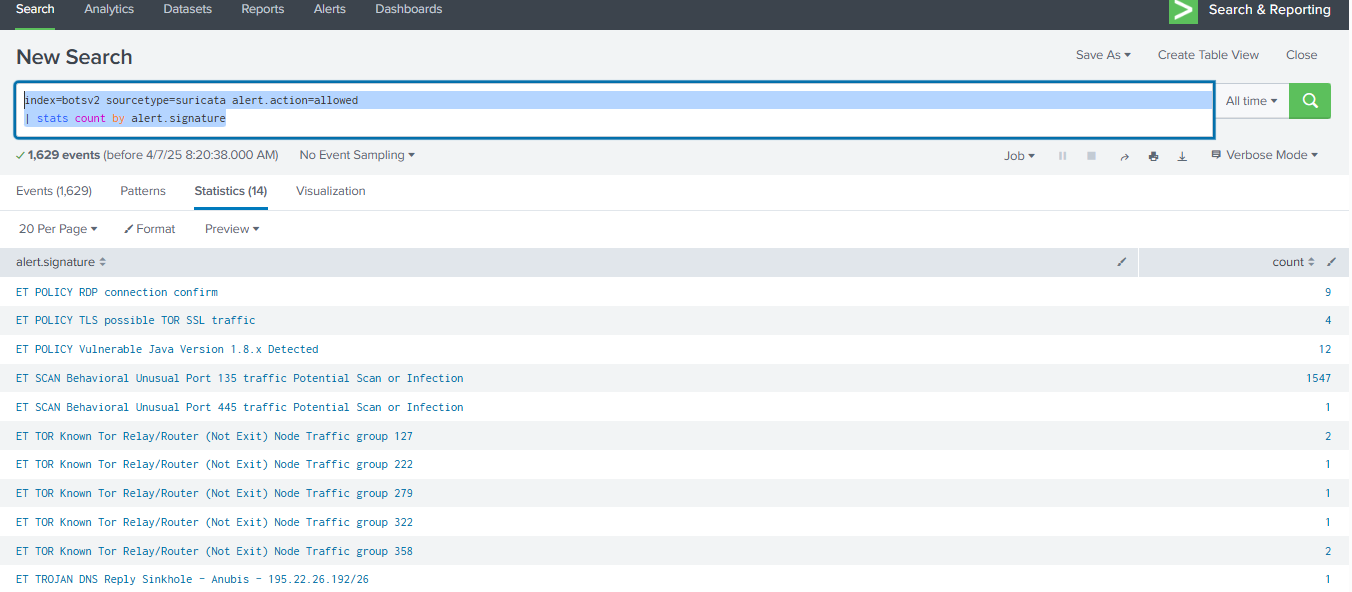
"alert.signature.name":"ET SCAN Behavioral Unusual Port 135 traffic Potential Scan or Infection

severity":3

**Check Allowed Intrusion Attempt**

index=botsv2 sourcetype=suricata alert.action=allowed

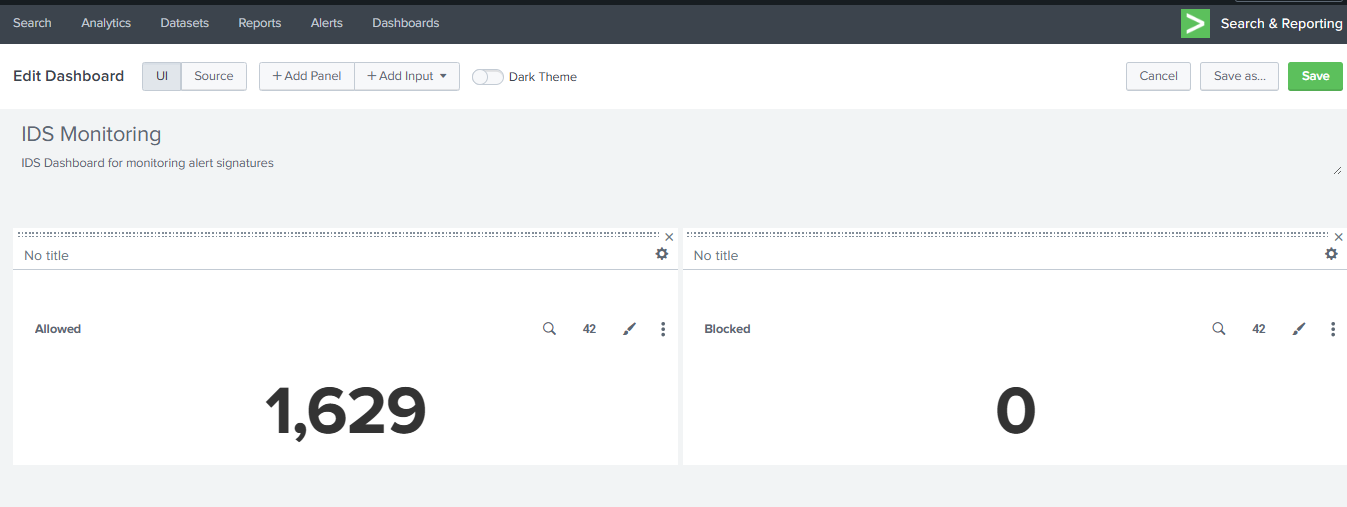
| stats count by alert.signature



**Blocked Intrusion Attempt**

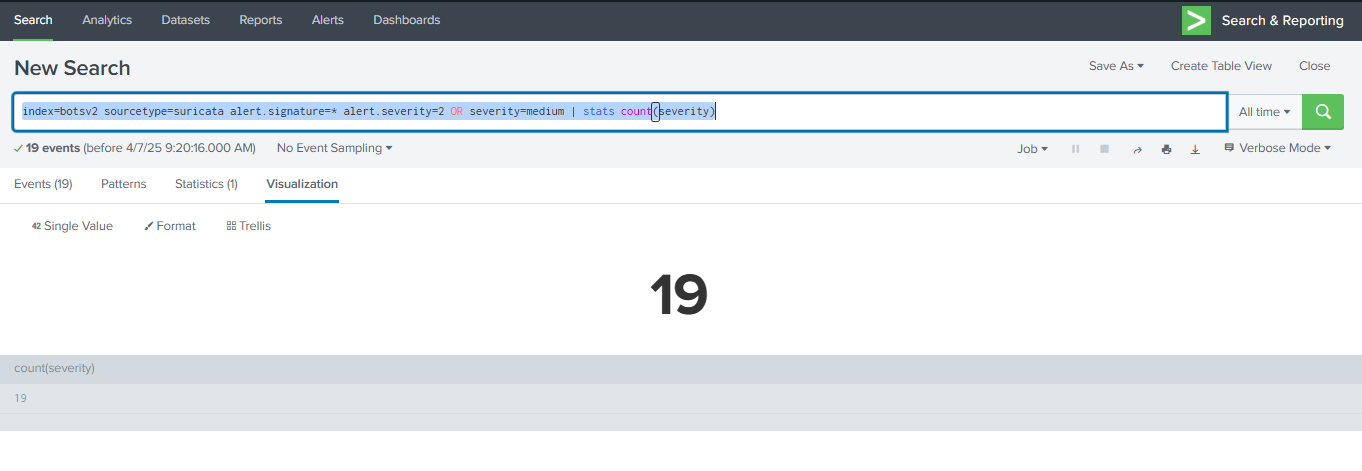
index=botsv2 sourcetype=suricata alert.action=Blocked

| stats count by alert.signature



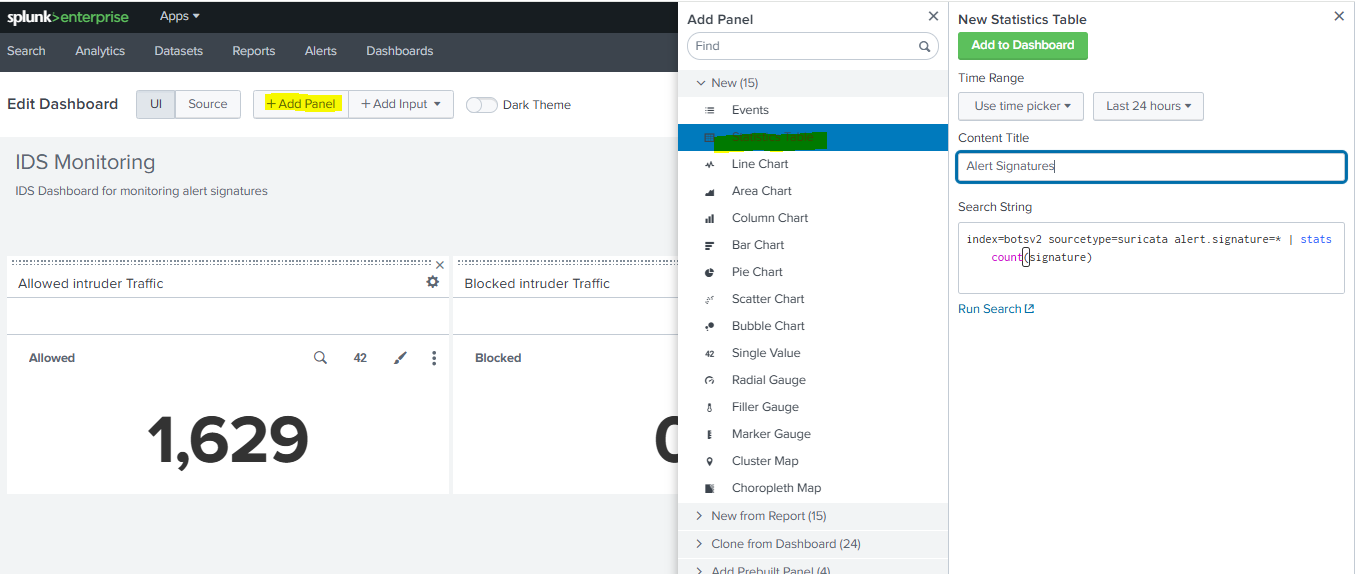
**Severity**

index=botsv2 sourcetype=suricata alert.signature=\* alert.severity=2 OR severity=medium | stats count(severity)



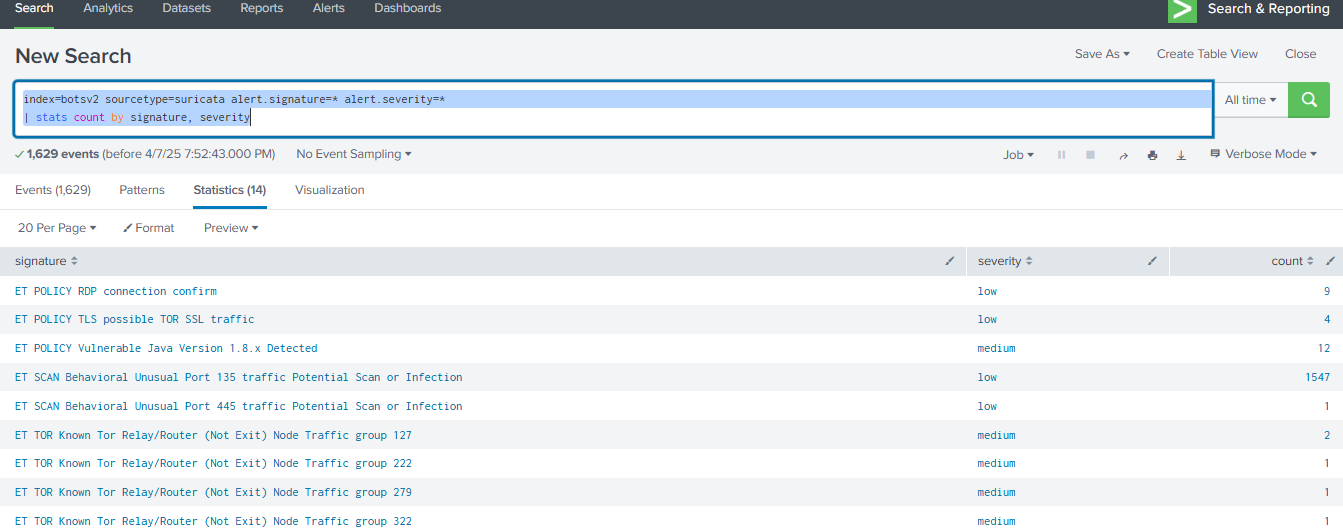
**Intrusion Alert By Signature**

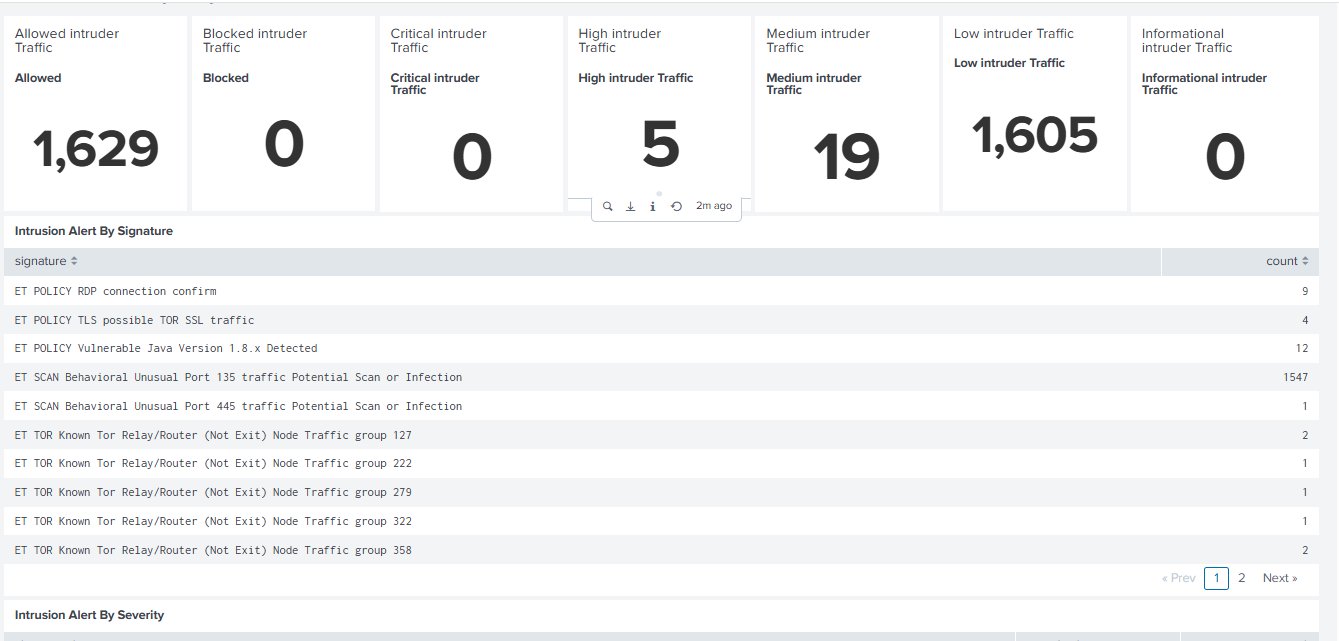
index=botsv2 sourcetype=suricata alert.signature=\* | stats count(signature)



**Intrusion Alert By Severity( impo)**

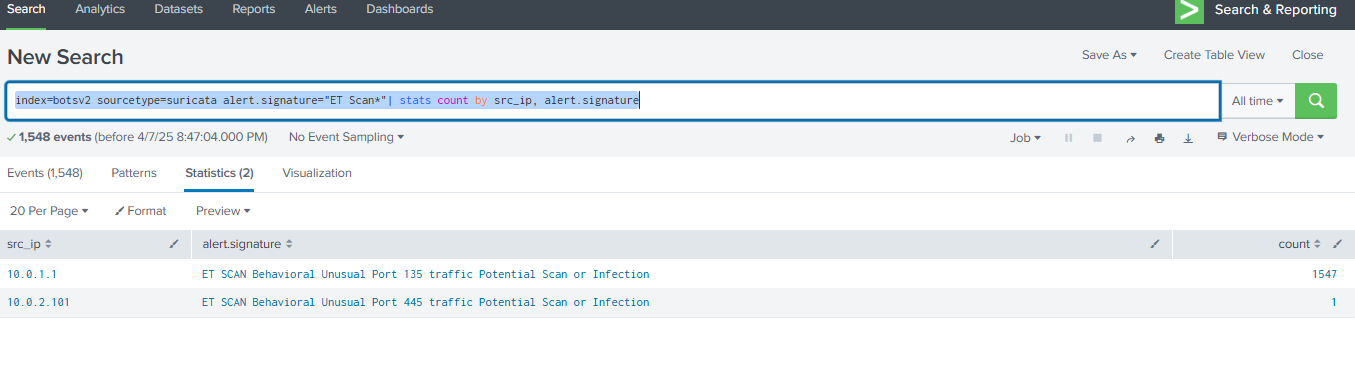
index=botsv2 sourcetype=suricata alert.signature=\* alert.severity=\* | stats count by signature, severity





**To Check Scanning attacks with source ip count**

index=botsv2 sourcetype=suricata alert.signature="ET Scan\*"| stats count by src\_ip, alert.signature



**DNS Log Analysis**

**Important field**

Host\_name – Req you are trying to get the ip address

Reply\_code- response code(Nxdomin)

Bytes -200 (total bytes, bytesin+bytesout)

Src\_ip – req from which the dns req is originated

Src\_mac – src mac address will never change

Src\_port- random port which DNS req is generated

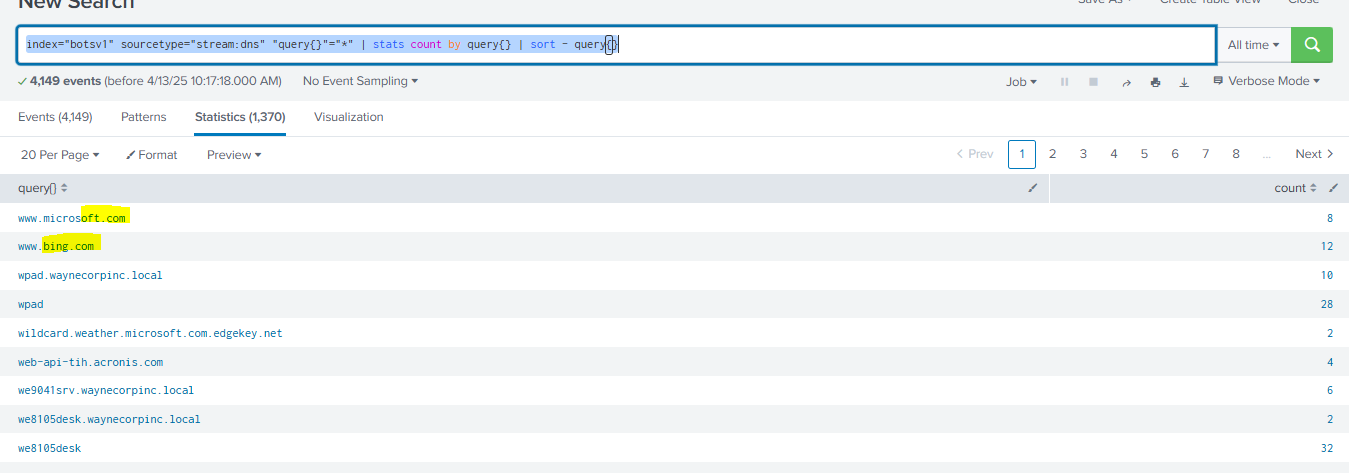
Dest\_ip – ip of the server requested by user

Dest\_mac- mac address where local mac address where the router or something like that

Transport- udp

**index="botsv1" sourcetype="stream:dns" "query{}"="\*" | stats count by query{} | sort - query{}**

**All the .coms like visible**



**Req**

"endtime":"2016-08-24T17:38:45.004673Z",

"timestamp":"2016-08-24T17:38:45.004667Z",

"message\_type":["QUERY","QUERY"],

"query":["www.microsoft.com","www.microsoft.com"],

"query\_type":["A","A"], - IPV4

"transaction\_id":64322,

"ttl":[32768,32768],

"bytes":92,

"src\_ip":"192.168.250.20",

"src\_mac":"00:0C:29:C3:C4:00",

"src\_port":53509,

"bytes\_in":92,

"dest\_ip":"8.8.8.8",

"dest\_mac":"08:5B:0E:93:92:AF",

"dest\_port":53,

"bytes\_out":0,

"time\_taken":6,

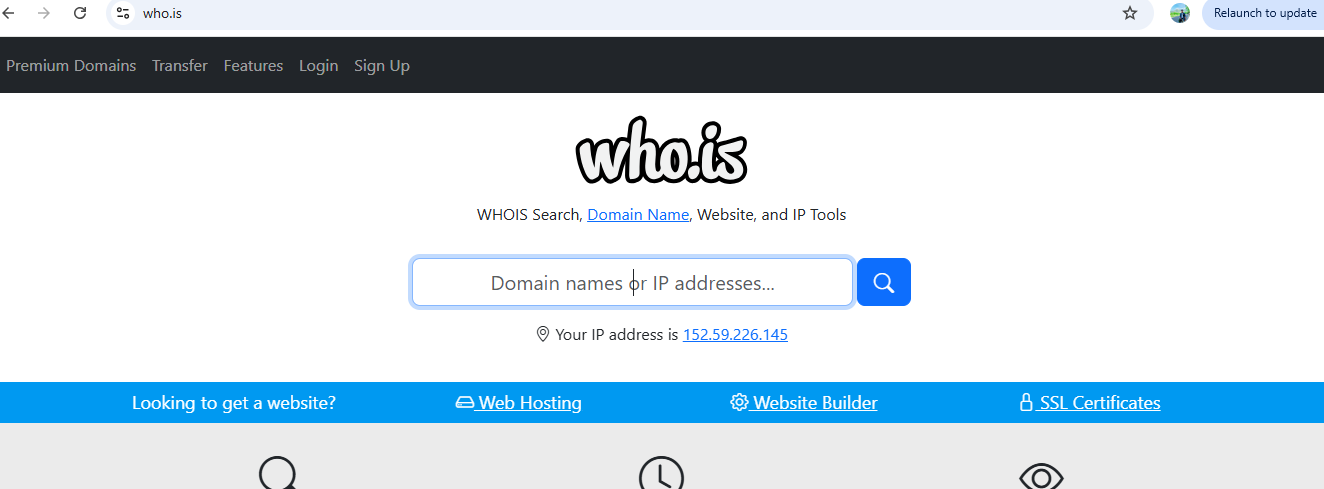
"transport":"udp

**Resp** (find using tran ID 64322 after removing query from the search) index="botsv1" sourcetype="stream:dns" [www.microsoft.com](http://www.microsoft.com)

endtime":"2016-08-24T17:38:45.026479Z","timestamp":"2016-08-24T17:38:45.026467Z","hostname":["www.microsoft.com-c-2.edgekey.net","www.microsoft.com-c-2.edgekey.net.globalredir.akadns.net","e2847.dspb.akamaiedge.net","www.microsoft.com-c-2.edgekey.net","www.microsoft.com-c-2.edgekey.net.globalredir.akadns.net","e2847.dspb.akamaiedge.net"],"host\_addr":["23.213.192.158","23.213.192.158"],"name":["www.microsoft.com","www.microsoft.com-c-2.edgekey.net","www.microsoft.com-c-2.edgekey.net.globalredir.akadns.net","e2847.dspb.akamaiedge.net","www.microsoft.com","www.microsoft.com-c-2.edgekey.net","www.microsoft.com-c-2.edgekey.net.globalredir.akadns.net","e2847.dspb.akamaiedge.net"],

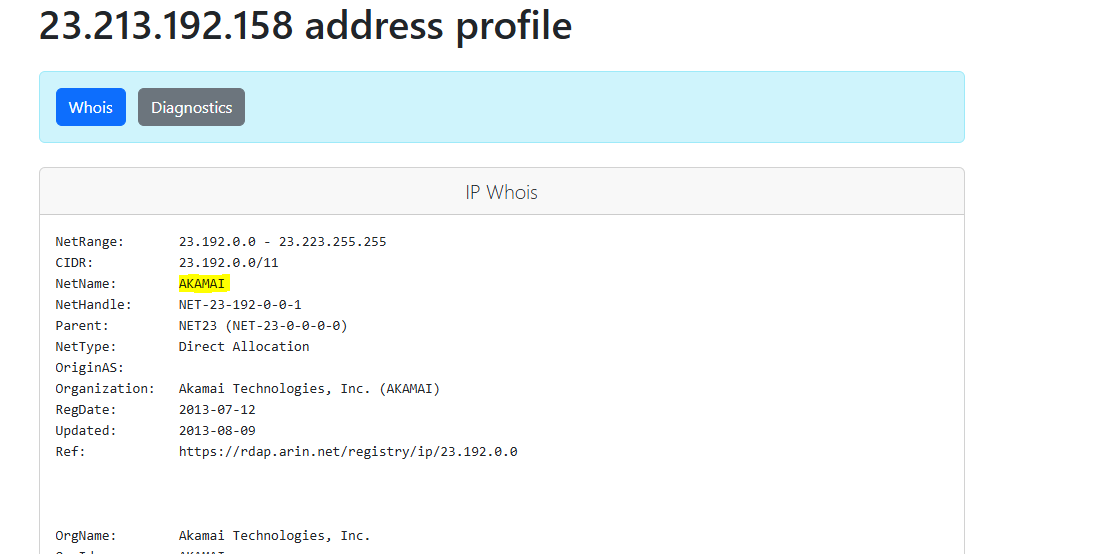
**"reply\_code":["NoError","NoError"],"**response\_time":[21794,21806],"transaction\_id":64322,"ttl":[866,16527,892,12,32768,866,16527,892,12,32768],"bytes":424,"src\_ip":"192.168.250.20","src\_mac":"00:0C:29:C3:C4:00","src\_port":53509,"bytes\_in":0,"dest\_ip":"8.8.8.8","dest\_mac":"08:5B:0E:93:92:AF","dest\_port":53,"bytes\_out":424,"time\_taken":12,"transport":"udp

Go to who.is to know the IP details of the requested domain

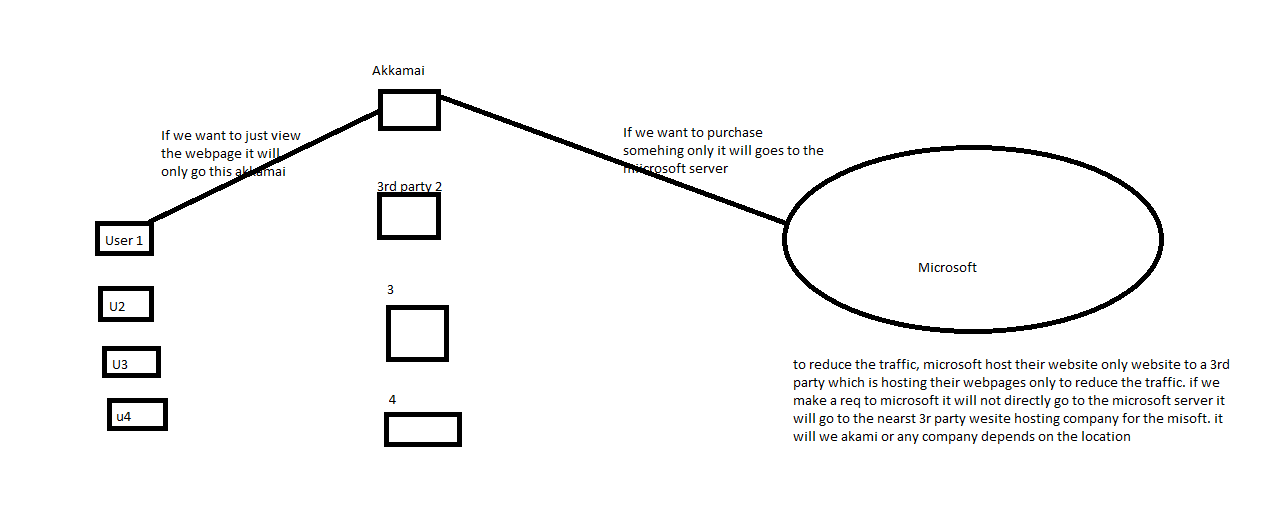


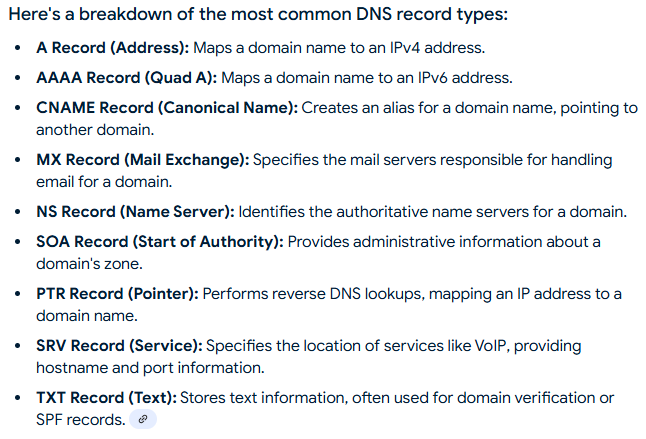
Search the host ip - "],"host\_addr":["23.213.192.158","23.213.192.158"]

From micro soft we are getting



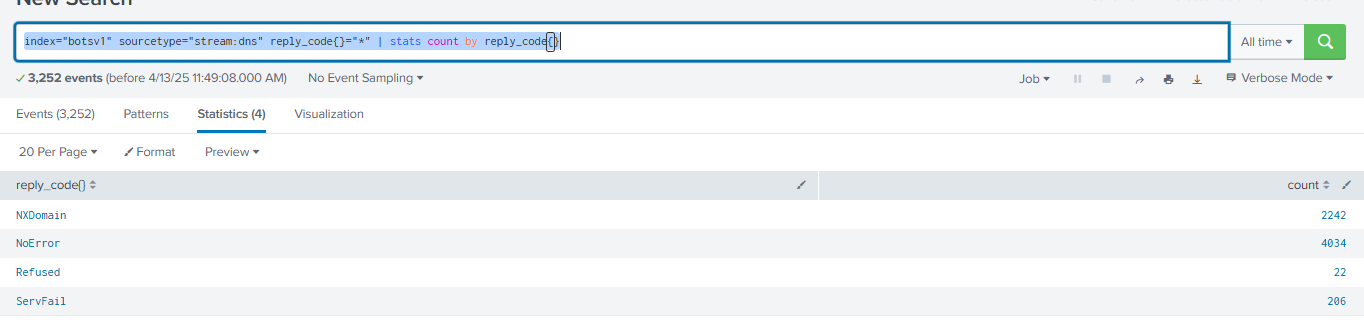
From Microsoft we are getting akkami coz these are cache server.





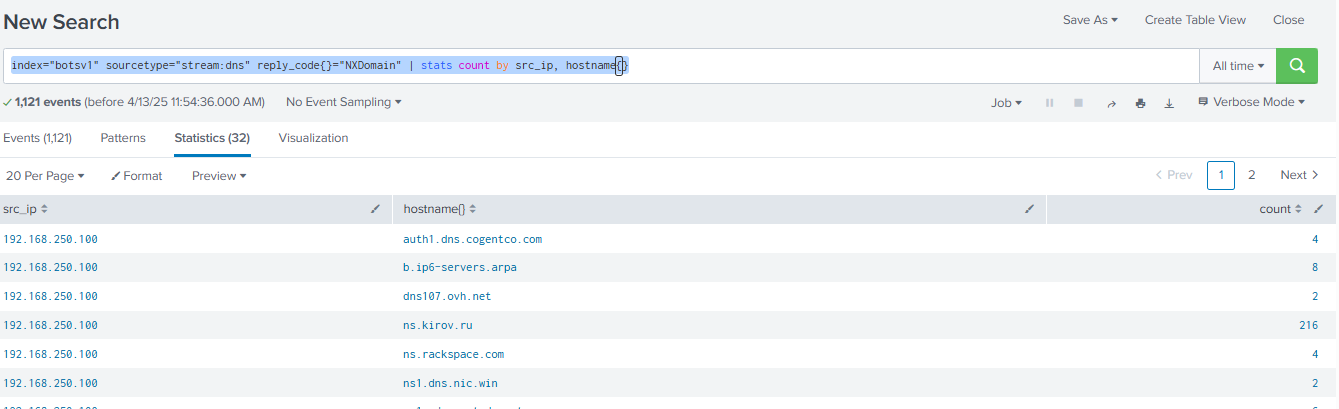
**To check the Reply codes**

**index="botsv1" sourcetype="stream:dns" reply\_code{}="\*" | stats count by reply\_code{}**



**To check the non existing domains req sources and hostname(to know which are the non existing domains req by each src)**

**index="botsv1" sourcetype="stream:dns" reply\_code{}="XDomain" | stats count by src\_ip**

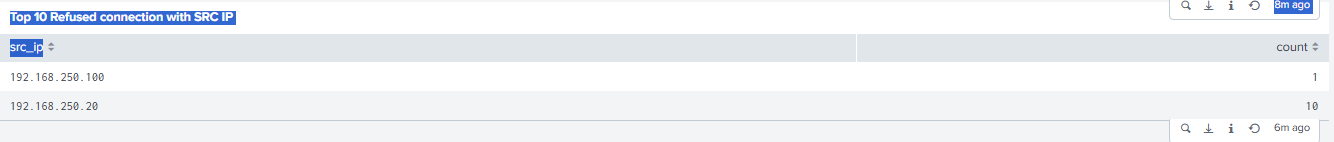


**Dashboard(Top 10 src \_ip with NX domain)**



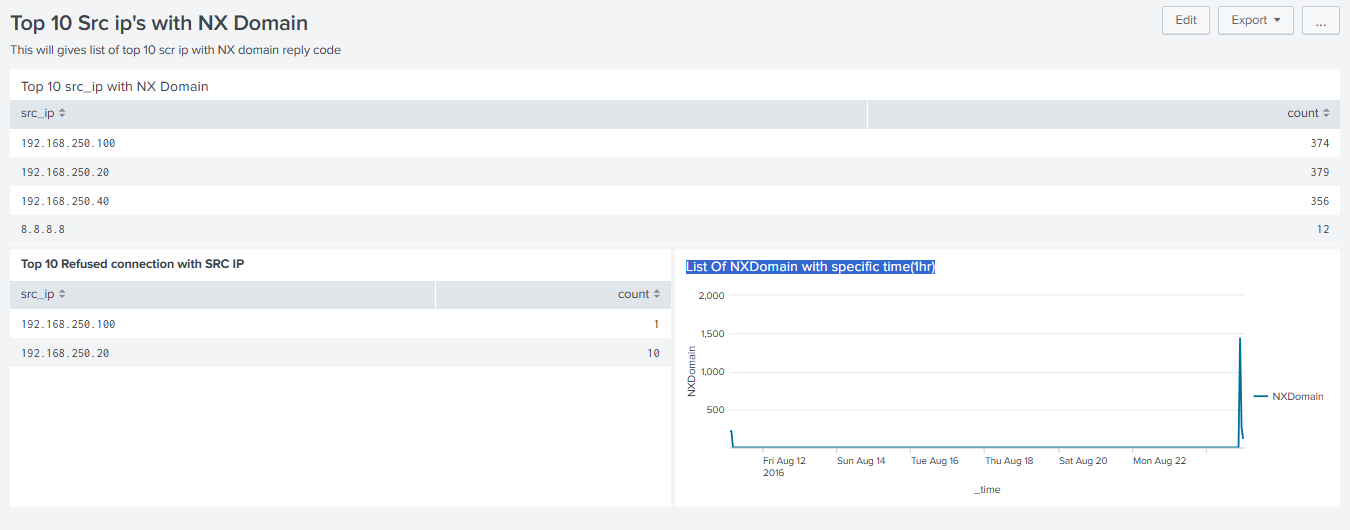
**Refused connection statistics table**

**index="botsv1" sourcetype="stream:dns" reply\_code{}="Refused" | stats count by src\_ip**

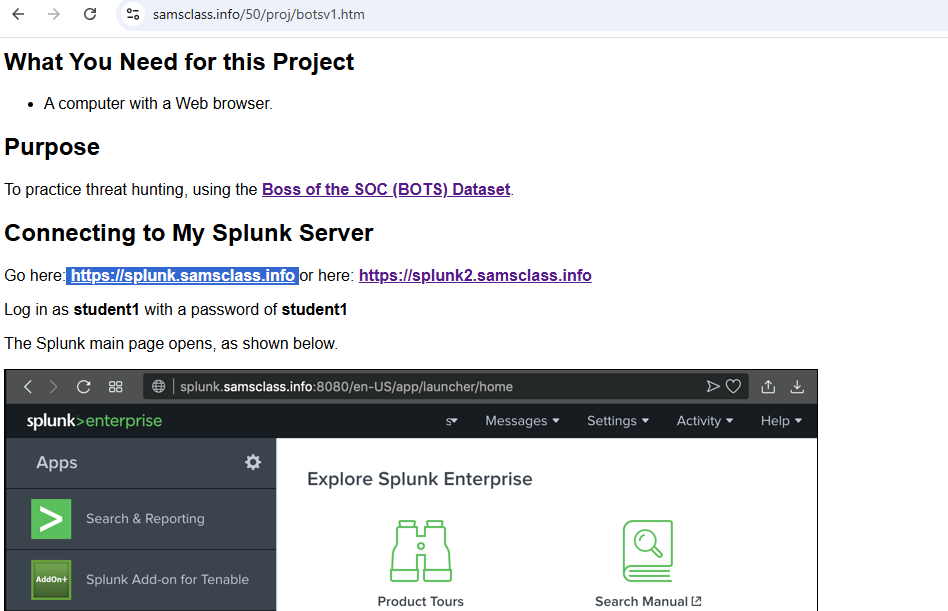


**Top 10 NXDomain in specific time(1h)**

**index="botsv1" sourcetype="stream:dns" reply\_code{}="NXDomain" | timechart span=1h count by reply\_code{}**



**Go to splunk2.samsclass and try all dashboard don’t edit it just cpy paste and come to our splunk**



**Http log**

index="botsv2" source="stream:http" uri\_path !=""

| rename count as counts, uri\_path as URI

| eval error=if(status>=400, counts, 0)

| stats sum(counts) as Count, sum(error) as Errors, sum(time\_taken) as TimeTaken by URI

| sort -Count

| eval Avg\_Response\_Time = (TimeTaken / Count) / 1000

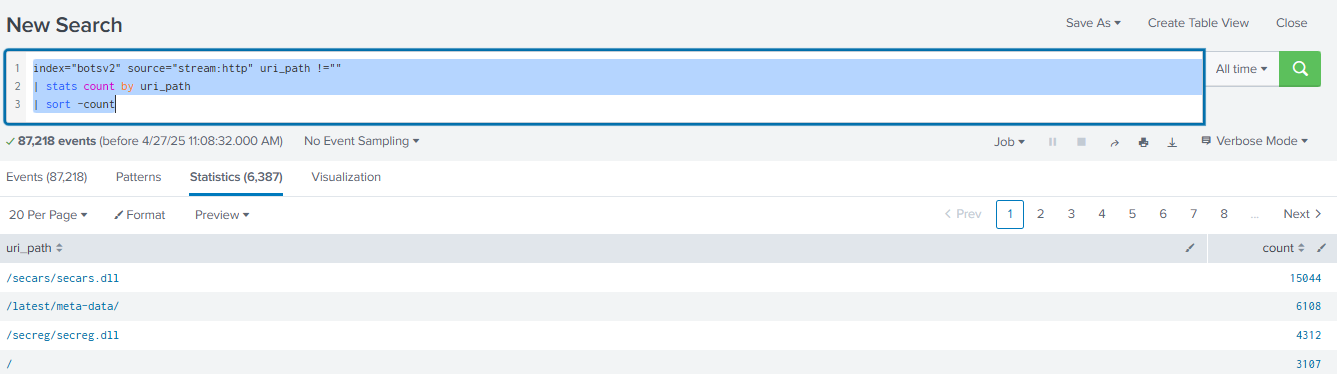
| fields URI, Count, Errors, TimeTaken, Avg\_Response\_Time

**Count of URI path**

index="botsv2" source="stream:http" uri\_path !=""

| stats count by uri\_path

| sort –count



**To get list of ip that used put or delete operation in the organization**

index="botsv2" source="stream:http" AND (http\_method=delete OR htpp\_method=put) AND status=200

| timechart span=600s count by dest\_ip

**To know and any suspicious req(put or delete)**

index="botsv2" source="stream:http" AND (http\_method=delete OR htpp\_method=put)

**To Check error status of req**

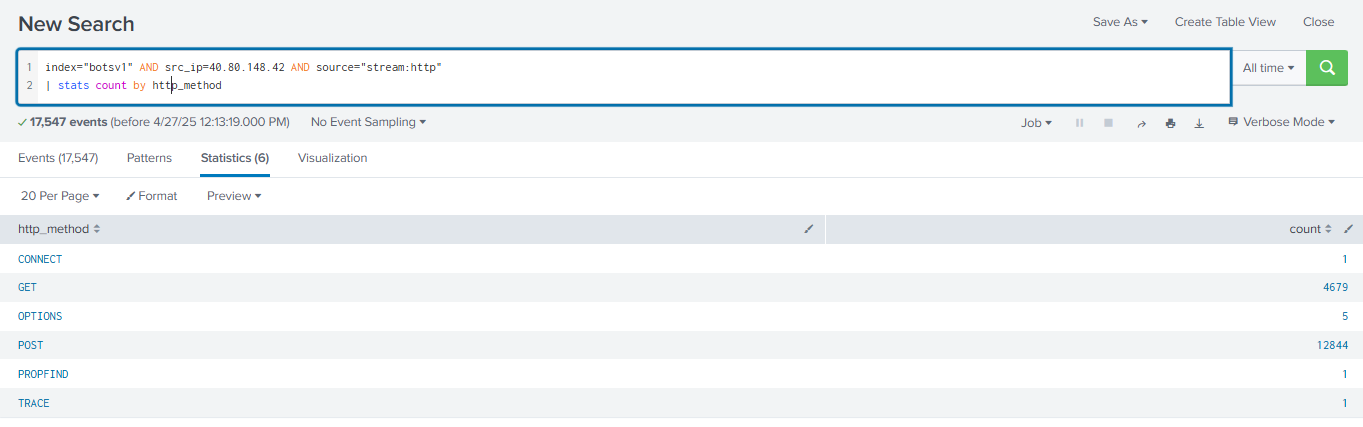
index="botsv2" source="stream:http" status>400

| timechart count by status

**To check a specific src\_ip methods request for the server.**

index="botsv2" AND src\_ip=40.80.148.42 AND source="stream:http"

| stats count by http\_method



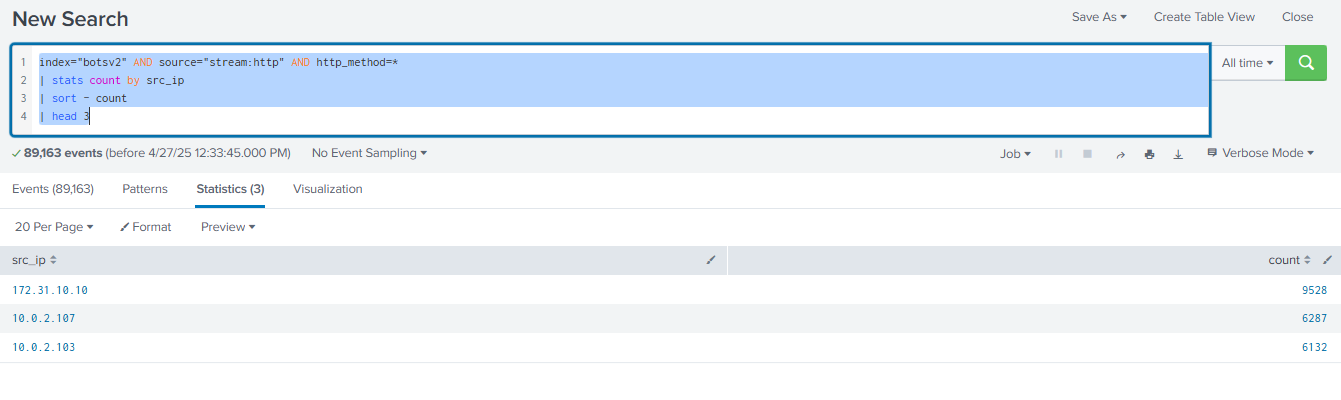
**Imp- Top 3 web traffic req by Src ip(we can use top or head)**

index="botsv2" AND source="stream:http" AND http\_method=\*

| stats count by src\_ip

| sort - count

| head 3



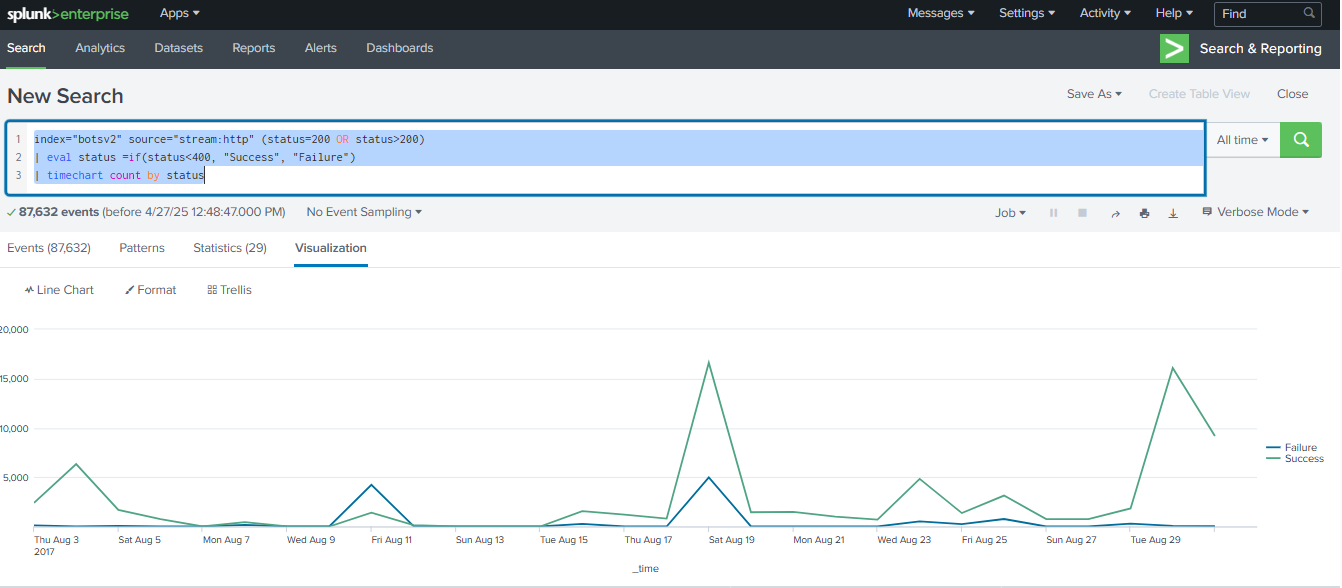
**Need to look (Top methods, Top error codes, Top 10 Users(Hash), Top 10 failed logins, Failed VS Success, top 10 user agent)**

**Success And Failure**

index="botsv2" source="stream:http" (status=200 OR status>200)

| eval status =if(status<400, "Success", "Failure")

| timechart count by status



**Antivirus Log source-** **symantec**

**If field is not visible**

### Step 3: Handle JSON with spath (if needed)

If the data looks like JSON but fields aren't extracted, try:

spl

CopyEdit

index=botsv2 sourcetype="symantec:ep:agent:file"

| spath

| table Host\_name, Event\_Description

Then retry your original query **after spath**:

spl

CopyEdit

index=botsv2 sourcetype="symantec:ep:agent:file"

| spath

| stats count(Event\_Description) by Host\_name

Thanks for checking — if **Step 3 (using spath) returned no values**, that confirms your data is **not in JSON format**, or at least **not parseable as JSON by Splunk**. That explains why fields like Host\_name and Event\_Description aren’t visible — **Splunk doesn’t know how to extract them** automatically.

Run below

**index=botsv2 sourcetype="symantec:ep:agent:file"**

**| head 1**

output 2017-08-29 04:10:28,Site: My Site,Server: uranus,Domain: Default,The management server received the client log successfully,wrk-ghoppy,grace.hoppy,FROTHLY.LOCAL date\_hour = 11date\_mday = 29date\_minute = 10date\_month = augustdate\_second = 28date\_wday = tuesdaydate\_year = 2017date\_zone = localhost = uranusindex = botsv2linecount = 1punct = --\_::,:\_\_,:\_,:\_,\_\_\_\_\_\_\_,-,.,.source = C:\\Program Files (x86)\\Symantec\\Symantec Endpoint Protection Manager\\data\\dump\\scm\_agent\_act.tmpsourcetype = symantec:ep:agent:filesplunk\_server = DESKTOP-C320R6Rtimeendpos = 19timestartpos = 0

###### ChatGPT said:

Thanks for sharing the \_raw output — this is very helpful.

Based on what you posted, the log is **plain text**, **not JSON**, and the fields you want (like Host\_name or Event\_Description) are **not automatically extracted** because:

* The log format is comma-separated (CSV-like) but lacks field names.
* The important values like wrk-ghoppy, grace.hoppy, and FROTHLY.LOCAL are just part of the message, not parsed into fields.

## 🔧 Step-by-Step: Create a Field Extraction

### 1️⃣ Go to Splunk Web UI

* Open your browser and log into **Splunk Web**

### 2️⃣ Go to Field Extractions Settings

* In the top menu bar, click:  
  **Settings → Fields → Field Extractions**

### 3️⃣ Click on "New Field Extraction"

* Look for the **"New Field Extraction"** button (usually top right) and click it.

### 4️⃣ Fill Out the Form:

| **Field** | **What to Enter** |
| --- | --- |
| **Destination App** | search (or whatever app you’re working in) |
| **Name** | extract\_symantec\_agent\_fields (or any name you like) |
| **Apply to** | Choose sourcetype and type symantec:ep:agent:file |
| **Type** | Select Inline |
| **Extraction/Transform** | Paste this regex below 👇 |

regex

CopyEdit

Site:\s(?<site>[^,]+),Server:\s(?<server>[^,]+),Domain:\s(?<domain>[^,]+),(?<event\_message>[^,]+),(?<host\_name>[^,]+),(?<user\_name>[^,]+),(?<user\_domain>[^\s]+)

### 5️⃣ Save

Click **Save** to create the extraction.

## ✅ Test It Works

Now go back to your Search app and run:

spl

CopyEdit

index=botsv2 sourcetype="symantec:ep:agent:file"

| table site, server, domain, event\_message, host\_name, user\_name, user\_domain

| head 5

If everything is correct, the table will show those fields auto-populated for each log line.

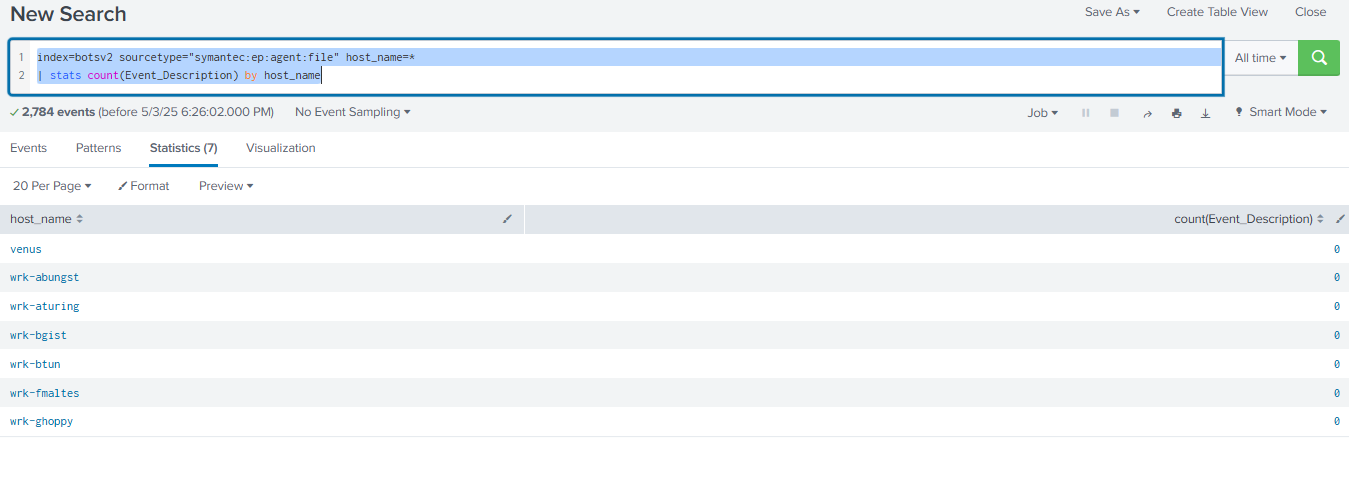
### 💡 Tip:

Once the field is saved, it becomes **visible in the "Interesting Fields"** section (left panel), and you can **use it in stats, filters, dashboards**, etc.

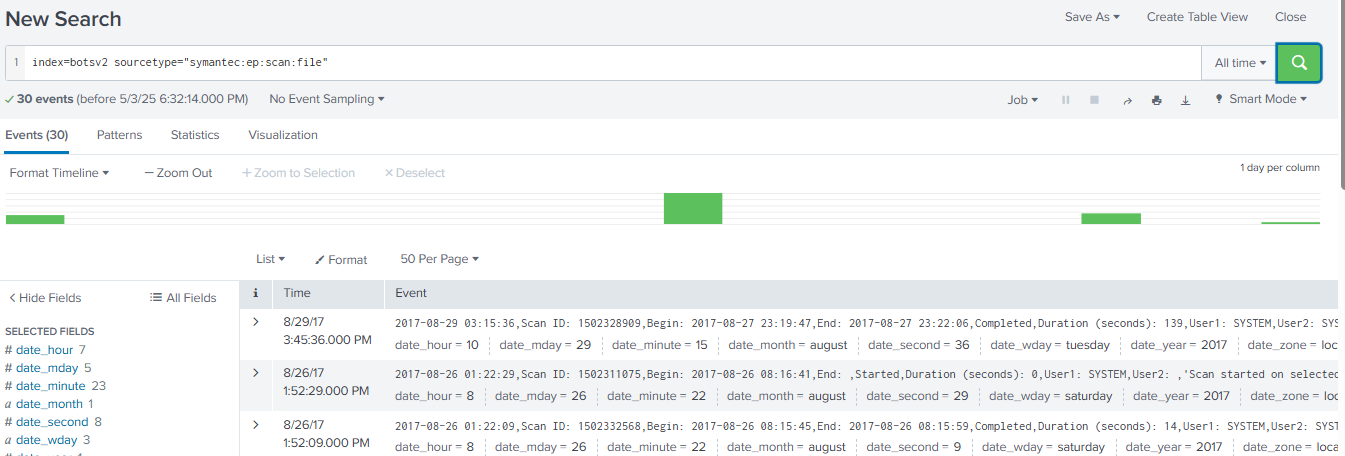
To know how many times each system has received events so we use host to sort

index=botsv2 sourcetype="symantec:ep:agent:file" host\_name=\*

| stats count(Event\_Description) by host\_name



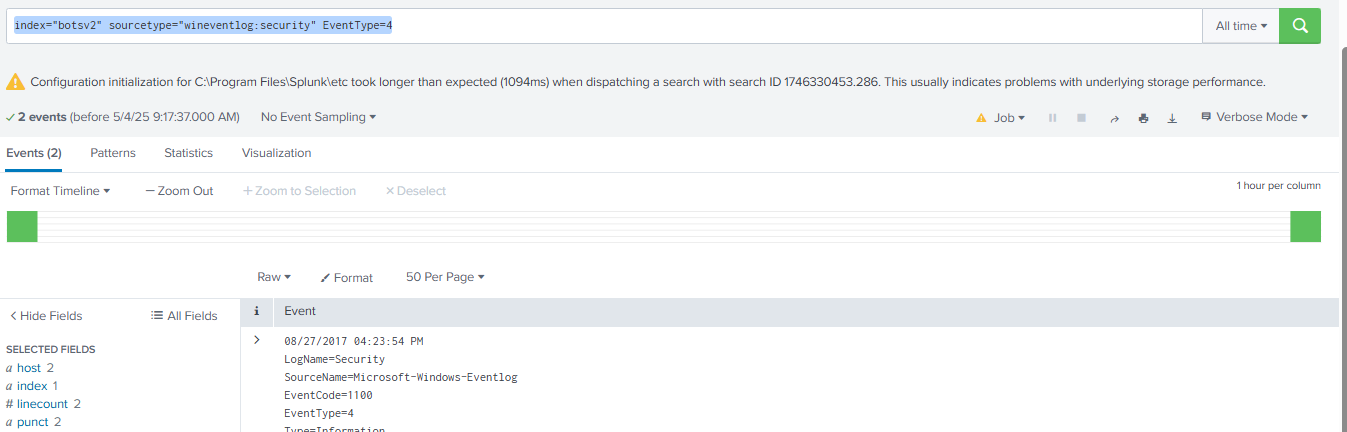
**Security based Events(Scanning)**



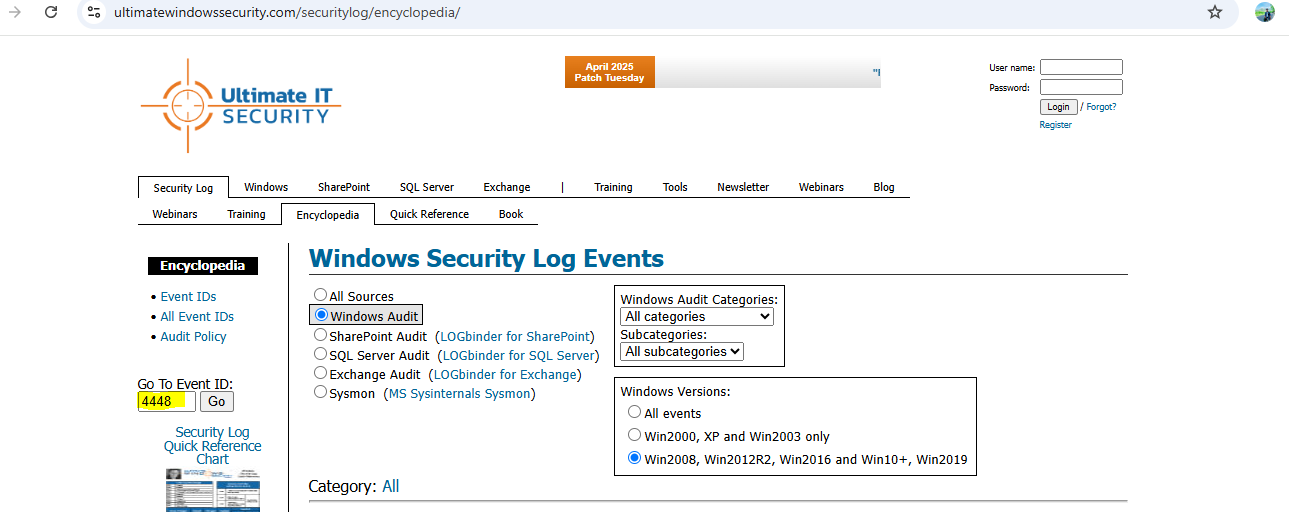
**Windows Log**

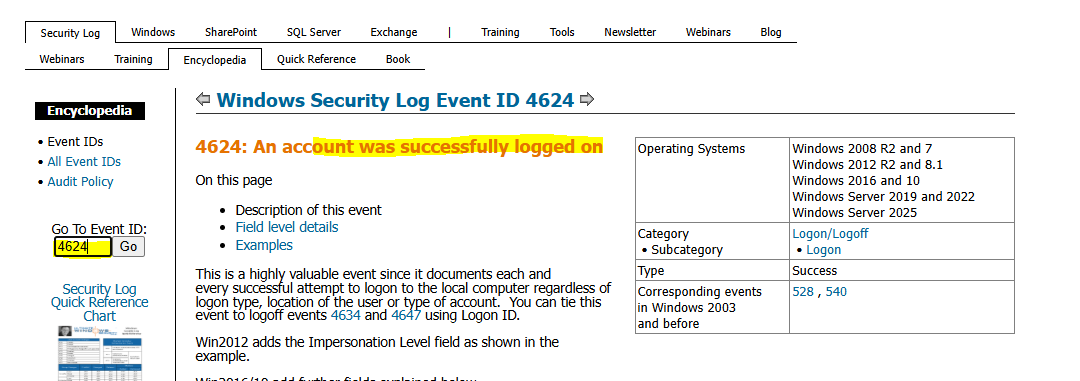
**If someone deleted all the logs(Level-4)**

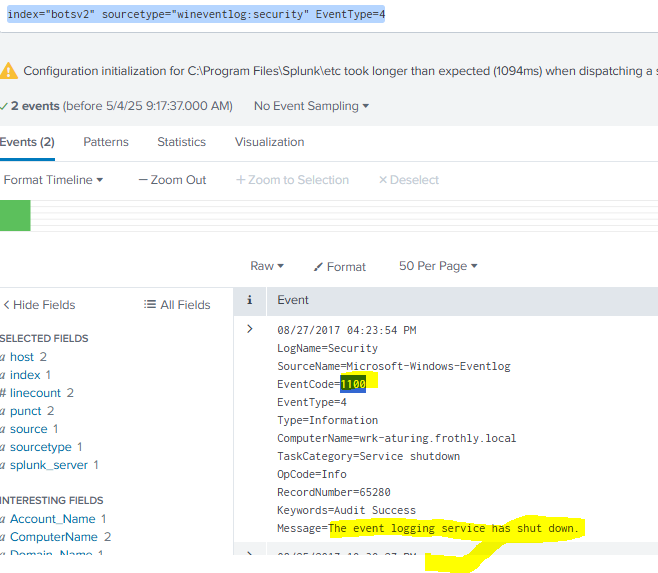
index="botsv2" sourcetype="wineventlog:security" EventType=4

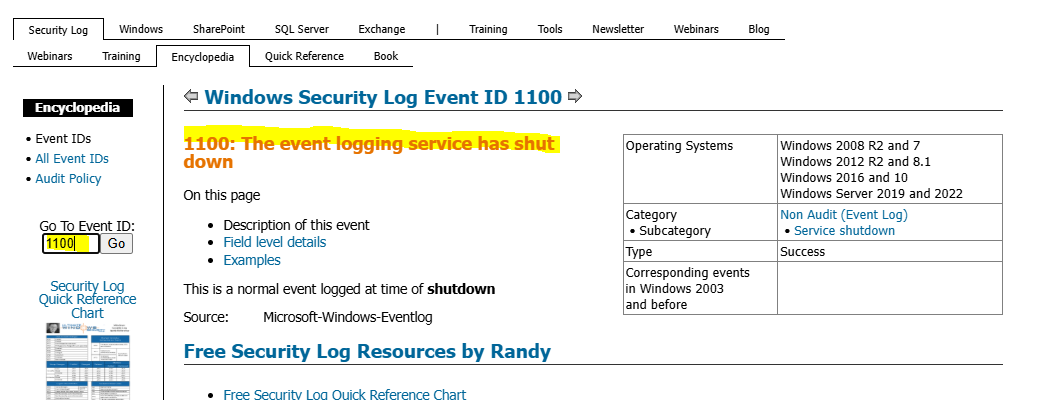


**We can use event ID to know which event occurred**









**EventCode=4688**

**EventType=0**

**Type=Information**

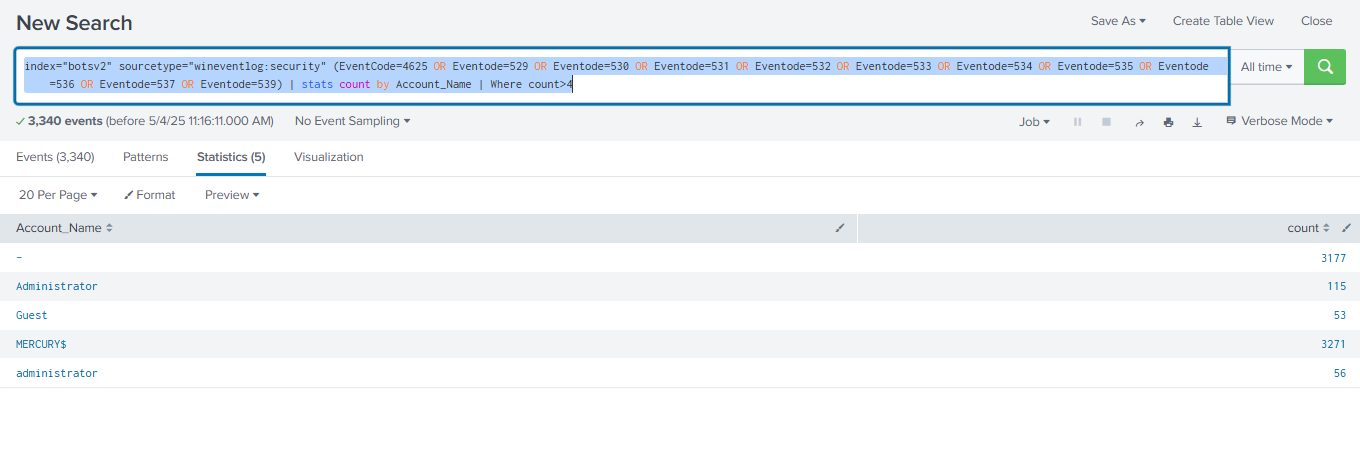
**ComputerName**=wrk-klagerf.frothly.local – device name

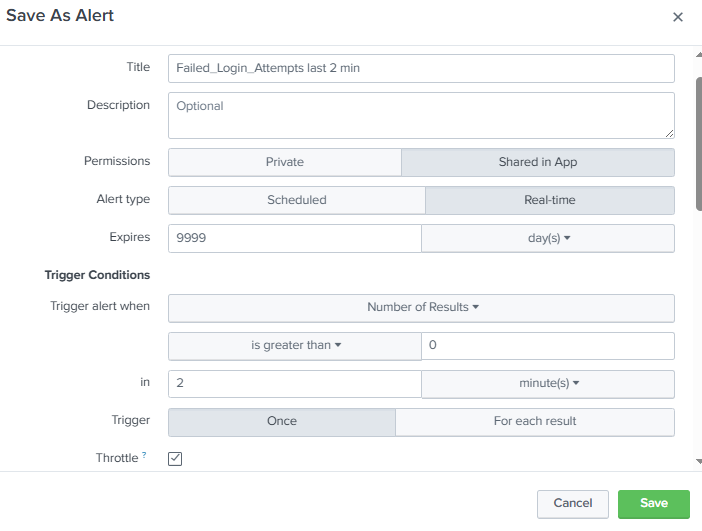
**Account Name: WRK-KLAGERF$ - User name**

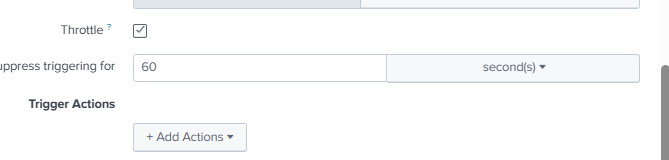
**Account Domain:** FROTHLY – Which domain, like in company which dep

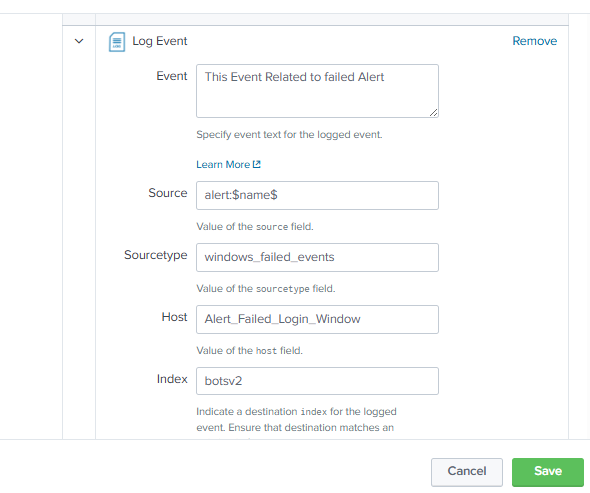
**Which Acc Have more than 4 login acc (Create alert)**

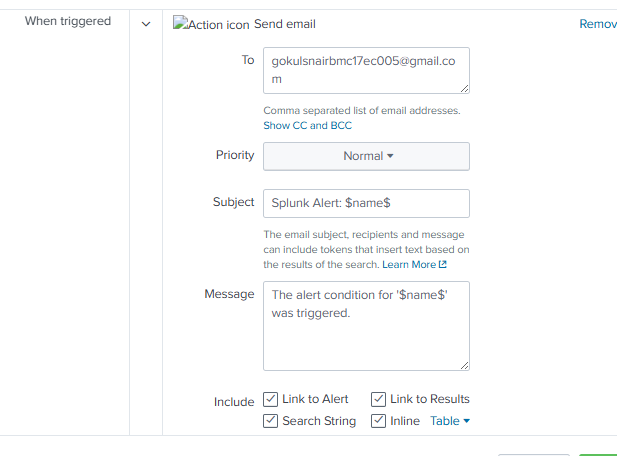
index="botsv2" sourcetype="wineventlog:security" (EventCode=4625 OR Eventode=529 OR Eventode=530 OR Eventode=531 OR Eventode=532 OR Eventode=533 OR Eventode=534 OR Eventode=535 OR Eventode=536 OR Eventode=537 OR Eventode=539) | stats count by Account\_Name | Where count>4

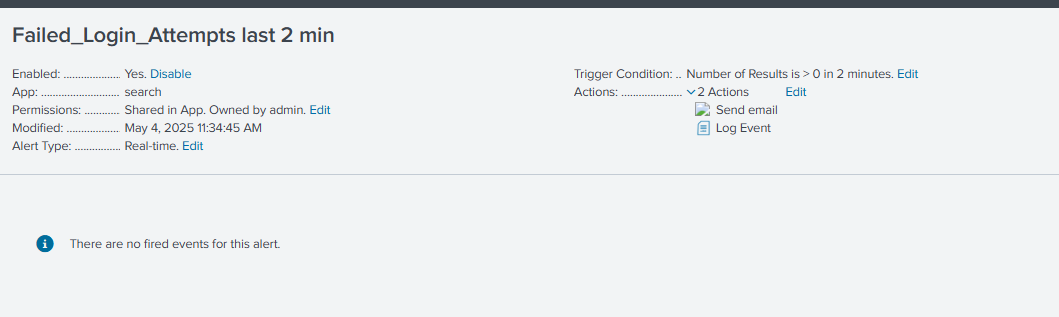






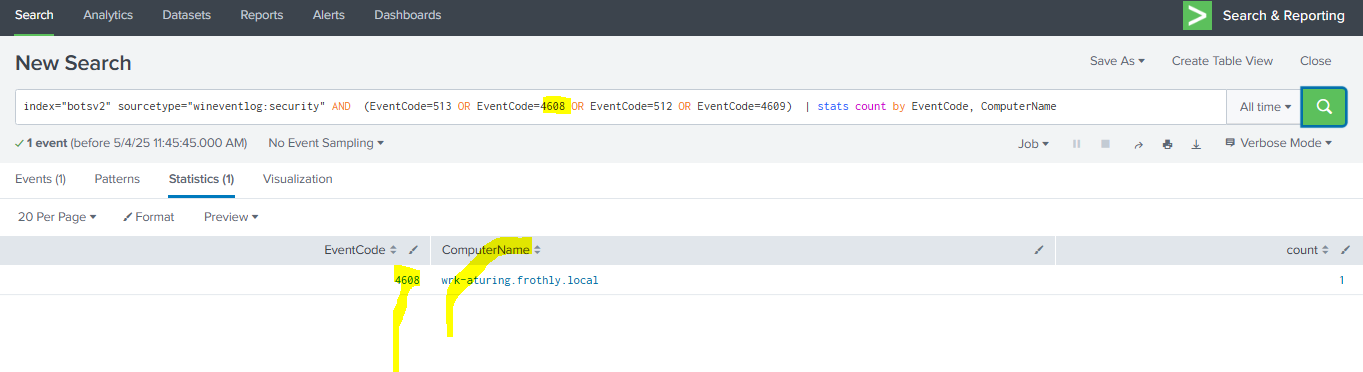






**Which Computer is trying to restarting**

index="botsv2" sourcetype="wineventlog:security" AND (EventCode=513 OR EventCode=4608 OR EventCode=512 OR EventCode=4609) | stats count by EventCode, ComputerName



**Symon Log(System Monitoring logs)**

Event ID 1: Process creation

Event ID 2: A process changed a file creation time

Event ID 3: Network connection

Event ID 4: Sysmon service state changed

Event ID 5: Process terminated

Event ID 6: Driver loaded

Event ID 7: Image loaded

Event ID 8: CreateRemoteThread

Event ID 9: RawAccessRead

Event ID 10: ProcessAccess

Event ID 11: FileCreate

**Sysmon log configuration**

**Step-1**

 Go to the official Microsoft Sysinternals site: <https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon>

 Click **Download Sysmon** — this downloads a ZIP file (e.g., Sysmon.zip).

 **Extract the ZIP**

**Create a folder in “C:\Tools\Sysmon” and extract the file i**

C:\Tools\Sysmon

**Step-2**

* Download a prebuilt config (recommended):
  + Visit: <https://github.com/SwiftOnSecurity/sysmon-config>
  + Download sysmonconfig-export.xml and rename it to sysmonconfig.xml

OR

* Create a **basic test config**:

Create a file named sysmonconfig.xml with this minimal content:

xml

CopyEdit

<Sysmon schemaversion="4.50">

<EventFiltering>

<RuleGroup name="default" groupRelation="or">

<ProcessCreate onmatch="include" />

</RuleGroup>

</EventFiltering>

</Sysmon>

Save it to the same folder where Sysmon64.exe is located

**Step-3**

 **Open Command Prompt as Administrator:**

* Press Start
* Type cmd
* Right-click → **Run as administrator**

 **Navigate to Sysmon folder:**

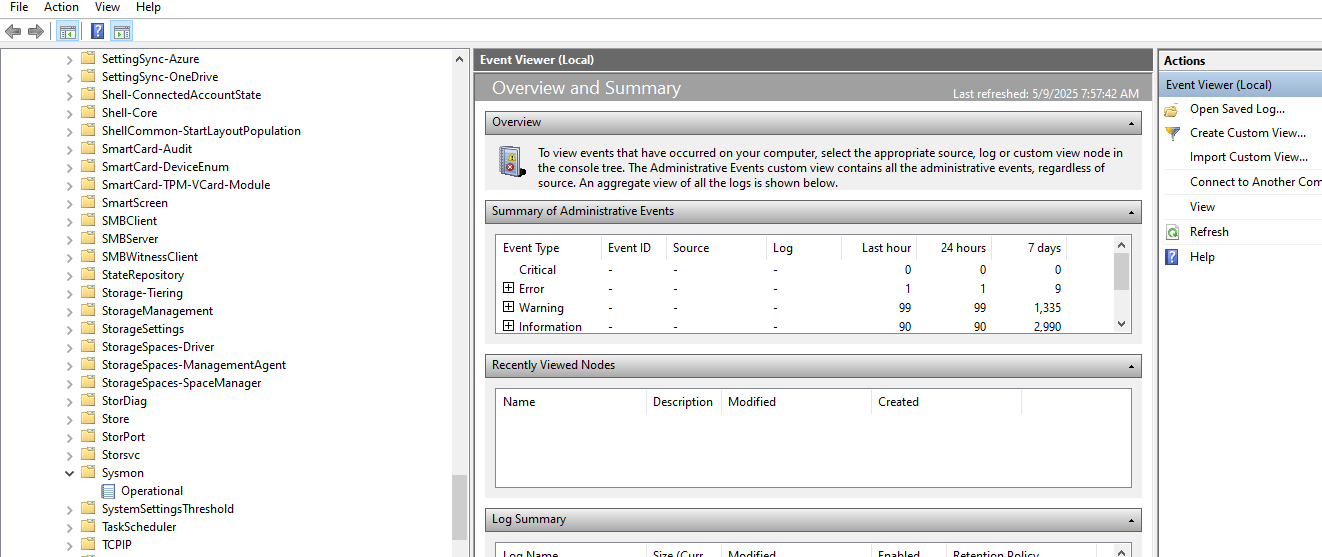
cmd

cd C:\Tools\Sysmon

 **Run the installation command:**

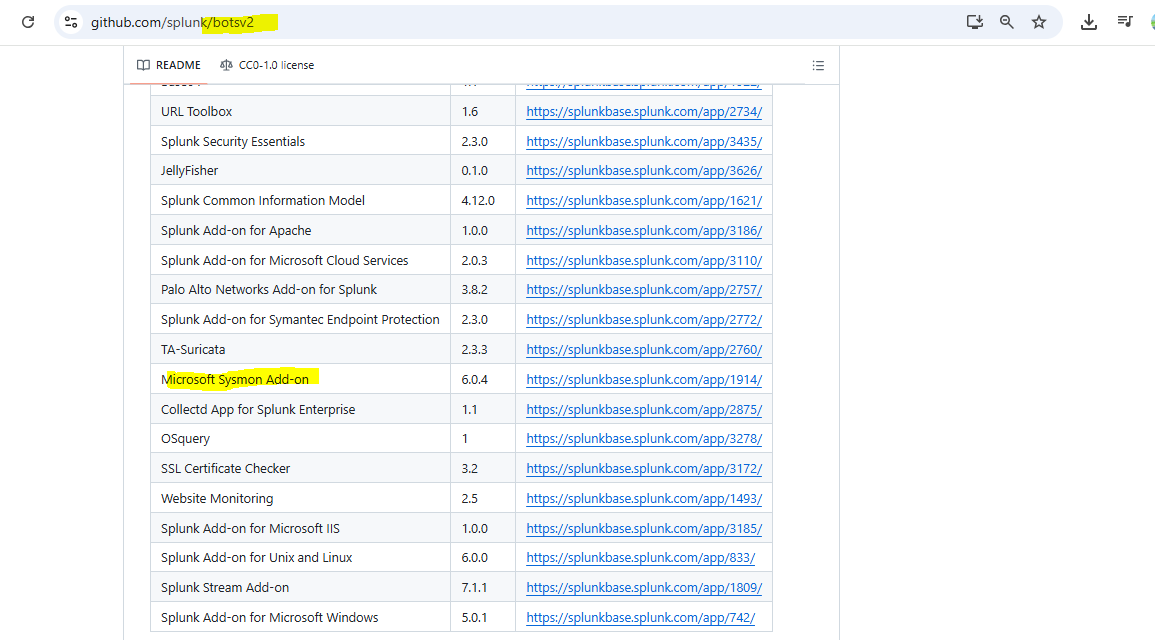
cmd

Sysmon64.exe -accepteula -i sysmonconfig.xml

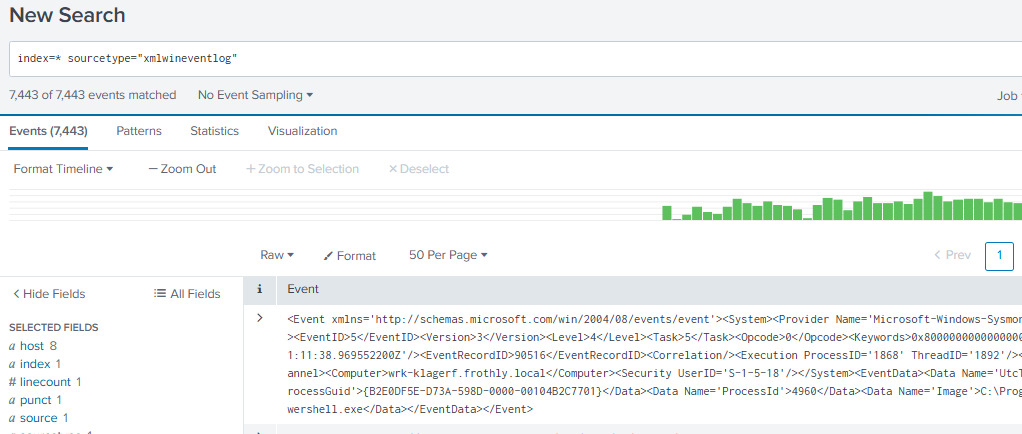


Event Viewer-🡪Application and serviceslog🡪Microsoft🡪 Sysmon

Go to splunk and configure Microsoft sysmon add-on



**System Mon log analysis**



**To know which are computers which the process initiated**

index=\* sourcetype="xmlwineventlog" EventID=1 | stats by ComputerName

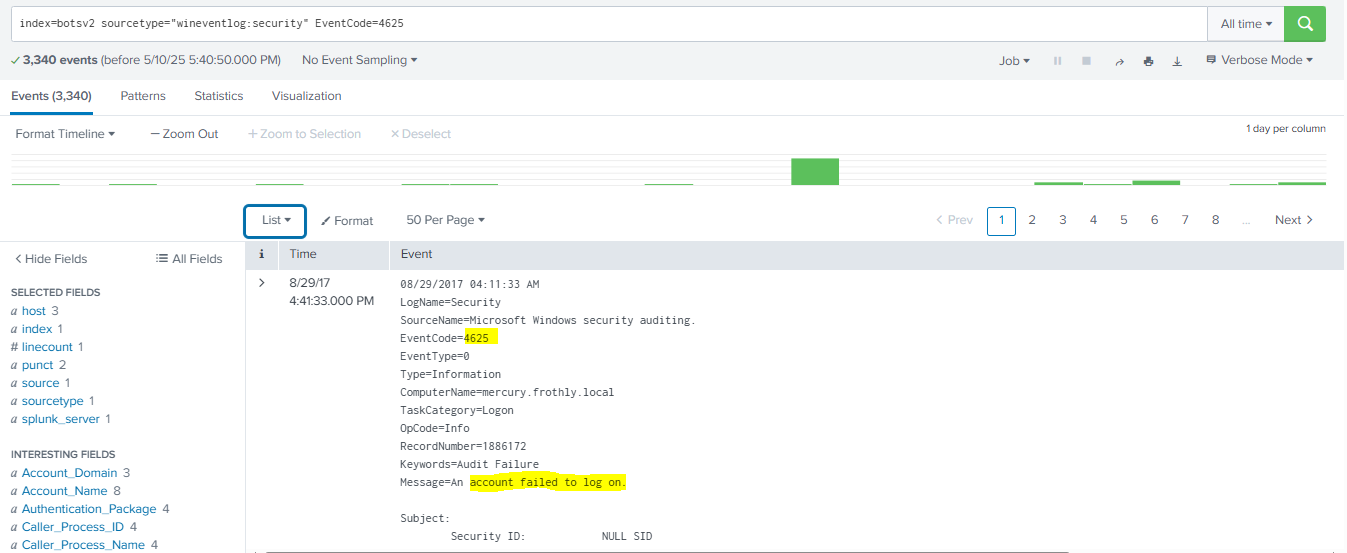
**-------------------------------------------------------------------------------------------------------------------------------------Use Cases**

**Data stream Analysis**

Windows security event ID-4624

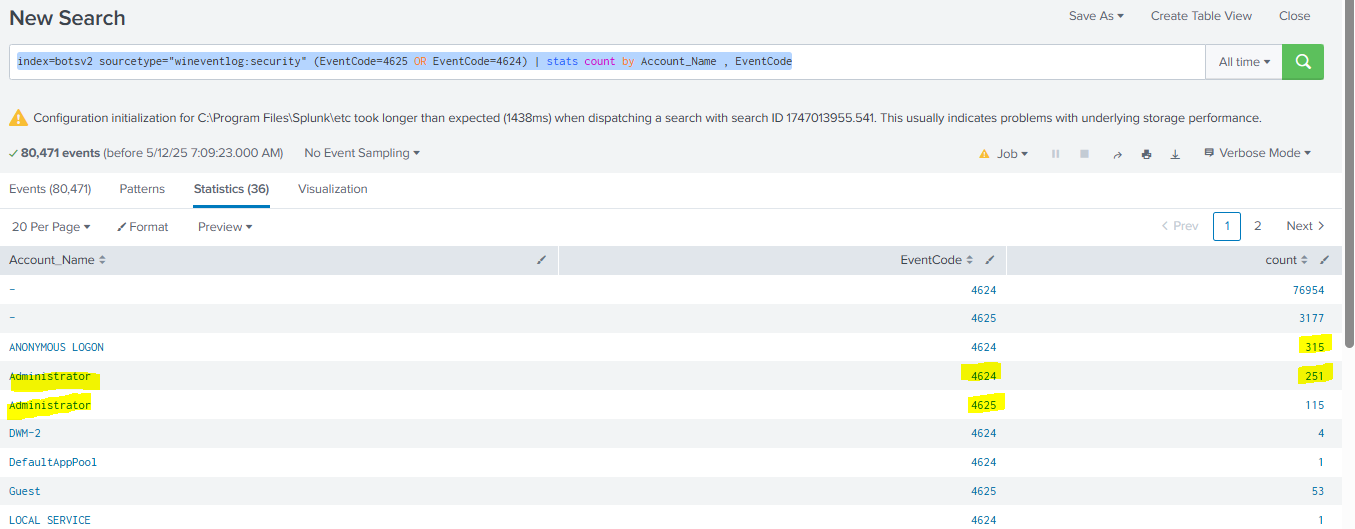
Windows security event ID-4625

Windows security event ID-4626



**To know how many success and failure from systems**

index=botsv2 sourcetype="wineventlog:security" (EventCode=4625 OR EventCode=4624) | stats count by Account\_Name , EventCode



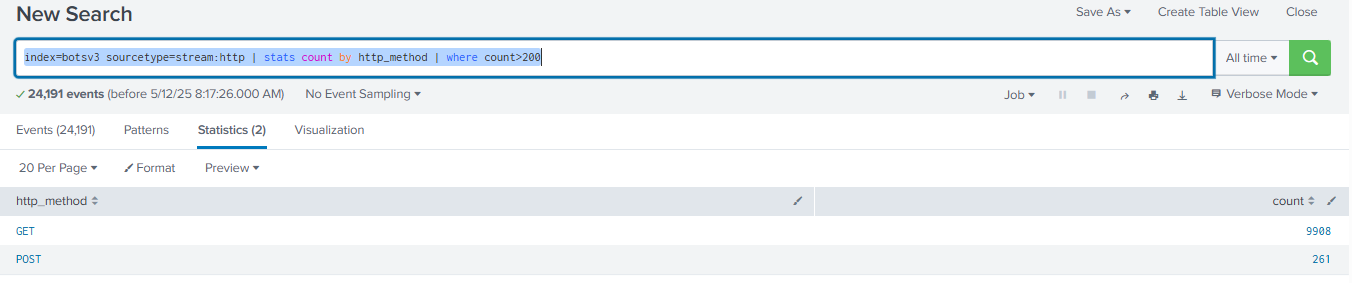
This might be an attacker coz success and failed logins are almost same

**Traffic from a printer to Work station**

index=botsv3 sourcetype=cisco:asa action=allowed OR action=success src\_ip='server\_printerip.csv' | stats count by src\_ip,dest\_ip

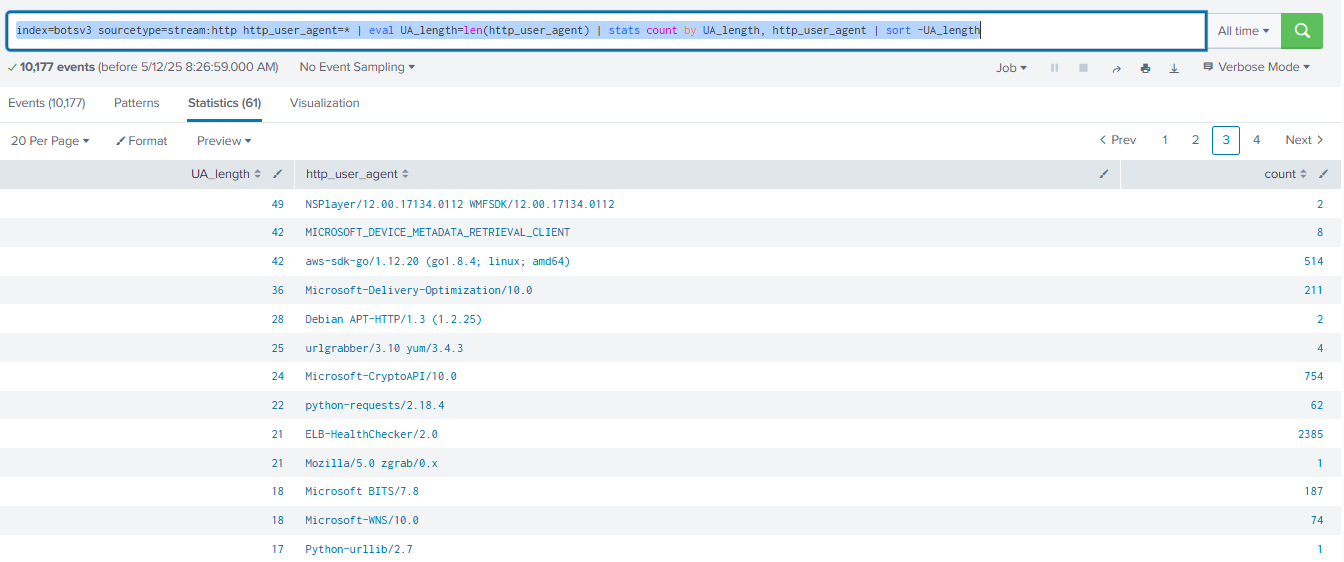
**Webservice methods count**

index=botsv3 sourcetype=stream:http | stats count by http\_method | where count>200



**Check the user agents and see if any of the length value is less than min and suspicious(user agents with min character leng is suspicious)**

index=botsv3 sourcetype=stream:http http\_user\_agent=\* | eval UA\_length=len(http\_user\_agent) | stats count by UA\_length, http\_user\_agent | sort -UA\_length



UA\_length is very lss UA\_length is alias value of http\_user\_agent and it will count the length or characters in http\_user\_agent