Blue Team Level 1 Certification (Standard)

Introduction to BTL1
- ~~Welcome to Blue Team Level 1!~~ 4 Topics
- ~~Lab and Forum Access~~

SECURITY FUNDAMENTALS DOMAIN
- ~~Introduction to Security Fundamentals~~ 1 Topic
- ~~Soft Skills~~ 7 Topics
- ~~Security Controls~~ 5 Topics | 1 Quiz
- ~~Networking 101~~ 6 Topics | 1 Quiz
- ~~Management Principles~~ 4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN
- ~~PA1) Introduction to Emails and Phishing~~ 7 Topics | 1 Quiz
- ~~PA2) Types of Phishing Emails~~ 10 Topics | 2 Quizzes
- ~~PA3) Tactics and Techniques Used~~ 12 Topics | 2 Quizzes
- ~~PA4) Investigating a Phishing Email~~ 8 Topics | 2 Quizzes
- ~~PA5) Analysing URLs, Attachments, and Artifacts~~ 8 Topics | 1 Quiz
- PA6) Taking Defensive Actions 12 Topics | 1 Quiz
- PA7) Report Writing 7 Topics | 1 Quiz
- PA8) Phishing Response Challenge 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN
- TI1) Introduction to Threat Intelligence 7 Topics
- TI2) Threat Actors & APTs 6 Topics | 2 Quizzes
- TI3) Operational Threat Intelligence 7 Topics | 1 Quiz
- TI4) Tactical Threat Intelligence 7 Topics | 1 Quiz
- TI5) Strategic Threat Intelligence 5 Topics | 1 Quiz
- TI6) Malware and Global Campaigns 6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN
- DF1) Introduction to Digital Forensics 5 Topics
- DF2) Forensics Fundamentals 10 Topics | 5 Quizzes

Splunk Crash Course – Search Queries

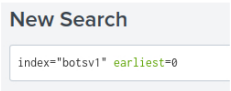
The BOTSv1 dataset we imported in the previous lesson has been imported to Splunk as an Index, which is essentially a collection of data. We can search through the data by navigating to the Search and Reporting App from the Splunk homepage, and entering the search query: `index="botsv1" earliest=0`. We can see there are hundreds of thousands of events found via this search query. Looking through the data like this is going to take forever, and that's where search queries come in.

We can combine text strings, file names, process names, IP addresses, operators and lots more to look for specific data in our index. We believe the best way to teach you about search queries is to just jump in and go through some examples together. We're going to cover:

- **Searching With Fields** (Selected Fields, Interesting Fields)
- **Field / Value Pairs** (AND, OR, NOT operators)
- **Wildcards**
- **Processes** (Sysmon Image field)

SEARCHING WITH FIELDS

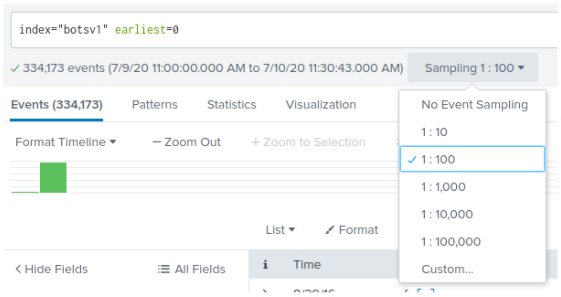
To show you what Fields are in Splunk, go to the Search and Reporting App, and enter in the following search query in the top bar:



What does this search query actually mean?

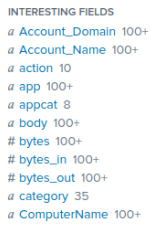
- **index="botsv1"** — We want to search against the botsv1 dataset that we imported in a previous lesson
- **earliest=0** — If we didn't use this argument, which tells Splunk to start looking at the first event in the dataset, we would need to change the date range (on the far left) to All Time, this way is just easier

Now this dataset still contains hundreds of thousands of events, and Splunk will take a little while to search through all of them to find any that meet our search criteria, in this case, all of them. To make things easier now, we are going to change the Sampling value (under the search bar on the left) from No Event Sampling (all events) to 1:100.

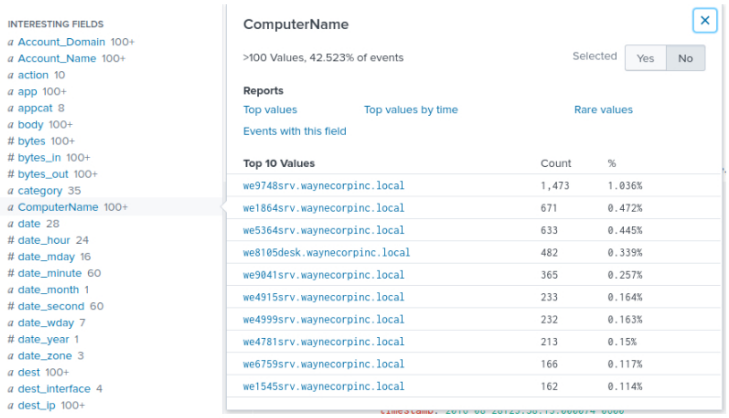


DF3) Digital Evidence Collection
8 Topics | 1 Quiz
DF4) Windows Investigations
3 Topics | 3 Quizzes
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk
5 Topics | 2 Quizzes
Section Introduction, Splunk
Splunk Crash Course – Navigating Splunk
Splunk Crash Course – Search Queries
Splunk Crash Course – Creating Alerts
Splunk Crash Course – Creating Dashboards
Lab) Splunk Investigation 1
Lab) Splunk Investigation 2
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 2 Quizzes
IR3) Detection and Analysis Phase
7 Topics | 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes
BTL1 EXAM
Exam Preparation
Using RDP and SSH
How to Start Your Exam

Okay, now we're working with a sample of the full dataset, so let's cover what Fields are. On the left-hand side of Splunk we can see "SELECTED FIELDS" and "INTERESTING FIELDS". This is information that has been extracted from the raw data, and sorted by Splunk. In the below screenshot we have listed some of the interesting fields, let's click on the bottom one, "ComputerName".

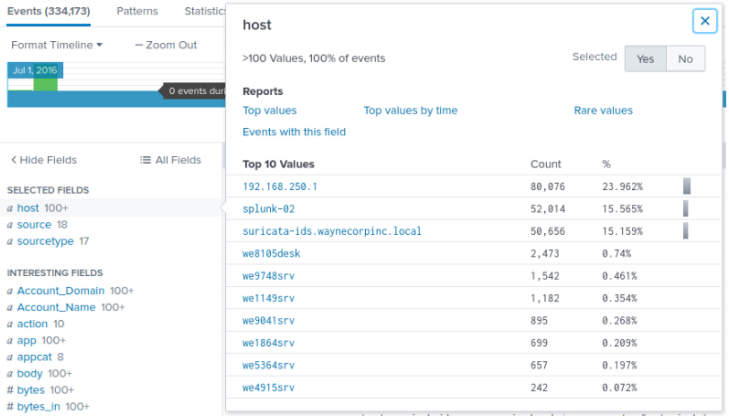


In the below screenshot you can see that Splunk has now pulled the information in this field from all of the raw events in our sample (1:100). We can see lots of different hostnames, and how many events this name is featured in. For example, the top value we9748srv.waynecorpinc.local is featured in 1473 events.



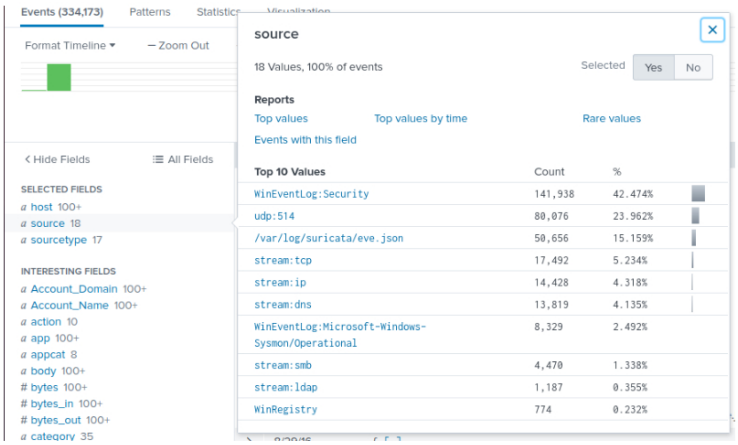
Let's move back up to the "SELECTED FIELDS" section, where we can see the number of hosts in our event sample (100+), the number of event sources (18), and the different sourcetypes of where data has come from (17).

Clicking on the host option will show us the 10 hosts that have had the most traffic. We can see that the "noisiest" host is 192.168.250.1, and the below that is splunk-02, and then suricata IDS.

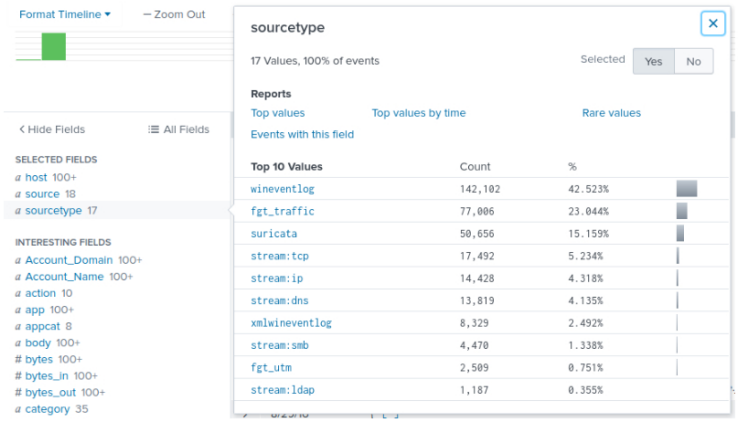


Next let's look at the 'source' option to see where the data we're dealing with is coming from. In the below

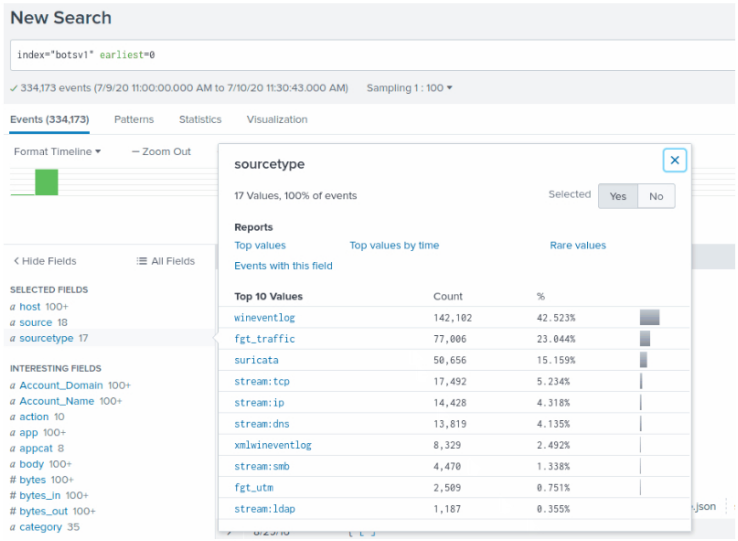
screenshot we can see that the number one source of logs in our event sample is Windows Event Logs, specifically security logs, making up 42%. Next is udp:514, which you should recognise as syslog! Followed by Suricata IDS logs as third in the top 10 list.



Below 'source' we have 'sourcetype' which shows us the type of data we have, which shows expectedly similar results to the 'source' field.



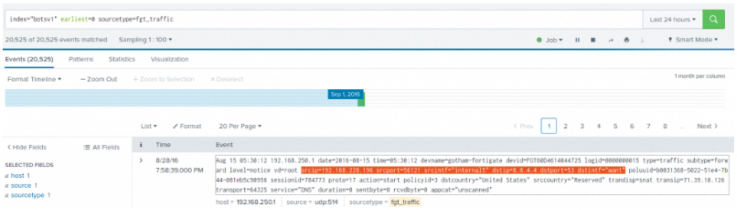
If we wanted to look at one of these log types in particular, such as 'wineventlog', we can simply click on it and Splunk will change our search query, as shown below.



This can be a great way to find specific information quickly, for example if we wanted to look at intrusion detection system logs, we'd filter on Suricata as our sourcetype. Let's say we want to look at network traffic – we select fgt_traffic from the 'sourcetype' field menu, to see logs associated with Fortigate Firewalls (fgt).

Please note, as we are using an event sample, you may get different results than us, and that's fine! It just means you're looking at a different group of events. If you don't see the sourcetype 'fgt_traffic' then try refreshing your search for `index="botsv1" earliest=0` to get a new 1:100 sample.

In the below screenshot you can see our search query has changed to include sourcetype=fgt_traffic at the end, and the first example shows a firewall log. We have highlighted the source ip, source port, source interface, destination ip, destination port, and destination interface values. These are also log fields, so the field 'srcip' holds the value of the source IP address. Remember from the previous SIEM domain lessons, where we mentioned that logs are not universal, and while this firewall log uses 'srcip', another log could use the field name 'source_ip' instead.



You should now understand that fields are property and value pairs from raw logs, and that we can use them to quickly narrow down our searches to look at specific log types, log sources, or quickly gather important information like hostnames and IP addresses.

FIELD / VALUE PAIRS

The simplest search we can conduct is for a field and a value, for example, searching against our data for the source IP field (src) and the IP address value 10.10.10.50.

```
search src="10.10.10.50"
```

With the above query, we're looking for any logs where the source IP is listed as 10.10.10.50. If we wanted to look for any logs or network traffic associated with this IP, we could also search for logs where the destination IP is stated as 10.10.10.50:

```
search src="10.10.10.50" OR dst="10.10.10.50"
```

Let's go through a simple scenario together. The Customer Support team have received a number of complaints that the company website is extremely slow, and some customers aren't able to access the site. The security team believes this may be a distributed denial-of-service attack, where multiple remote systems attempt to crash or use up all of the server's resources so that legitimate clients can't access it. Using the following simple query we could see what traffic is being directed towards the web server:

```
search dst="10.10.100.5"
```

While this would show us any logs where the destination IP is the web server, it will also show any other logs or traffic going to that server, which could result in a lot of logs that we are not interested in. We can apply additional arguments in our search query to perform actions such as filtering on HTTP traffic only.

WILDCARDS

What is a wildcard? A wildcard operator is the asterisk character (*) that can be used to mean **anything**. To explain what we mean, let's go through another example. Security analysts determine that the host 10.10.10.73 has been compromised by a malicious actor, and that the next likely step in their plan is to search for other systems in that network (10.10.10.0/24). Using Splunk, we could see if the infected host has communicated with any of the other hosts using the query:

```
search src="10.10.10.73" dst="10.10.10.*"
```

In the above example, the wildcard **dst="10.10.10.*"** is being used to represent any IP address that begins with "10.10.10.". We could also use this to look for words that may have different versions, such as "pass" and "password". For example, we could search for logs that contain information about login failures with the following:

```
search pass* AND fail*
```

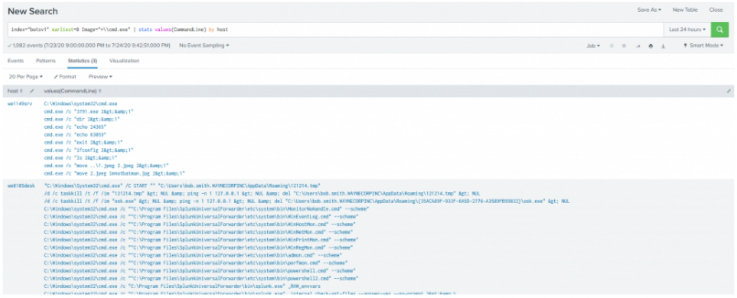
So with this query, it will return any logs that contain the following:

- "pass" "fail"
- "password" "fail"
- "pass" "failure"
- "password" "failure"

SEARCHING FOR PROCESSES

```
index="botsv1" earliest=0 Image="*\\cmd.exe" | stats values(CommandLine) by host
```

The above search query is using a new parameter, "Image=". This is derived from Sysmon logs, such as Event ID 1, 'New Process Created'. The Image field in Sysmon events shows the executable that has generated the process, in this example, cmd.exe, which should be located at C:\Windows\System32\cmd.exe (but we can wildcard the path). After the search for cmd.exe, we're retrieving the events using values(CommandLine) to show what commands were used, and finally sorting it per host. Let's see how this search looks once it has been run (with no event sampling):



ADDITIONAL RESOURCES

If you want to learn more about searching in Splunk, we highly recommend you read the documentation on searching here – https://docs.splunk.com/Documentation/Splunk/8.0.4/SearchTutorial/Startsearching

Or watch this great YouTube video created by the team at Splunk – https://www.youtube.com/watch?v=xtyH_6iMxwA

Privacy & Cookies Policy
Privacy - Terms