Splunk Cloud SIEM Lab

You are a security analyst working at the e-commerce store Buttercup Games. You've been tasked with identifying whether there are any possible security issues with the mail server. To do so, you must explore any failed SSH logins for the root account.

SIEM tools like Splunk allow the collection of data and logs from numerous sources so that it may be viewed, analyzed, and alert.

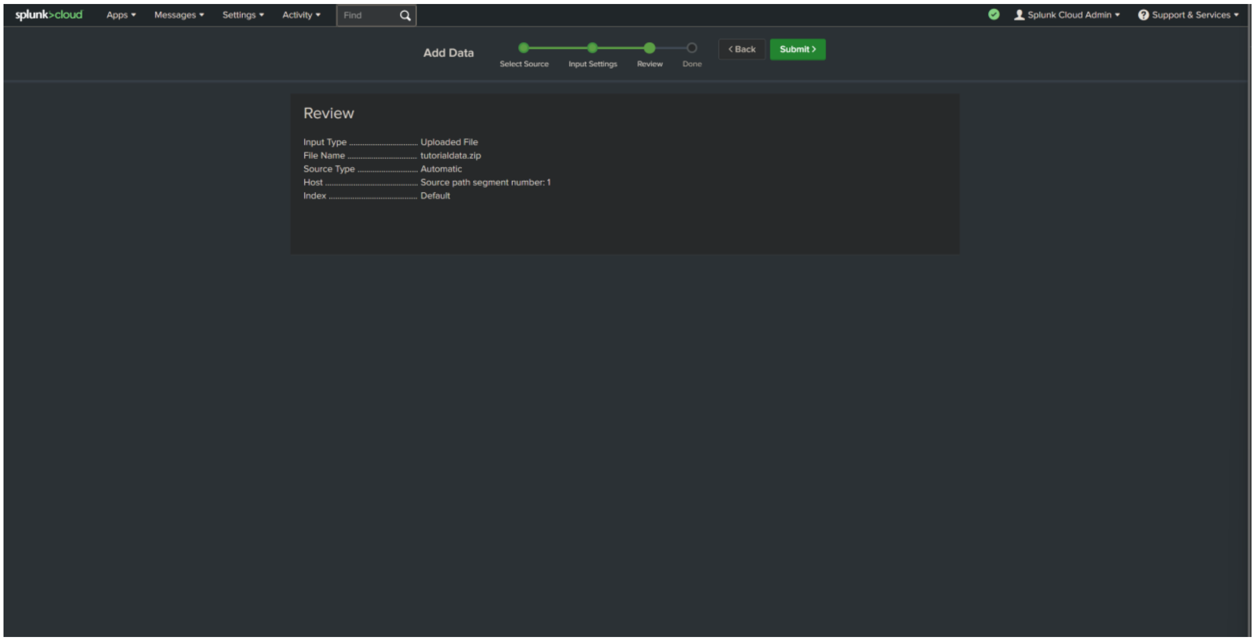
Lab Overview

- Upload sample log data
- Search through indexed data
- Evaluate search results
- Identify different data sources
- Locate failed SSH login(s) for the root account

The following are the details of the data in a zipped file which you will upload it into Splunk*:*

- mailsv - Buttercup Games' mail server. Examine events generated from this host.
- vendor_sales - Information about Buttercup Games' retail sales.
- www1 - This is one of Buttercup Games' web applications.
- www2 - This is one of Buttercup Games' web applications.
- www3 - This is one of Buttercup Games' web applications.

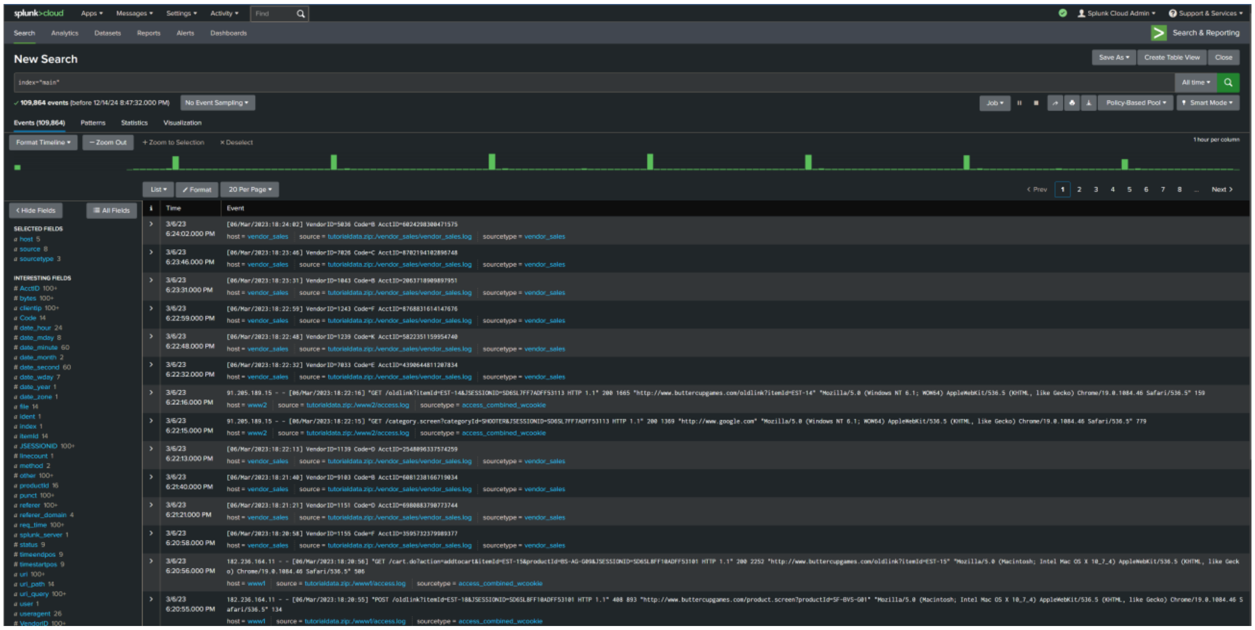
1. Login to Splunk
2. Add data to Splunk bar, upload sample tutorialdata.zip provided for the lab (https://drive.google.com/file/d/1nDz_DZB4ADbD4tvaDa54_l1FoT_jtVy4/view)



Review

Input Type .... Uploaded File
File Name .... tutorialdata.zip
Source Type .... Automatic
Host .... Source path segment number: 1
Index .... Default

3. Navigate to the Search and Reporting tab, enter your search query *index="main"* to view the query data and select *All time* to view all events across all time.



```
index="main"
```

✓ 109,864 events (before 12/14/24 8:47:32.000 PM)

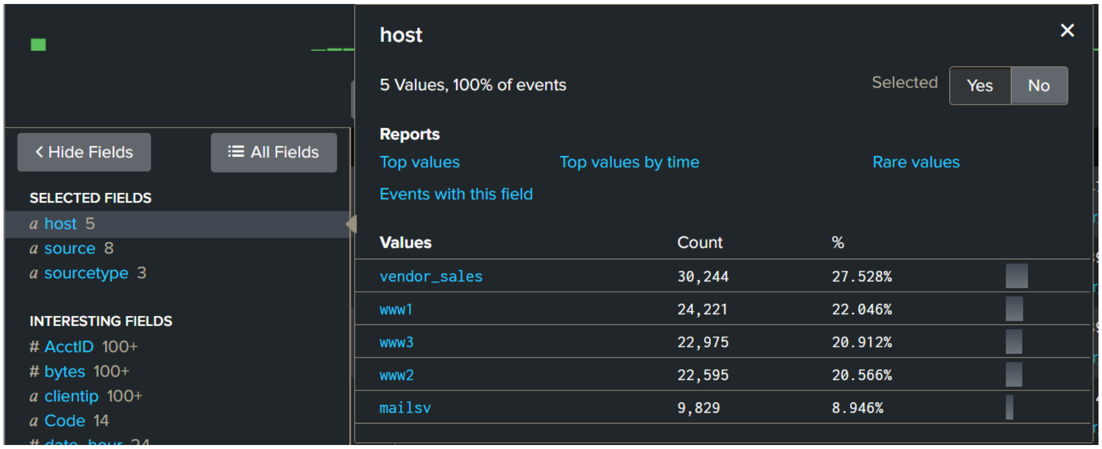
SELECTED FIELDS
a host 5
a source 8
a sourcetype 3

INTERESTING FIELDS
AcctID 100+
# bytes 100+
a clientip 100+
a Code 14
# date_hour 24
# date_mday 8
# date_minute 60
a date_month 2
# date_second 60
a date_wday 7
# date_year 1
a date_zone 1
a file 14
a ident 1
a index 1
a itemId 14
a JSESSIONID 100+
# linecount 1
a method 2
# other 100+
a productId 16
a punct 100+
a referer 100+
a referer_domain 4
a req_time 100+
a splunk_server 1
# status 9
# timeendpos 9
# timestartpos 9
a uri 100+
a uri_path 14
a uri_query 100+
a user 1
a useragent 26
VendorID 100+

```
> 3/6/23 6:24:02.000 PM  [06/Mar/2023:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575
                         host = vendor_sales | source = tutorialdata.zip:./vendor_sales/vendor_sales.log | sourcetype = vendor_sales
> 3/6/23 6:23:46.000 PM  [06/Mar/2023:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748
                         host = vendor_sales | source = tutorialdata.zip:./vendor_sales/vendor_sales.log | sourcetype = vendor_sales
> 3/6/23 6:23:31.000 PM  [06/Mar/2023:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951
                         host = vendor_sales | source = tutorialdata.zip:./vendor_sales/vendor_sales.log | sourcetype = vendor_sales
> 3/6/23 6:22:59.000 PM  [06/Mar/2023:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676
                         host = vendor_sales | source = tutorialdata.zip:./vendor_sales/vendor_sales.log | sourcetype = vendor_sales
> 3/6/23 6:22:48.000 PM  [06/Mar/2023:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740
                         host = vendor_sales | source = tutorialdata.zip:./vendor_sales/vendor_sales.log | sourcetype = vendor_sales
> 3/6/23 6:22:32.000 PM  [06/Mar/2023:18:22:32] VendorID=7033 Code=E AcctID=4390644811207834
                         host = vendor_sales | source = tutorialdata.zip:./vendor_sales/vendor_sales.log | sourcetype = vendor_sales
> 3/6/23 6:22:16.000 PM  91.205.189.15 - - [06/Mar/2023:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159
                         host = www2 | source = tutorialdata.zip:./www2/access.log | sourcetype = access_combined_wcookie
> 3/6/23 6:22:15.000 PM  91.205.189.15 - - [06/Mar/2023:18:22:15] "GET /category.screen?categoryId=SHOOTER&JSESSIONID=SD6SL7FF7ADFF53113 HTTP 1.1" 200 1369 "http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 779
                         host = www2 | source = tutorialdata.zip:./www2/access.log | sourcetype = access_combined_wcookie
> 3/6/23 6:22:13.000 PM  [06/Mar/2023:18:22:13] VendorID=1139 Code=D AcctID=2548096337574259
                         host = vendor_sales | source = tutorialdata.zip:./vendor_sales/vendor_sales.log | sourcetype = vendor_sales
> 3/6/23 6:21:40.000 PM  [06/Mar/2023:18:21:40] VendorID=9103 Code=B AcctID=6081238166719034
                         host = vendor_sales | source = tutorialdata.zip:./vendor_sales/vendor_sales.log | sourcetype = vendor_sales
> 3/6/23 6:21:21.000 PM  [06/Mar/2023:18:21:21] VendorID=1151 Code=D AcctID=6980883790773744
                         host = vendor_sales | source = tutorialdata.zip:./vendor_sales/vendor_sales.log | sourcetype = vendor_sales
> 3/6/23 6:20:58.000 PM  [06/Mar/2023:18:20:58] VendorID=1155 Code=F AcctID=3595732379989377
                         host = vendor_sales | source = tutorialdata.zip:./vendor_sales/vendor_sales.log | sourcetype = vendor_sales
> 3/6/23 6:20:56.000 PM  182.236.164.11 - - [06/Mar/2023:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Geck
                         o) Chrome/19.0.1084.46 Safari/536.5" 506
                         host = www1 | source = tutorialdata.zip:./www1/access.log | sourcetype = access_combined_wcookie
> 3/6/23 6:20:55.000 PM  182.236.164.11 - - [06/Mar/2023:18:20:55] "POST /oldlink?itemId=EST-18&JSESSIONID=SD6SL8FF10ADFF53101 HTTP 1.1" 408 893 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 S
                         afari/536.5" 134
                         host = www1 | source = tutorialdata.zip:./www1/access.log | sourcetype = access_combined_wcookie
```

4. There are three common attributes for the Selected Fields: host, source, and sourcetype

- Host: Specifies the name of the network host from which the event originated.



host

5 Values, 100% of events

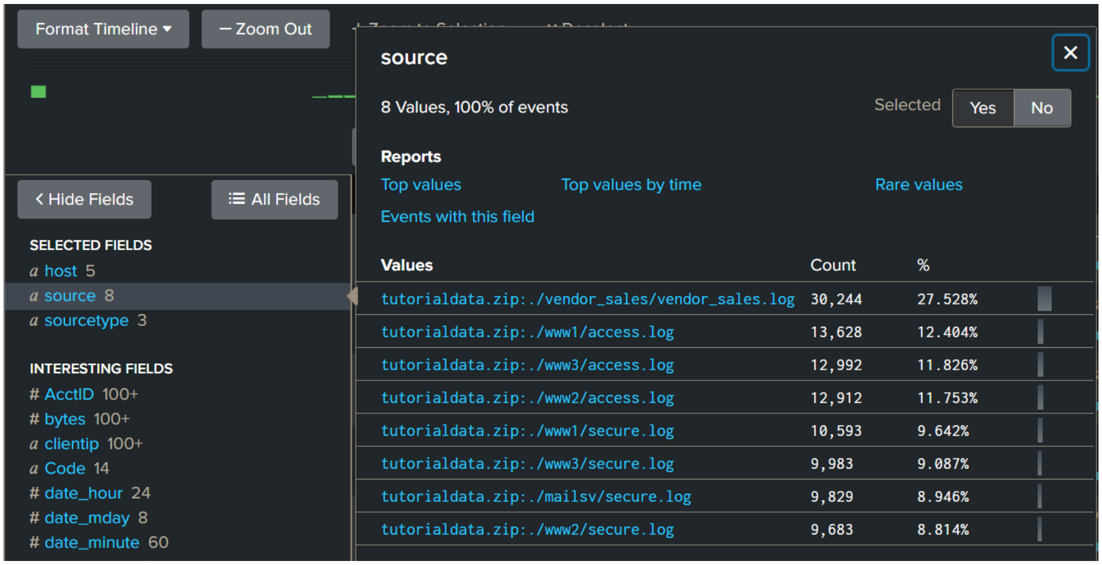
Reports

Top values | Top values by time | Rare values

Events with this field

Values	Count	%
vendor_sales	30,244	27.528%
www1	24,221	22.046%
www3	22,975	20.912%
www2	22,595	20.566%
mailsv	9,829	8.946%

- Source: Indicates the filename from which the event originates



source

8 Values, 100% of events

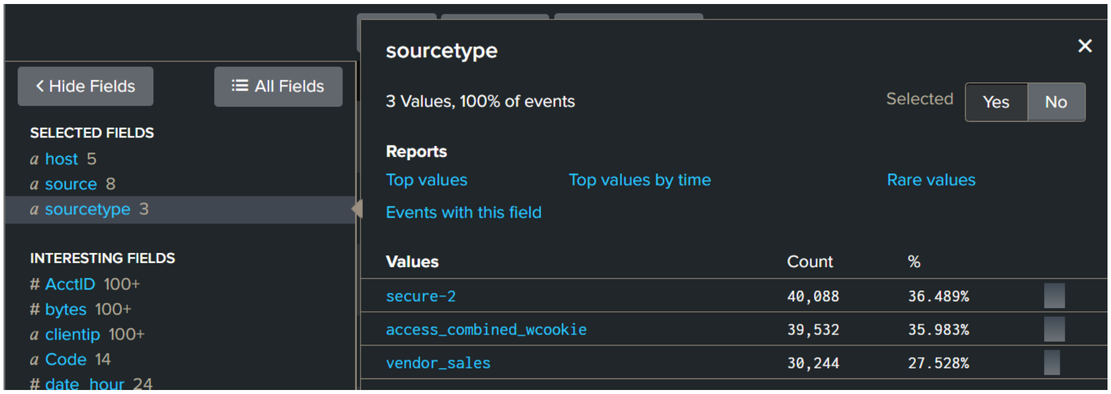
Reports

Top values | Top values by time | Rare values

Events with this field

Values	Count	%
tutorialdata.zip:./vendor_sales/vendor_sales.log	30,244	27.528%
tutorialdata.zip:./www1/access.log	13,628	12.404%
tutorialdata.zip:./www3/access.log	12,992	11.826%
tutorialdata.zip:./www2/access.log	12,912	11.753%
tutorialdata.zip:./www1/secure.log	10,593	9.642%
tutorialdata.zip:./www3/secure.log	9,983	9.087%
tutorialdata.zip:./mailsv/secure.log	9,829	8.946%
tutorialdata.zip:./www2/secure.log	9,683	8.814%

- sourcetype: Determines how data is formatted in structure of the event data.



sourcetype

3 Values, 100% of events

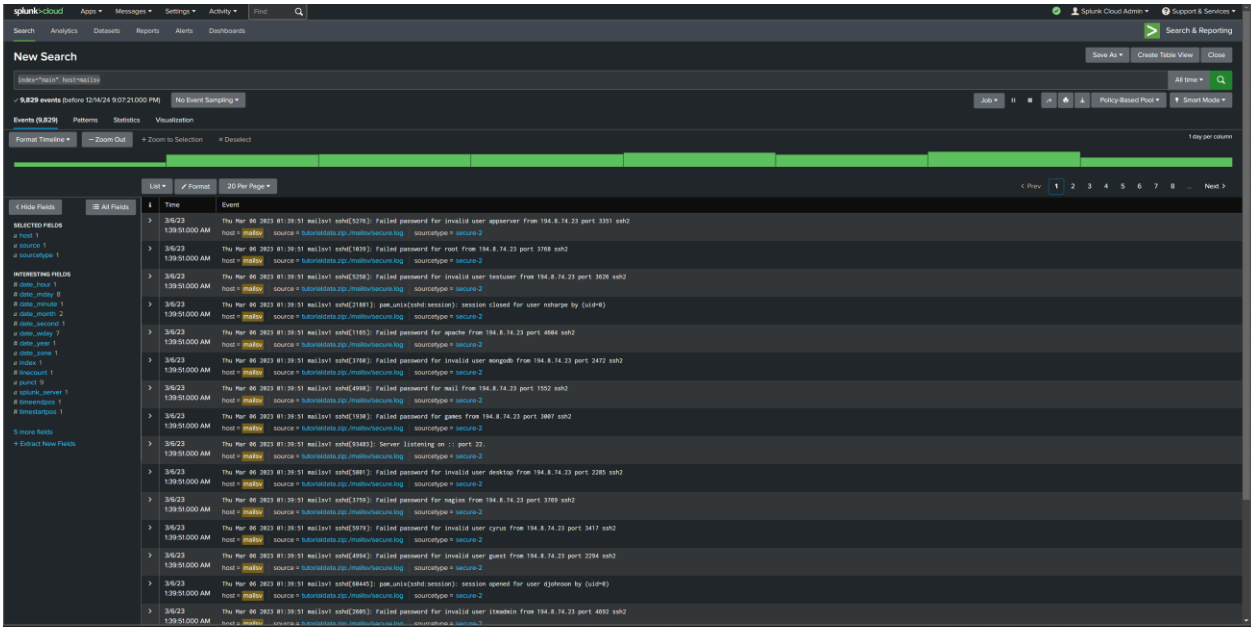
Reports

Top values | Top values by time | Rare values

Events with this field

Values	Count	%
secure-2	40,088	36.489%
access_combined_wcookie	39,532	35.983%
vendor_sales	30,244	27.528%

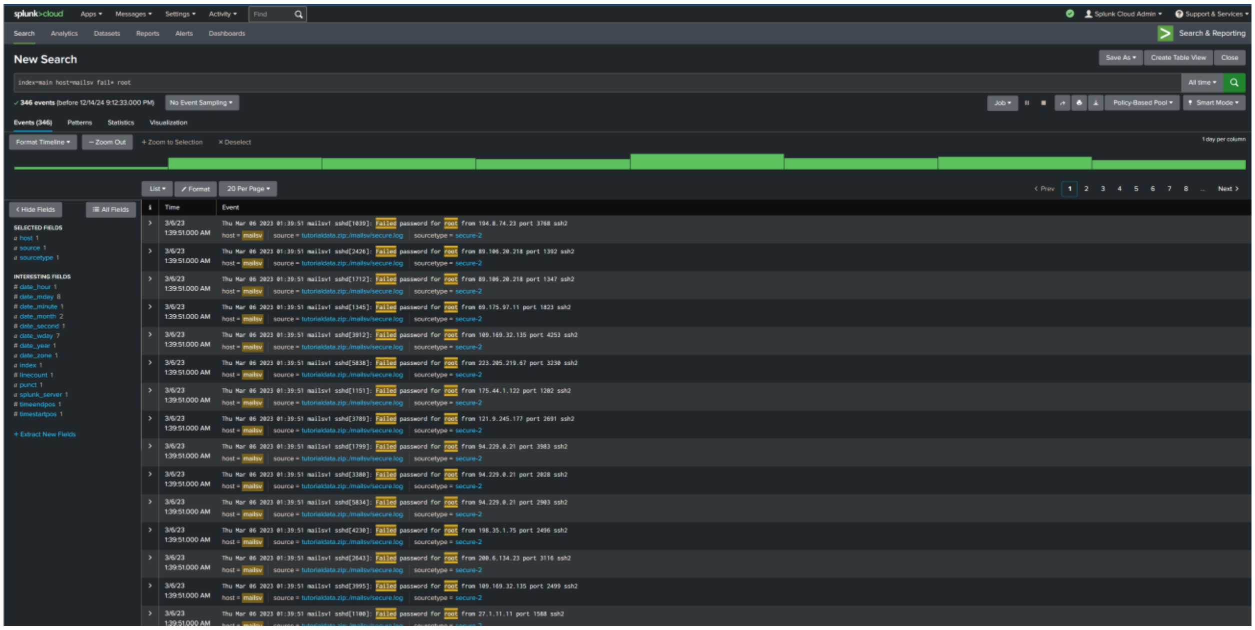
5. Explore any failed SSH logins for the root account on the mail server. To narrow down the search, query *index="main" host=mailsv.* The search results have narrowed to over 9000 events that are generated by the mail server.



```
index="main" host=mailsv
✓ 9,829 events (before 12/14/24 9:07:21.000 PM)
```

```
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[21881]: pam_unix(sshd:session): session closed for user nsharpe by (uid=0)
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[1930]: Failed password for games from 194.8.74.23 port 3007 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[93483]: Server listening on :: port 22.
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[5801]: Failed password for invalid user desktop from 194.8.74.23 port 2285 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[3759]: Failed password for nagios from 194.8.74.23 port 3769 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[5979]: Failed password for invalid user cyrus from 194.8.74.23 port 3417 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[4994]: Failed password for invalid user guest from 194.8.74.23 port 2294 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[60445]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[2605]: Failed password for invalid user itmadmin from 194.8.74.23 port 4092 ssh2
```

6. Continue to narrow down the search results generated by the mail server to locate any failed SSH logins for the root account. Query *index=main host=mailsv fail* root.*
 This search expands on the search from the previous task and searches for the keyword fail*. The wildcard tells Splunk to expand the search term to find other terms that contain the word fail such as failure, failed, etc. Lastly, the keyword root searches for any event that contains the term root.



```
index=main host=mailsv fail* root
✓ 346 events (before 12/14/24 9:12:33.000 PM)
```

```
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[2426]: Failed password for root from 89.106.20.218 port 1392 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[1712]: Failed password for root from 89.106.20.218 port 1347 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[1345]: Failed password for root from 69.175.97.11 port 1823 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[3912]: Failed password for root from 109.169.32.135 port 4253 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[5838]: Failed password for root from 223.205.219.67 port 3230 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[1151]: Failed password for root from 175.44.1.122 port 1202 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[3789]: Failed password for root from 121.9.245.177 port 2691 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[1799]: Failed password for root from 94.229.0.21 port 3983 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[3380]: Failed password for root from 94.229.0.21 port 2028 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[5834]: Failed password for root from 94.229.0.21 port 2903 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[4230]: Failed password for root from 198.35.1.75 port 2496 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[2643]: Failed password for root from 200.6.134.23 port 3116 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[3995]: Failed password for root from 109.169.32.135 port 2499 ssh2
                       host = mailsv  source = tutorialdata.zip:./mailsv/secure.log  sourcetype = secure-2
3/6/23 1:39:51.000 AM  Thu Mar 06 2023 01:39:51 mailsv1 sshd[1100]: Failed password for root from 27.1.11.11 port 1588 ssh2
```

7. Investigation:
   - There are over 100,000 events that are contained in the main index across all time.
   - Host: Specifies the name of the network host from which the event originated.
   - Source: Indicates the filename from which the event originates
   - sourcetype: Determines how data is formatted in structure of the event data.
   - As of February 11th, 2024, there have been 346 failed SSH logins for the root account on the mail server.