TASK 2: Security Alert Monitoring & Incident Response

1. **Environment Setup**

   ○ Tool used: Splunk Free Trial

   ○ Platform: Kali Linux / Browser

---

2. Installing Splunk

To simulate a real SOC workflow, I needed to install and run **Splunk Enterprise** locally:

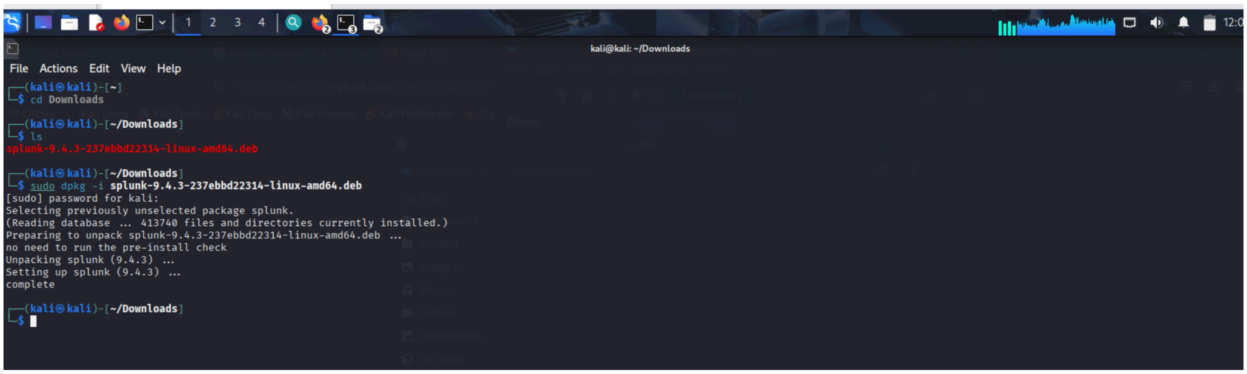
Steps Taken:

- Registered for a free account at: splunk.com
- Downloaded **Splunk Enterprise** `.deb` file for Linux (64-bit)
- Moved the file to Kali's `Downloads` directory

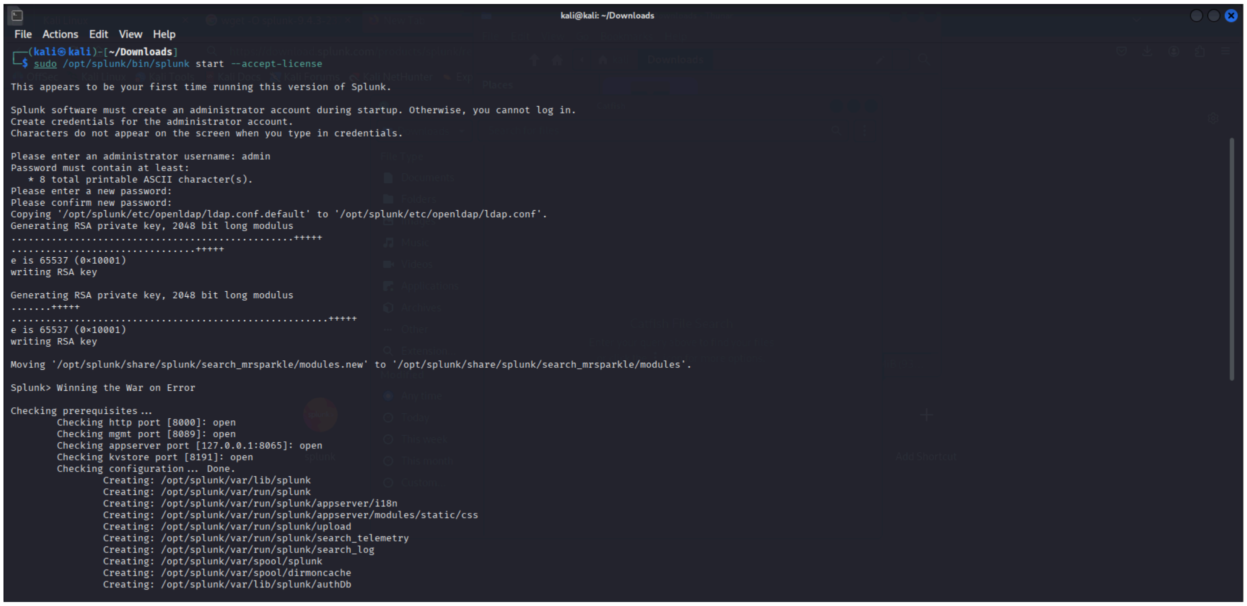
Installation Command Used:

bash

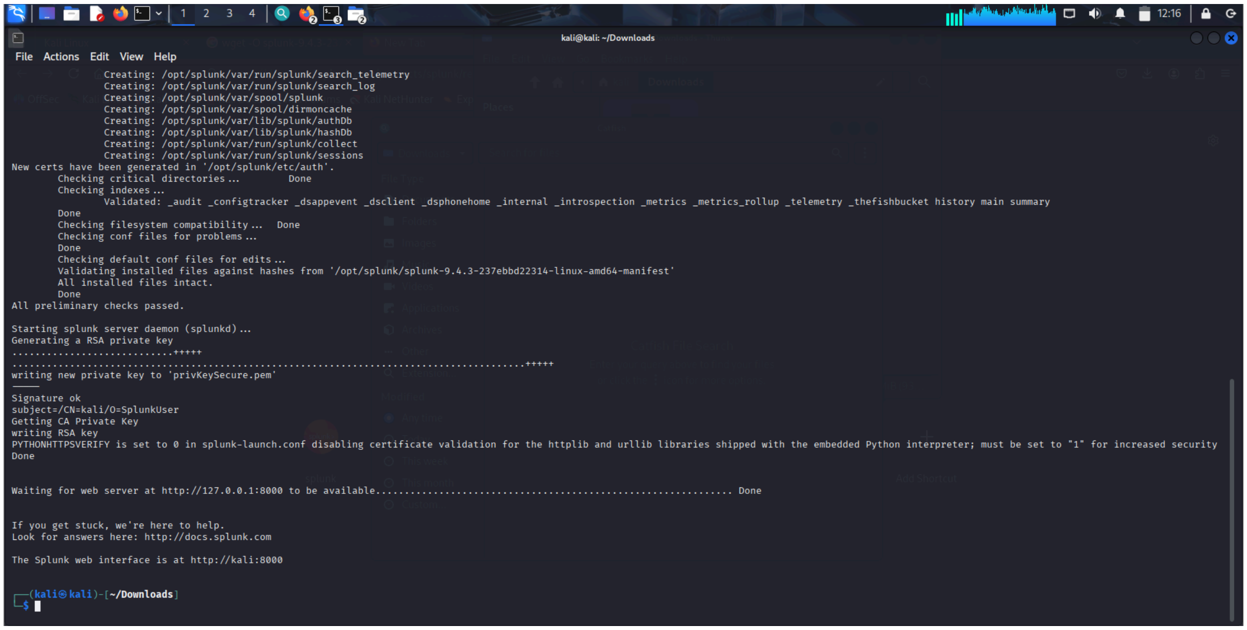
```
cd ~/Downloads

sudo dpkg -i splunk-9.4.3-xxxx-linux-amd64.deb
```



```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
splunk-9.4.3-237ebbd22314-linux-amd64.deb

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i splunk-9.4.3-237ebbd22314-linux-amd64.deb
[sudo] password for kali:
Selecting previously unselected package splunk.
(Reading database ... 413740 files and directories currently installed.)
Preparing to unpack splunk-9.4.3-237ebbd22314-linux-amd64.deb ...
no need to run the pre-install check
Unpacking splunk (9.4.3) ...
Setting up splunk (9.4.3) ...
complete

┌──(kali㉿kali)-[~/Downloads]
└─$ 
```



```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo /opt/splunk/bin/splunk start --accept-license

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise, you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: admin
Password must contain at least:
   * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password:
Copying '/opt/splunk/etc/openldap/ldap.conf.default' to '/opt/splunk/etc/openldap/ldap.conf'.
Generating RSA private key, 2048 bit long modulus
.................................................+++++
................................+++++
e is 65537 (0×10001)
writing RSA key

Generating RSA private key, 2048 bit long modulus
.......+++++
.......................................................+++++
e is 65537 (0×10001)
writing RSA key

Moving '/opt/splunk/share/splunk/search_mrsparkle/modules.new' to '/opt/splunk/share/splunk/search_mrsparkle/modules'.

Splunk> Winning the War on Error

Checking prerequisites ...
        Checking http port [8000]: open
        Checking mgmt port [8089]: open
        Checking appserver port [127.0.0.1:8065]: open
        Checking kvstore port [8191]: open
        Checking configuration ... Done.
                Creating: /opt/splunk/var/lib/splunk
                Creating: /opt/splunk/var/run/splunk
                Creating: /opt/splunk/var/run/splunk/appserver/i18n
                Creating: /opt/splunk/var/run/splunk/appserver/modules/static/css
                Creating: /opt/splunk/var/run/splunk/upload
                Creating: /opt/splunk/var/run/splunk/search_telemetry
                Creating: /opt/splunk/var/run/splunk/search_log
                Creating: /opt/splunk/var/spool/splunk
                Creating: /opt/splunk/var/spool/dirmoncache
                Creating: /opt/splunk/var/lib/splunk/authDb
```



```
                Creating: /opt/splunk/var/run/splunk/search_telemetry
                Creating: /opt/splunk/var/run/splunk/search_log
                Creating: /opt/splunk/var/spool/splunk
                Creating: /opt/splunk/var/spool/dirmoncache
                Creating: /opt/splunk/var/lib/splunk/authDb
                Creating: /opt/splunk/var/lib/splunk/hashDb
                Creating: /opt/splunk/var/run/splunk/collect
                Creating: /opt/splunk/var/run/splunk/sessions
New certs have been generated in '/opt/splunk/etc/auth'.
        Checking critical directories ...        Done
        Checking indexes ...
                Validated: _audit _configtracker _dsappevent _dsclient _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary
        Done
        Checking filesystem compatibility ...  Done
        Checking conf files for problems ...
        Done
        Checking default conf files for edits ...
        Validating installed files against hashes from '/opt/splunk/splunk-9.4.3-237ebbd22314-linux-amd64-manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd) ...
Generating a RSA private key
............................+++++
.....................................................................................+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=kali/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done


Waiting for web server at http://127.0.0.1:8000 to be available............................................................. Done


If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://kali:8000


┌──(kali㉿kali)-[~/Downloads]
└─$ 
```

- Accepted license and created admin login using:

```
sudo /opt/splunk/bin/splunk start --accept-license
```

- Accessed the Splunk Web Interface at:

  ```
  http://localhost:8000
  ```

---

3. Preparing the Log Data

Original Log Format:

The internship provided logs in a simple text format:

```
2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
```

This format was not compatible with Splunk's event parsing engine.Thus, To make the data compatible with Splunk:

- Opened the text file in Kali’s Text Editor
- Reformatted the data into CSV format with headers

---

4. Fixing the Log Format

To enable Splunk to correctly parse the logs:

- I opened **Text Editor** in Kali Linux
- Reformatted the logs into a proper `.csv` format with headers:

✅ Sample Format:

```
timestamp,user,ip,action,threat

2025-07-03 06:13:14,charlie,10.0.0.5,connection attempt,

2025-07-03 05:48:14,bob,10.0.0.5,malware detected,Trojan Detected

2025-07-03 07:02:14,alice,203.0.113.77,login failed,
```

- Saved the file as:

  `SOC_Task2_Formatted.csv`

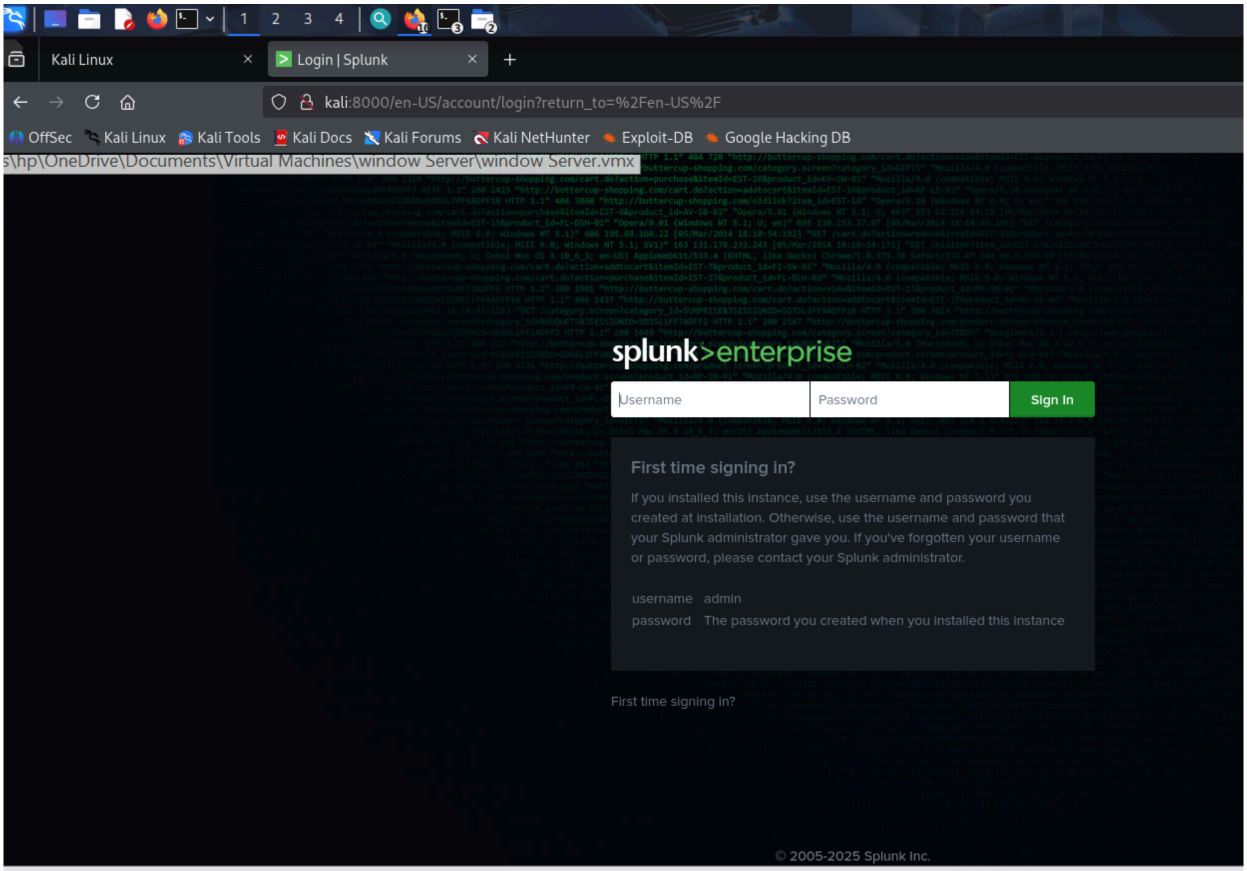
in the Kali `Downloads` folder.

---

5. Uploading Log File into Splunk

From Splunk Web Interface:

1. **Settings** → **Add Data**
2. **Upload** → Selected `SOC_Task2_Formatted.csv`
3. On **Set Source Type**:
   - Chose: `Structured > csv`
4. On **Input Settings**:
   - Index: `main`
5. Reviewed & clicked **Submit**


Kali Linux
Login | Splunk
kali:8000/en-US/account/login?return_to=%2Fen-US%2F
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
s\hp\OneDrive\Documents\Virtual Machines\window Server\window Server.vmx
splunk>enterprise
Username
Password
Sign In

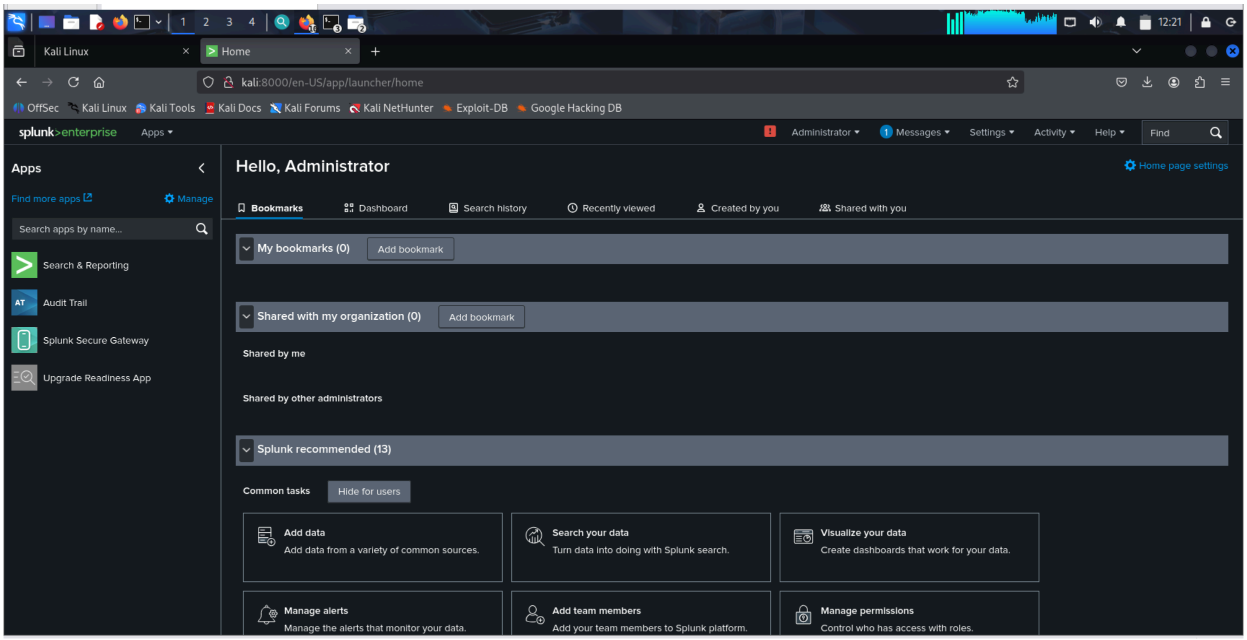
First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password The password you created when you installed this instance

First time signing in?

© 2005-2025 Splunk Inc.


12:21
Kali Linux
Home
kali:8000/en-US/app/launcher/home
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
splunk>enterprise Apps ▾
Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find
Apps
Find more apps Manage
Search apps by name...
Search & Reporting
Audit Trail
Splunk Secure Gateway
Upgrade Readiness App
Home page settings
Bookmarks Dashboard Search history Recently viewed Created by you Shared with you
Add bookmark
Add bookmark
Hide for users

Hello, Administrator

My bookmarks (0)

Shared with my organization (0)

Shared by me

Shared by other administrators

Splunk recommended (13)

Common tasks

Add data
Add data from a variety of common sources.

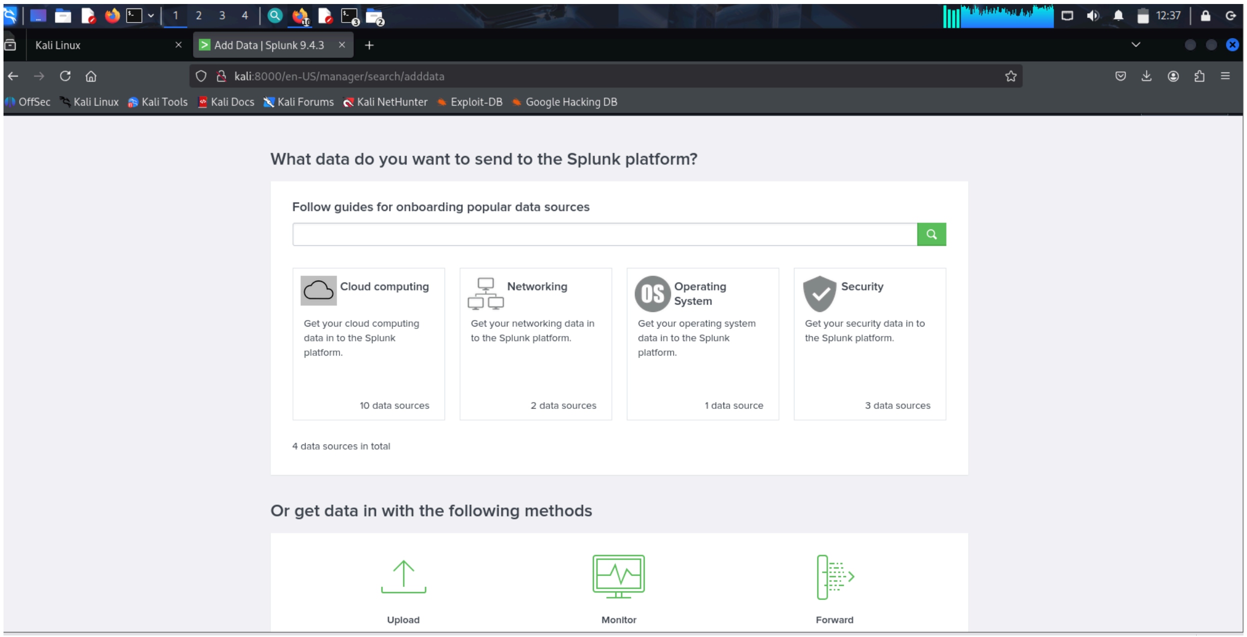
Search your data
Turn data into doing with Splunk search.

Visualize your data
Create dashboards that work for your data.

Manage alerts
Manage the alerts that monitor your data.

Add team members
Add your team members to Splunk platform.

Manage permissions
Control who has access with roles.



What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources

Cloud computing

Get your cloud computing data in to the Splunk platform.

10 data sources

Networking

Get your networking data in to the Splunk platform.

2 data sources

Operating System

Get your operating system data in to the Splunk platform.

1 data source

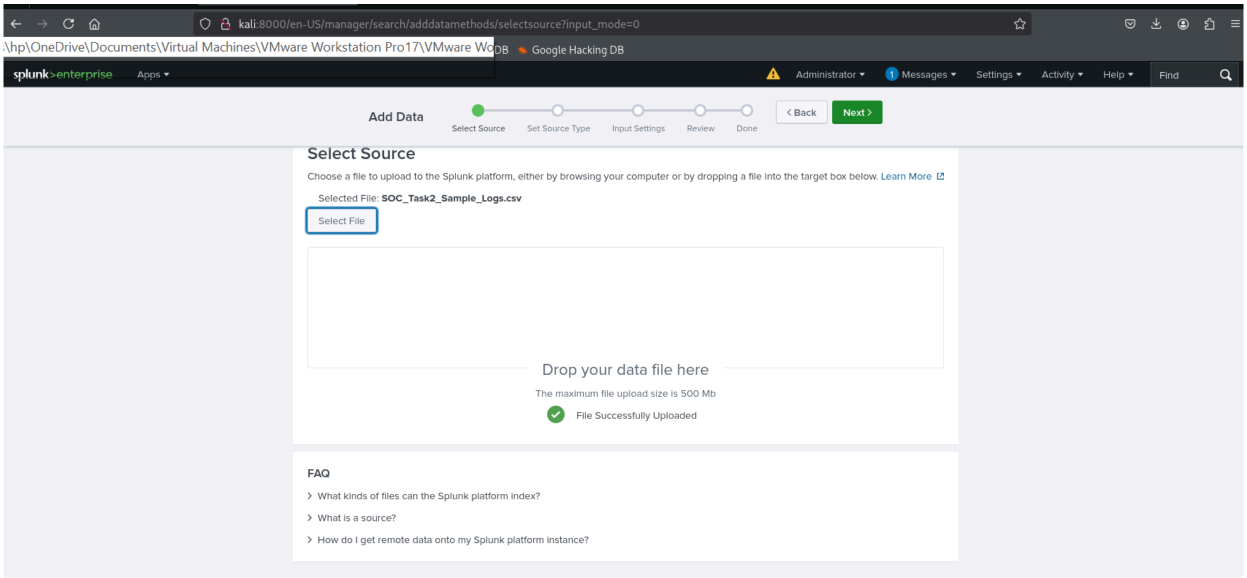
Security

Get your security data in to the Splunk platform.

3 data sources

4 data sources in total

Or get data in with the following methods



Select Source

Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below. Learn More

Selected File: **SOC_Task2_Sample_Logs.csv**

Drop your data file here

The maximum file upload size is 500 Mb

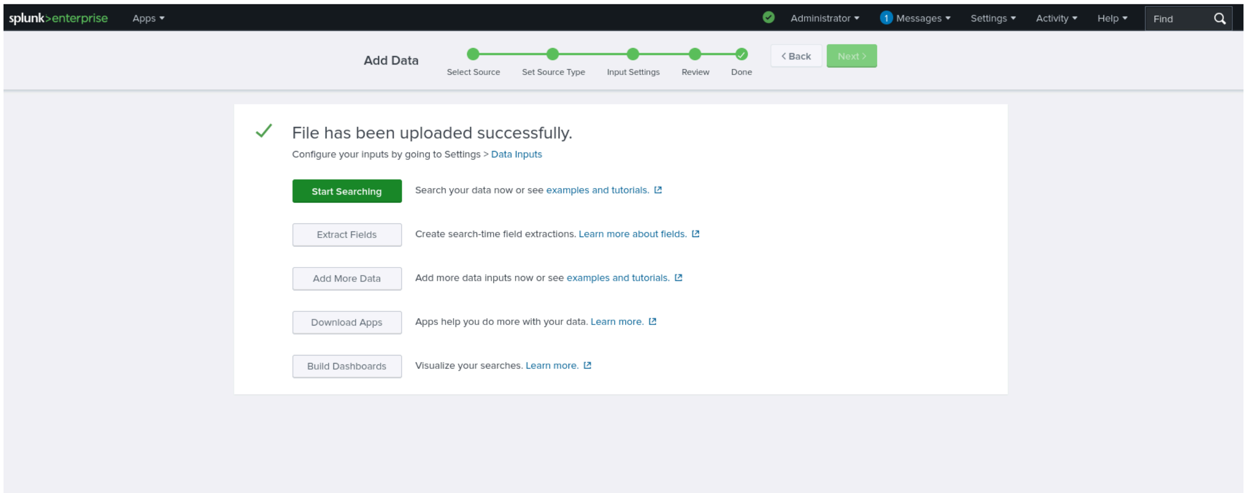
✓ File Successfully Uploaded

FAQ

› What kinds of files can the Splunk platform index?

› What is a source?

› How do I get remote data onto my Splunk platform instance?



✓ File has been uploaded successfully.

Configure your inputs by going to Settings > Data Inputs

Start Searching — Search your data now or see examples and tutorials.

Extract Fields — Create search-time field extractions. Learn more about fields.

Add More Data — Add more data inputs now or see examples and tutorials.

Download Apps — Apps help you do more with your data. Learn more.

Build Dashboards — Visualize your searches. Learn more.

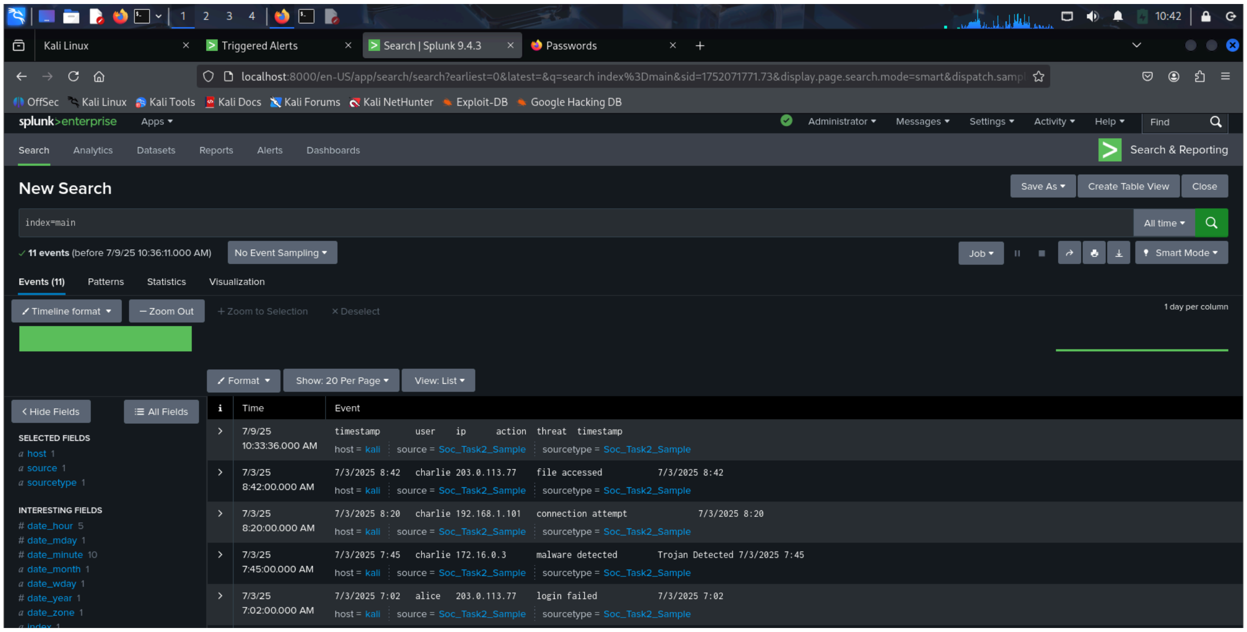
✅ Splunk confirmed that the data input was created successfully.

---

6. Next Steps (Performed)

Ran Searches in Splunk using:

- `source="Soc_Task2_Formatted.csv" "malware detected"`
- `source="Soc_Task2_Formatted.csv" "login failed"`
- `source="Soc_Task2_Formatted.csv" "file accessed"`



New Search

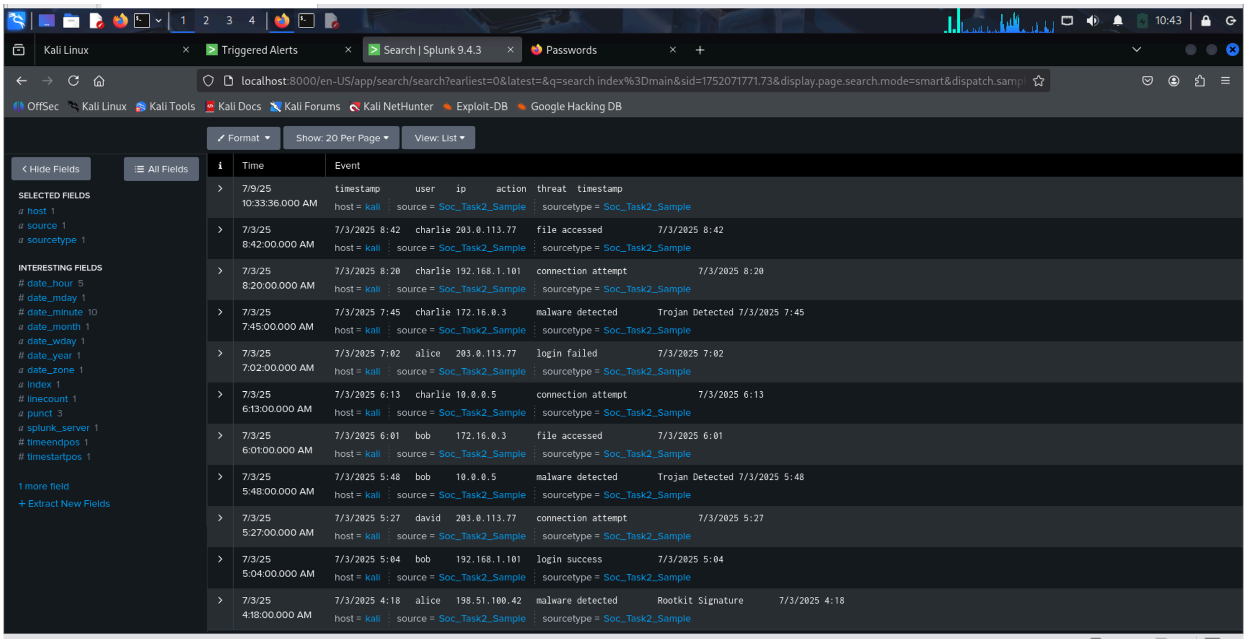
```
index=main
```

✓ 11 events (before 7/9/25 10:36:11.000 AM) No Event Sampling

SELECTED FIELDS
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS
- date_hour 5
- date_mday 1
- date_minute 10
- date_month 1
- date_wday 1
- date_year 1
- date_zone 1
- index 1

```
i  Time                 Event
>  7/9/25               timestamp       user    ip      action  threat  timestamp
   10:33:36.000 AM      host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 8:42   charlie 203.0.113.77    file accessed          7/3/2025 8:42
   8:42:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 8:20   charlie 192.168.1.101   connection attempt            7/3/2025 8:20
   8:20:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 7:45   charlie 172.16.0.3      malware detected       Trojan Detected 7/3/2025 7:45
   7:45:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 7:02   alice   203.0.113.77    login failed           7/3/2025 7:02
   7:02:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
```

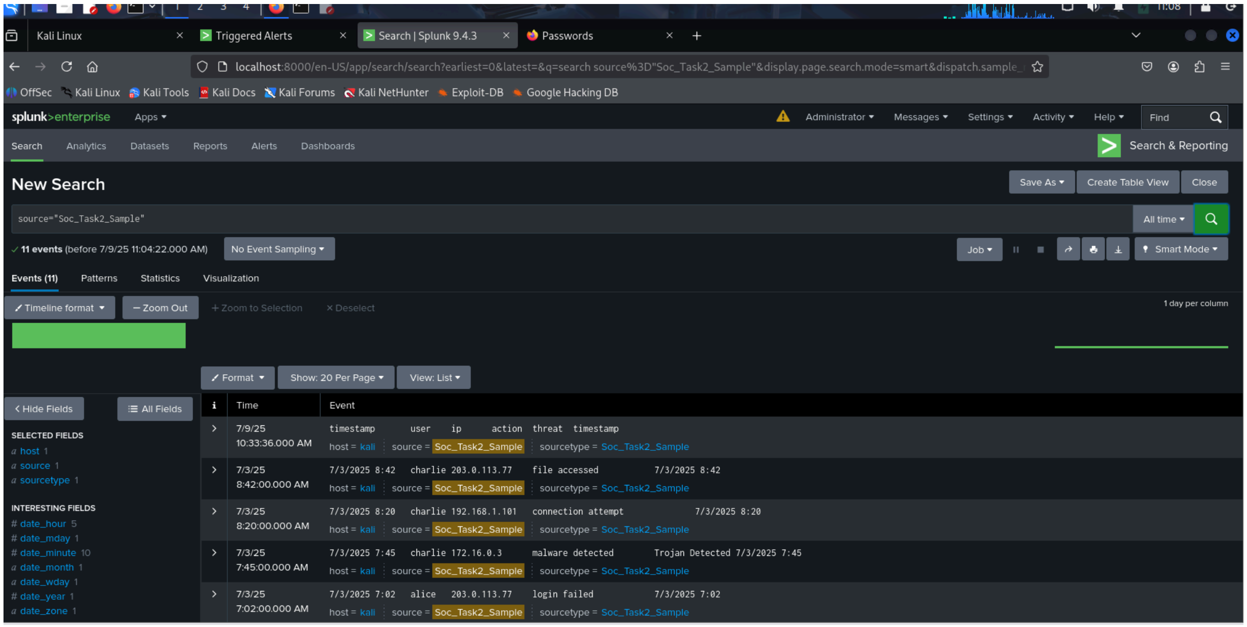


SELECTED FIELDS
- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS
- date_hour 5
- date_mday 1
- date_minute 10
- date_month 1
- date_wday 1
- date_year 1
- date_zone 1
- index 1
- linecount 1
- punct 3
- splunk_server 1
- timeendpos 1
- timestartpos 1

1 more field
+ Extract New Fields

```
i  Time                 Event
>  7/9/25               timestamp       user    ip      action  threat  timestamp
   10:33:36.000 AM      host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 8:42   charlie 203.0.113.77    file accessed          7/3/2025 8:42
   8:42:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 8:20   charlie 192.168.1.101   connection attempt            7/3/2025 8:20
   8:20:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 7:45   charlie 172.16.0.3      malware detected       Trojan Detected 7/3/2025 7:45
   7:45:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 7:02   alice   203.0.113.77    login failed           7/3/2025 7:02
   7:02:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 6:13   charlie 10.0.0.5        connection attempt            7/3/2025 6:13
   6:13:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 6:01   bob     172.16.0.3      file accessed          7/3/2025 6:01
   6:01:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 5:48   bob     10.0.0.5        malware detected       Trojan Detected 7/3/2025 5:48
   5:48:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 5:27   david   203.0.113.77    connection attempt            7/3/2025 5:27
   5:27:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 5:04   bob     192.168.1.101   login success          7/3/2025 5:04
   5:04:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 4:18   alice   198.51.100.42   malware detected       Rootkit Signature      7/3/2025 4:18
   4:18:00.000 AM       host = kali  source = Soc_Task2_Sample  sourcetype = Soc_Task2_Sample
```



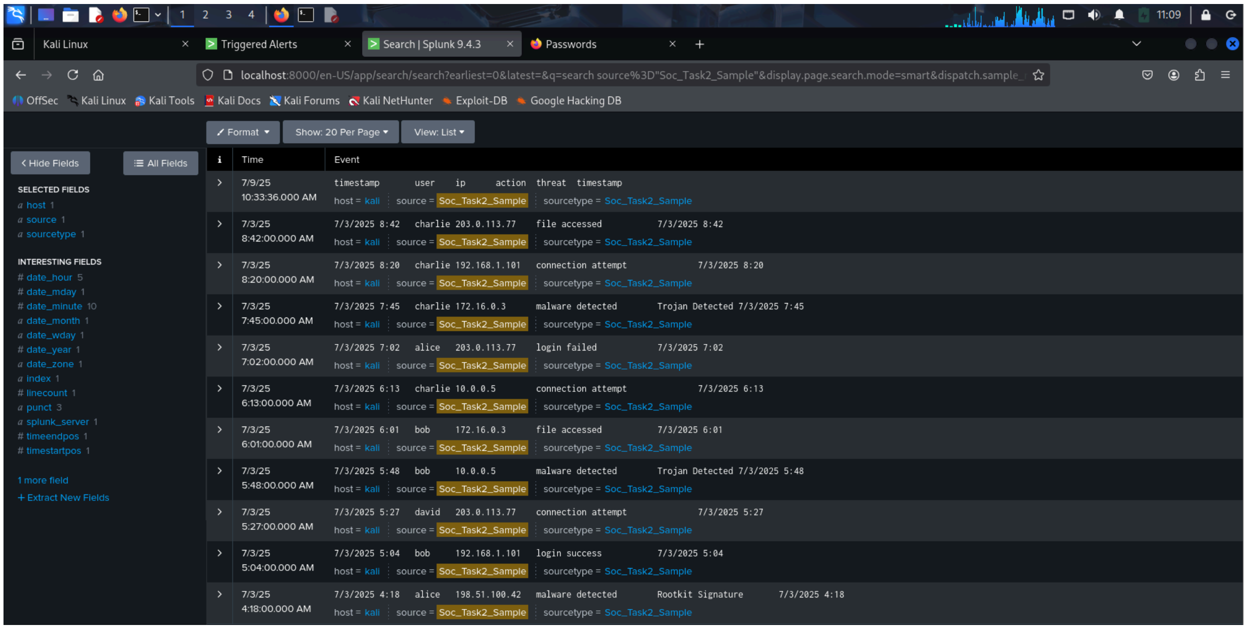
```
source="Soc_Task2_Sample"
```

✓ 11 events (before 7/9/25 11:04:22.000 AM) No Event Sampling

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- # date_hour 5
- # date_mday 1
- # date_minute 10
- a date_month 1
- a date_wday 1
- # date_year 1
- a date_zone 1

```
i  Time                 Event
>  7/9/25               timestamp       user    ip      action  threat  timestamp
   10:33:36.000 AM      host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 8:42   charlie 203.0.113.77    file accessed           7/3/2025 8:42
   8:42:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 8:20   charlie 192.168.1.101   connection attempt              7/3/2025 8:20
   8:20:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 7:45   charlie 172.16.0.3      malware detected        Trojan Detected 7/3/2025 7:45
   7:45:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 7:02   alice   203.0.113.77    login failed            7/3/2025 7:02
   7:02:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
```



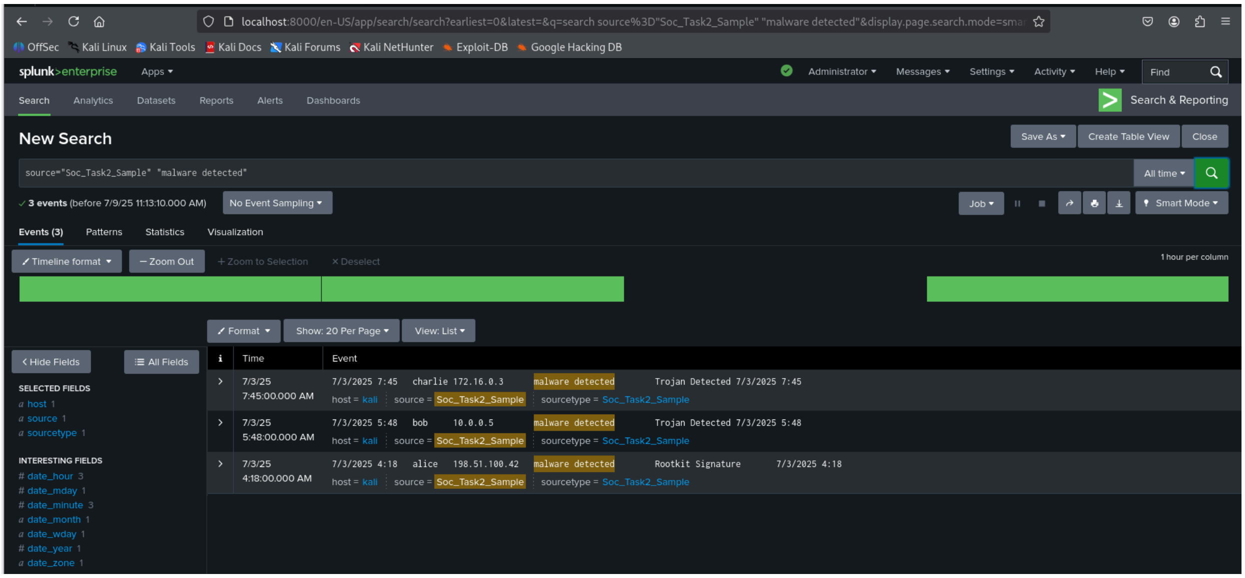
SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- # date_hour 5
- # date_mday 1
- # date_minute 10
- a date_month 1
- a date_wday 1
- # date_year 1
- a date_zone 1
- a index 1
- # linecount 1
- a punct 3
- a splunk_server 1
- # timeendpos 1
- # timestartpos 1

1 more field

+ Extract New Fields

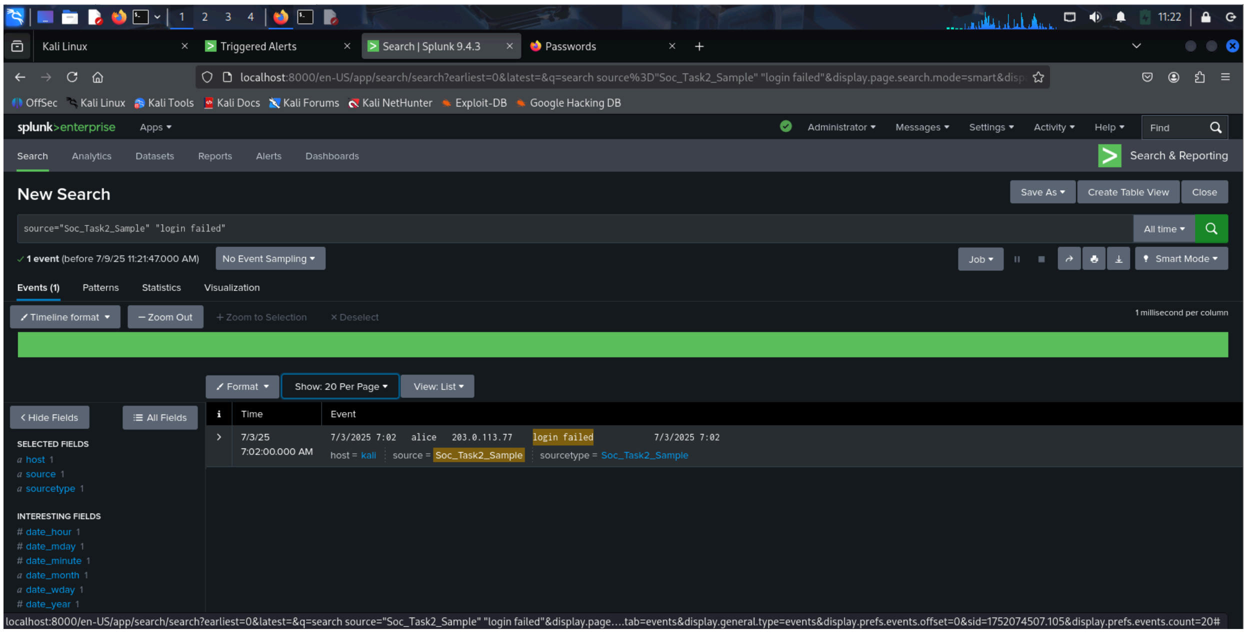
```
i  Time                 Event
>  7/9/25               timestamp       user    ip      action  threat  timestamp
   10:33:36.000 AM      host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 8:42   charlie 203.0.113.77    file accessed           7/3/2025 8:42
   8:42:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 8:20   charlie 192.168.1.101   connection attempt              7/3/2025 8:20
   8:20:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 7:45   charlie 172.16.0.3      malware detected        Trojan Detected 7/3/2025 7:45
   7:45:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 7:02   alice   203.0.113.77    login failed            7/3/2025 7:02
   7:02:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 6:13   charlie 10.0.0.5        connection attempt              7/3/2025 6:13
   6:13:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 6:01   bob     172.16.0.3      file accessed           7/3/2025 6:01
   6:01:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 5:48   bob     10.0.0.5        malware detected        Trojan Detected 7/3/2025 5:48
   5:48:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 5:27   david   203.0.113.77    connection attempt              7/3/2025 5:27
   5:27:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 5:04   bob     192.168.1.101   login success           7/3/2025 5:04
   5:04:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25               7/3/2025 4:18   alice   198.51.100.42   malware detected        Rootkit Signature       7/3/2025 4:18
   4:18:00.000 AM       host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
```



```
source="Soc_Task2_Sample" "malware detected"
```

✓ 3 events (before 7/9/25 11:13:10.000 AM)

```
i  Time                  Event
>  7/3/25                7/3/2025 7:45   charlie 172.16.0.3     malware detected       Trojan Detected 7/3/2025 7:45
   7:45:00.000 AM        host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25                7/3/2025 5:48   bob     10.0.0.5       malware detected       Trojan Detected 7/3/2025 5:48
   5:48:00.000 AM        host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
>  7/3/25                7/3/2025 4:18   alice   198.51.100.42  malware detected       Rootkit Signature      7/3/2025 4:18
   4:18:00.000 AM        host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
```



```
source="Soc_Task2_Sample" "login failed"
```

✓ 1 event (before 7/9/25 11:21:47.000 AM)

```
i  Time                  Event
>  7/3/25                7/3/2025 7:02   alice   203.0.113.77   login failed           7/3/2025 7:02
   7:02:00.000 AM        host = kali   source = Soc_Task2_Sample   sourcetype = Soc_Task2_Sample
```

These searches helped filter and retrieve relevant events for:

- Malware alerts
- Failed login attempts
- Suspicious file access activities

7. Threat Severity Summary:

Threat Type	Severity
Malware Detected	**High**
Multiple Failed Logins	**Medium**
Connection Attempts	**Low**
Rootkit Detected	**Critical**
File Accessed from 10.0.x or 198.x.x.x	**Medium**

8. Alert Categorization and Prioritization

- Timeline of events
- Alert classification (High/Med/Low)
- Recommendations

Below is a summary table showing the categorization and prioritization of security events identified during log analysis in Splunk.

Timestamp	User	Action	Threat / Detail	IP Address	Severity	Justification
2025-07-03 05:48:14	bob	malware detected	Trojan Detected	10.0.0.5	High	Malware poses high system risk
2025-07-03 04:18:14	alice	malware detected	Rootkit Signature	198.51.100.42	Critical	Rootkits are stealthy and dangerous
2025-07-03 07:45:14	charlie	malware detected	Trojan Detected	172.16.0.3	High	Trojan attack on internal IP
2025-07-03 07:02:14	alice	login failed	N/A	203.0.113.77	Medium	Failed login from external IP
2025-07-03 08:42:14	charlie	file accessed	N/A	203.0.113.77	Low	Normal file access unless repeated
2025-07-03 05:27:14	david	connection attempt	N/A	203.0.113.77	Medium	Suspicious repeated attempts
2025-07-03 05:04:14	bob	login success	N/A	192.168.1.101	Low	Valid login from known IP

Analysis Summary

- **Malware detected from users `bob`, `alice`, `charlie`**
- **Rootkit Signature detected from `alice`**
- **Failed login attempt from `alice`**
- **Suspicious connection attempts from IPs like `203.0.113.77`**

9. Simulate Communication with Stakeholders about the Incident

Subject: Incident Alert: Trojan Malware Detected on Host 10.0.0.5

Dear Team,

This is to notify you that on **July 3, 2025**, at **05:48 AM**, our monitoring systems detected a **Trojan malware infection** on internal IP `10.0.0.5` associated with user `bob`.

Incident Details:

- **Type:** Malware Detected (Trojan)
- **IP:** 10.0.0.5
- **User:** bob
- **Severity:** High
- **Action Taken:** Logged and reported for immediate isolation

We recommend initiating malware scans, reviewing lateral movement,Patch and update systems and enforcing user authentication policies.

Please escalate to SOC Lead if further investigation is needed.

Regards,
Mary-Claret Ogwuegbu
SOC Intern – Future Interns
`futureinterns.com`

How SOC Teams Track and Manage Threats Using Dashboards and Playbooks

Dashboards in Splunk

As part of this simulation, I created a simple dashboard in Splunk to help visualize threat trends and track security events efficiently.

Under a section titled **"SOC Dashboard Panel – Malware Detection"**,

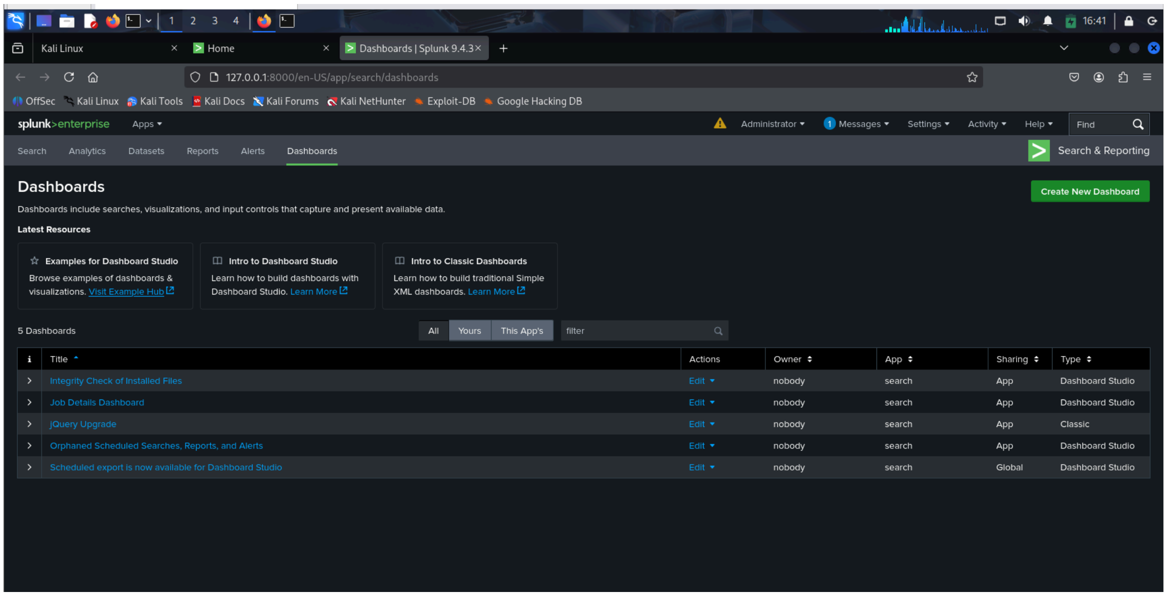
I navigated to **Search & Reporting**

Filtered for malware incidents using:

```
source="Soc_Task2_Sample" "malware detected"
```

- Switched to the **Visualization tab** and selected a **Bar Chart**
- Saved the panel to a dashboard titled: **SOC Threat Overview**
- Panel Name: **Malware Detections by User**
- This visual helped illustrate how many malware incidents were associated with each user

Screenshot of the dashboard was taken and added to the report under visual evidence.



Dashboards

Dashboards include searches, visualizations, and input controls that capture and present available data.

Latest Resources

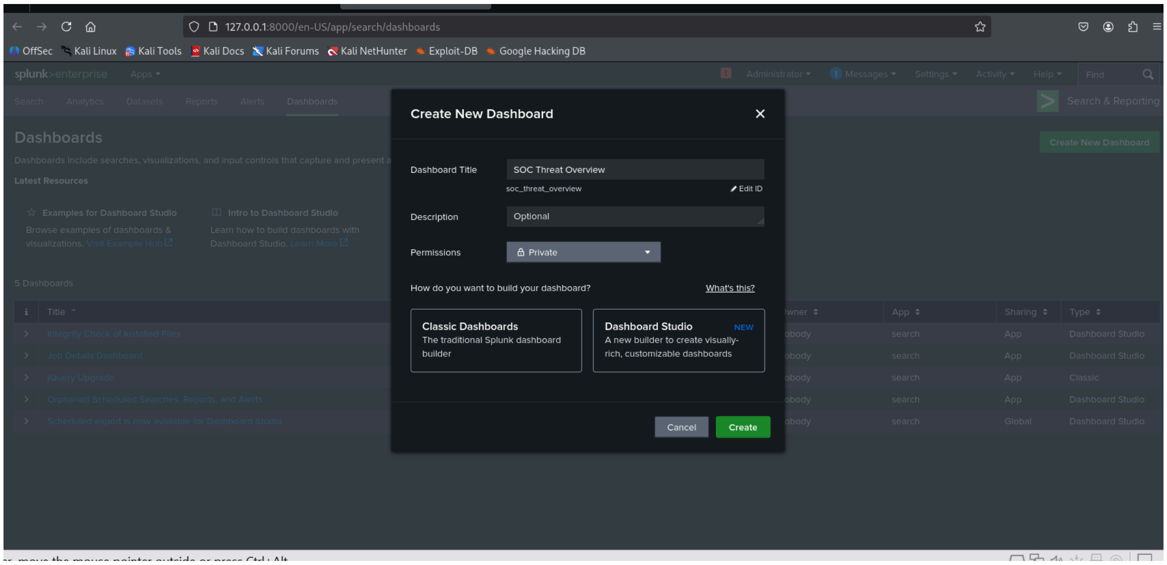
☆ **Examples for Dashboard Studio**
Browse examples of dashboards & visualizations. Visit Example Hub

Intro to Dashboard Studio
Learn how to build dashboards with Dashboard Studio. Learn More

Intro to Classic Dashboards
Learn how to build traditional Simple XML dashboards. Learn More

5 Dashboards

i	Title	Actions	Owner	App	Sharing	Type
›	Integrity Check of Installed Files	Edit ▾	nobody	search	App	Dashboard Studio
›	Job Details Dashboard	Edit ▾	nobody	search	App	Dashboard Studio
›	jQuery Upgrade	Edit ▾	nobody	search	App	Classic
›	Orphaned Scheduled Searches, Reports, and Alerts	Edit ▾	nobody	search	App	Dashboard Studio
›	Scheduled export is now available for Dashboard Studio	Edit ▾	nobody	search	Global	Dashboard Studio



Dashboards

Dashboards include searches, visualizations, and input controls that capture and present a

Latest Resources

Examples for Dashboard Studio
Browse examples of dashboards & visualizations. Visit Example Hub

Intro to Dashboard Studio
Learn how to build dashboards with Dashboard Studio. Learn More

5 Dashboards

i	Title	Owner	App	Sharing	Type
>	Integrity Check of Installed Files	nobody	search	App	Dashboard Studio
>	Job Details Dashboard	nobody	search	App	Dashboard Studio
>	jQuery Upgrade	nobody	search	App	Classic
>	Optimized Scheduled Searches, Reports, and Alerts	nobody	search	App	Dashboard Studio
>	Scheduled export is now available for Dashboard Studio	nobody	search	Global	Dashboard Studio

Create New Dashboard

Dashboard Title: SOC Threat Overview

soc_threat_overview

Edit ID

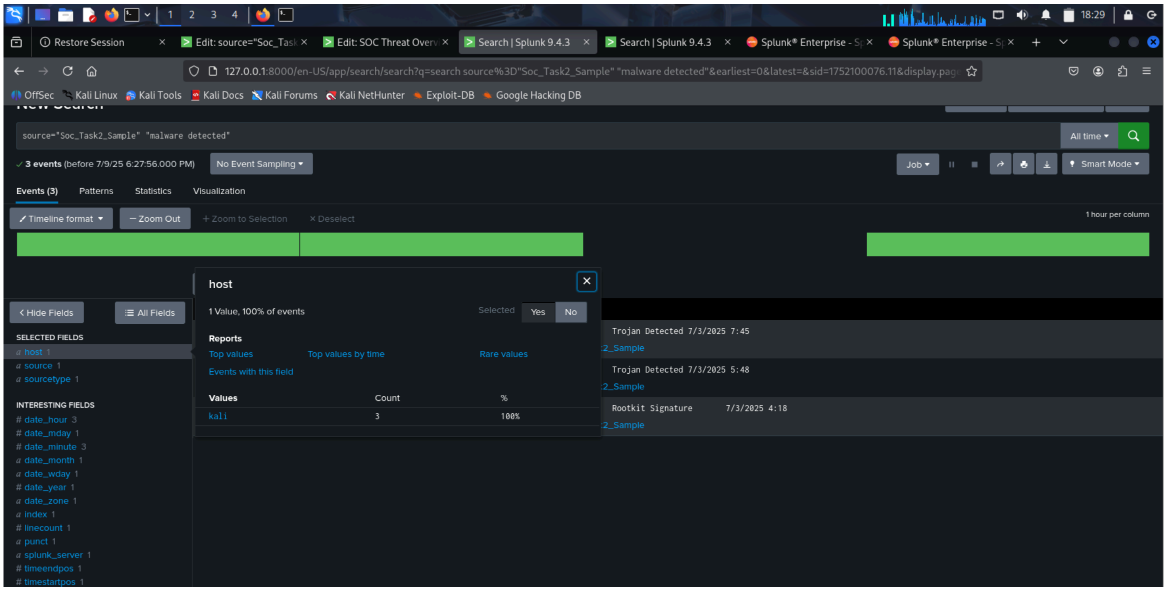
Description: Optional

Permissions: Private

How do you want to build your dashboard? What's this?

Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards



127.0.0.1:8000/en-US/app/search/search?q=search source%3D"Soc_Task2_Sample" "malware detected"&earliest=0&latest=&sid=1752100076.11&display.page

```
source="Soc_Task2_Sample" "malware detected"
```

✓ **3 events** (before 7/9/25 6:27:56.000 PM)

SELECTED FIELDS
- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS
- # date_hour 3
- # date_mday 1
- # date_minute 3
- a date_month 1
- a date_wday 1
- # date_year 1
- a date_zone 1
- a index 1
- # linecount 1
- a punct 1
- a splunk_server 1
- # timeendpos 1
- # timestartpos 1

host

1 Value, 100% of events

Selected: Yes [✓ No]

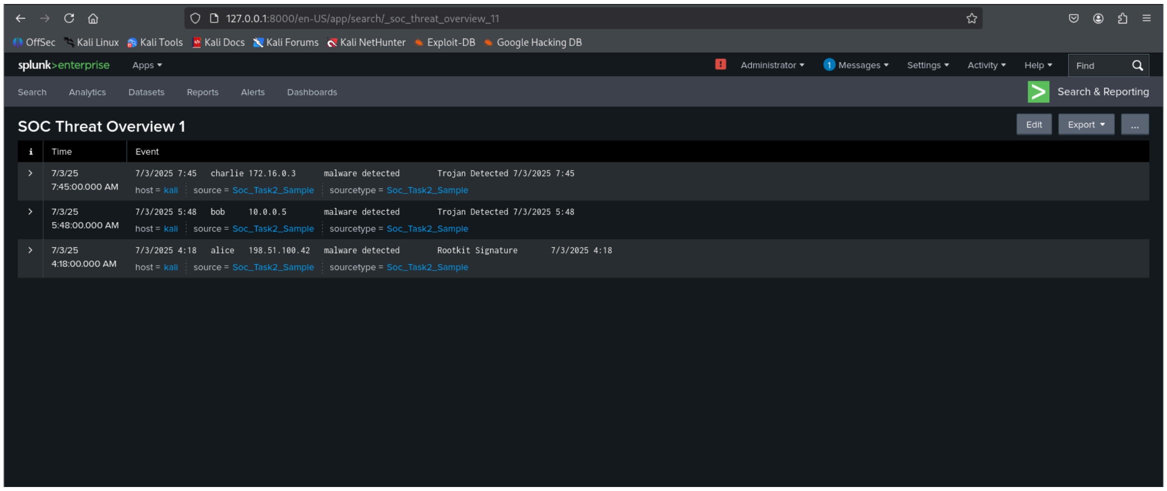
Reports

Top values · Top values by time · Rare values

Events with this field

Values	Count	%
kali	3	100%

```
Trojan Detected 7/3/2025 7:45
2_Sample
Trojan Detected 7/3/2025 5:48
2_Sample
Rootkit Signature      7/3/2025 4:18
2_Sample
```



SOC Threat Overview 1

i	Time	Event
>	7/3/25 7:45:00.000 AM	7/3/2025 7:45 charlie 172.16.0.3 malware detected Trojan Detected 7/3/2025 7:45 host = kali source = Soc_Task2_Sample sourcetype = Soc_Task2_Sample
>	7/3/25 5:48:00.000 AM	7/3/2025 5:48 bob 10.0.0.5 malware detected Trojan Detected 7/3/2025 5:48 host = kali source = Soc_Task2_Sample sourcetype = Soc_Task2_Sample
>	7/3/25 4:18:00.000 AM	7/3/2025 4:18 alice 198.51.100.42 malware detected Rootkit Signature 7/3/2025 4:18 host = kali source = Soc_Task2_Sample sourcetype = Soc_Task2_Sample

Purpose:
Dashboards like this help SOC analysts detect trends in user activity, identify frequent attackers or vulnerable systems, and present insights clearly to management.

SOC Playbook (Simulated)

A playbook is a step-by-step guide used by SOC teams to handle specific security incidents efficiently and consistently.

Simulated Malware Detection Playbook:

Step	Action	Description
1	Review Alert	Confirm malware alert is valid in Splunk logs
2	Isolate Affected Host	Remove infected host from the network
3	Investigate User Activity	Analyze behavior of user tied to infected machine
4	Run Malware Scan	Perform AV scan on affected host

5	Patch and Secure System	Ensure system updates and security patches applied
6	Report Incident	Notify stakeholders and update SOC incident logs

These structured steps help ensure that responses are quick, coordinated, and repeatable — which is vital in a real-world SOC environment.