Cyber Security Task 2

Report By: Vivek Yadav

Internship: Future Interns – Cyber Security

Internship Date: 02-07-2025

SECURITY ALERT MONITORING & INCIDENT RESPONSE

About the Task

This internship project introduced me to real-world SOC (Security Operations Center) practices. The primary objective was to simulate the daily tasks of a SOC Analyst, including security alert monitoring, threat analysis, incident response, and stakeholder communication.

The simulation helped develop core skills required in cybersecurity operations using industry-grade SIEM tools.

Tools Used

- **Splunk Free Trial** - SIEM platform used to ingest and analyze system logs.
- **Elastic Stack (ELK)** - Open-source SIEM platform used for visualizing and analyzing security event logs.
- **SOC_Task2_Sample_Logs** - Sample data set provided for simulation.
- **Google Docs** - For creating this report.

Task Summary

1. Set up and explored both **Splunk** and **Elastic Stack**.
2. Uploaded and analyzed sample logs in both tools.
3. Identified suspicious activity using filters and searches such as:
    - Malware detection
    - Failed login attempts

- Suspicious IP addresses
- Unusual connection attempts

4. Took screenshots of dashboards and key findings.
5. Categorized and prioritized alerts.
6. Created an incident response report outlining the threat timeline and impact.
7. Drafted communication notes for hypothetical incident reporting.

Alert Summary and Classification

#	Alert Type	Description	Severity	Tool Used
1	Malware Detected	Malware detected on host 192.168.1.23	High	Splunk
2	Failed Login Attempts	Multiple failed logins for user 'admin'	Medium	Splunk
3	Suspicious IP	Connection attempt from IP 203.0.113.77	Medium	ELK
4	Unusual User Activity	User logged in at unusual hours	Low	ELK
5	Repeated Auth Failures	Auth errors from internal subnet repeatedly	Medium	ELK

Incident Timeline (Sample)

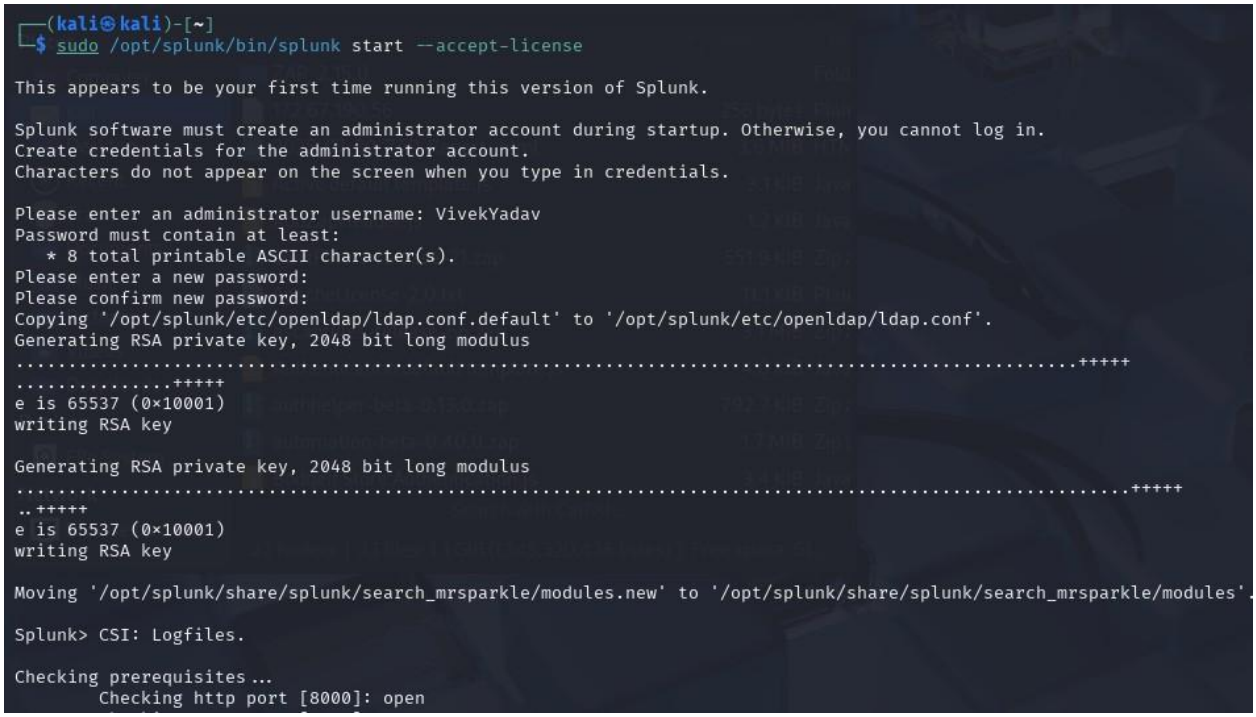
Time (UTC)	Event Description
08:00 AM, July 3	Multiple failed logins detected for user 'admin'
08:21 AM, July 3	Suspicious IP 203.0.113.77 attempted connection
08:30 AM, July 3	Malware signature matched in logs
09:00 AM, July 3	Alerts escalated for further investigation

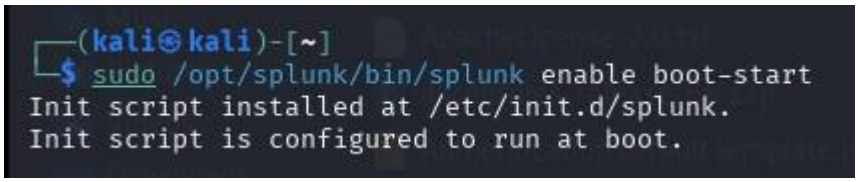
Incident Response Actions

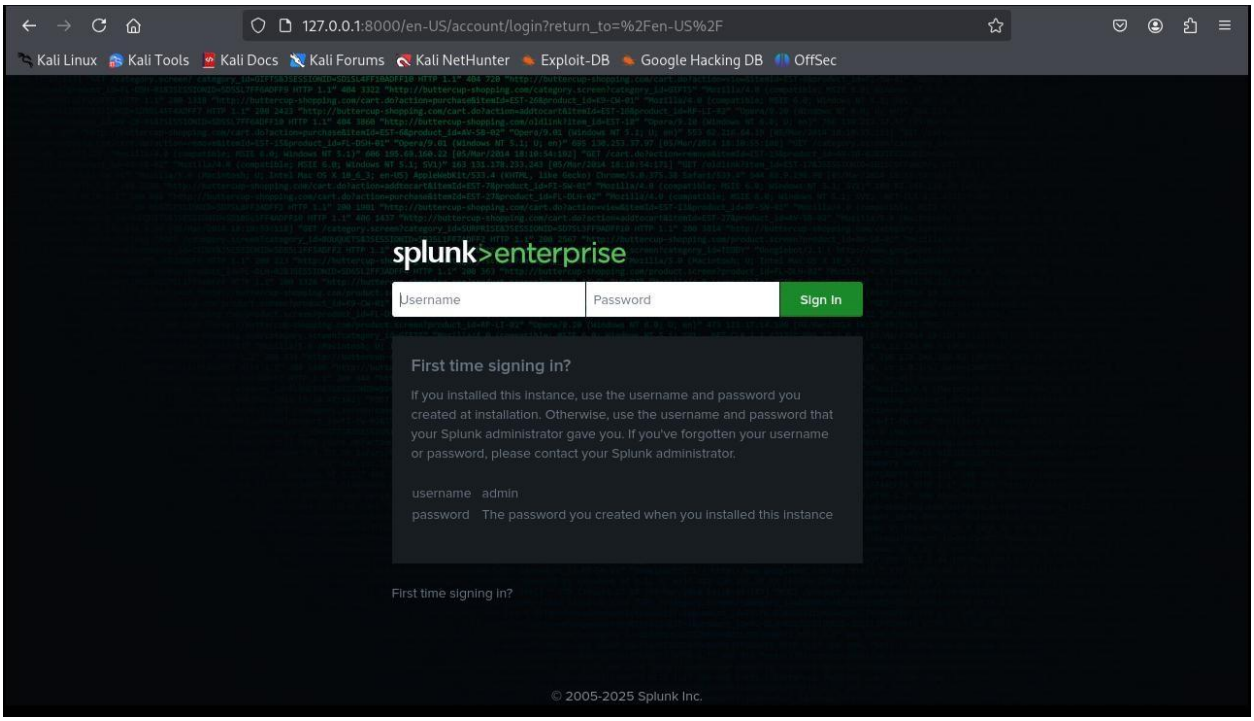
- Blocked suspicious external IP via firewall.

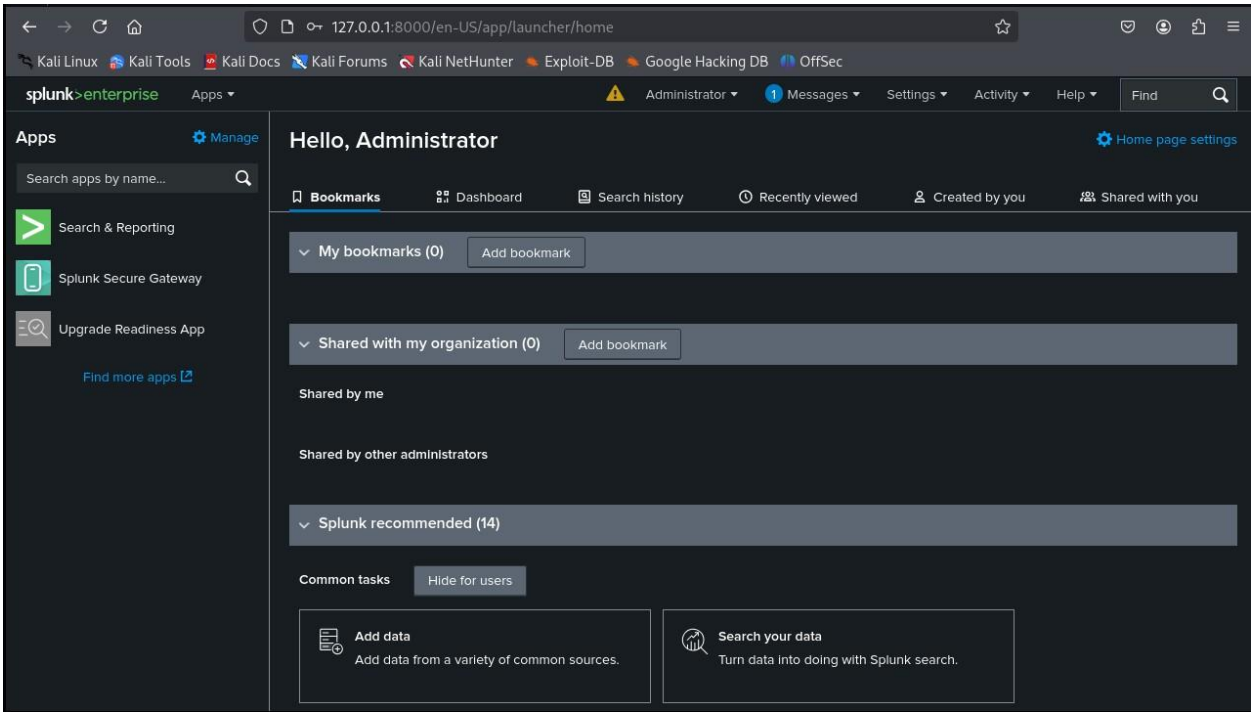
- Isolated affected host 192.168.1.23.
- Forced password reset for user 'admin'.
- Enabled 2FA for privileged accounts.
- Initiated malware scan across endpoint devices.

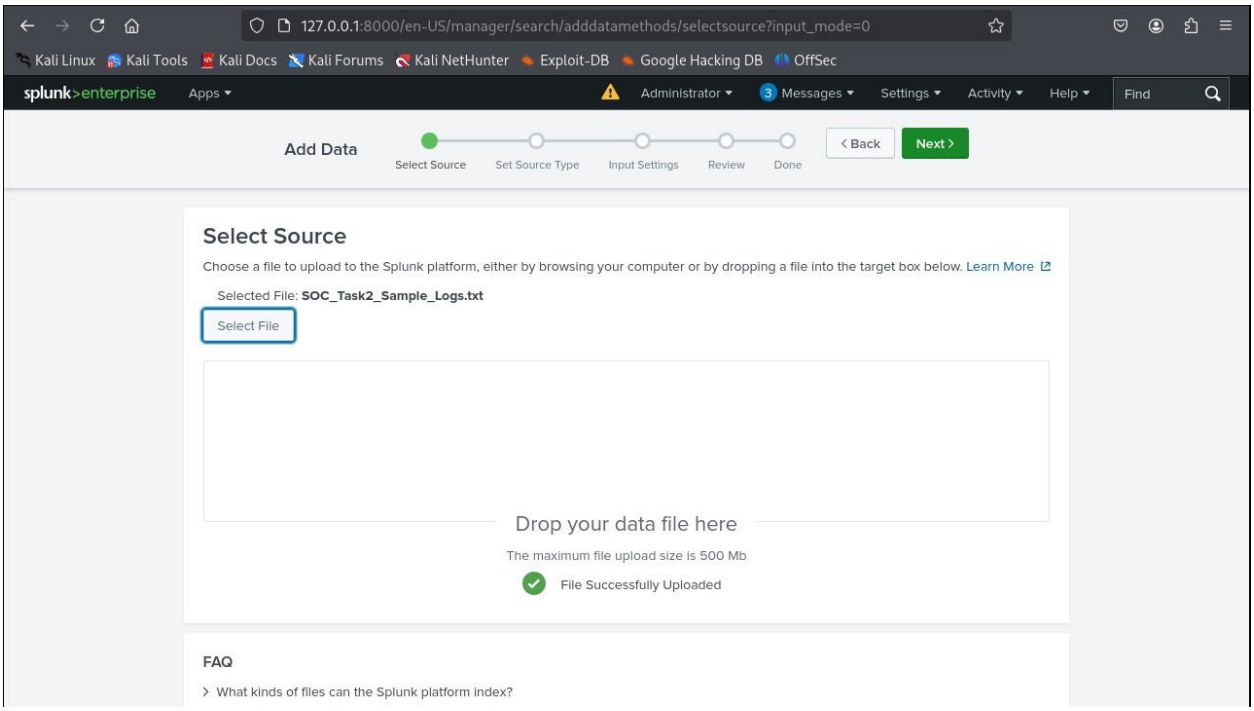
Dashboards & Visualization Splunk Tool

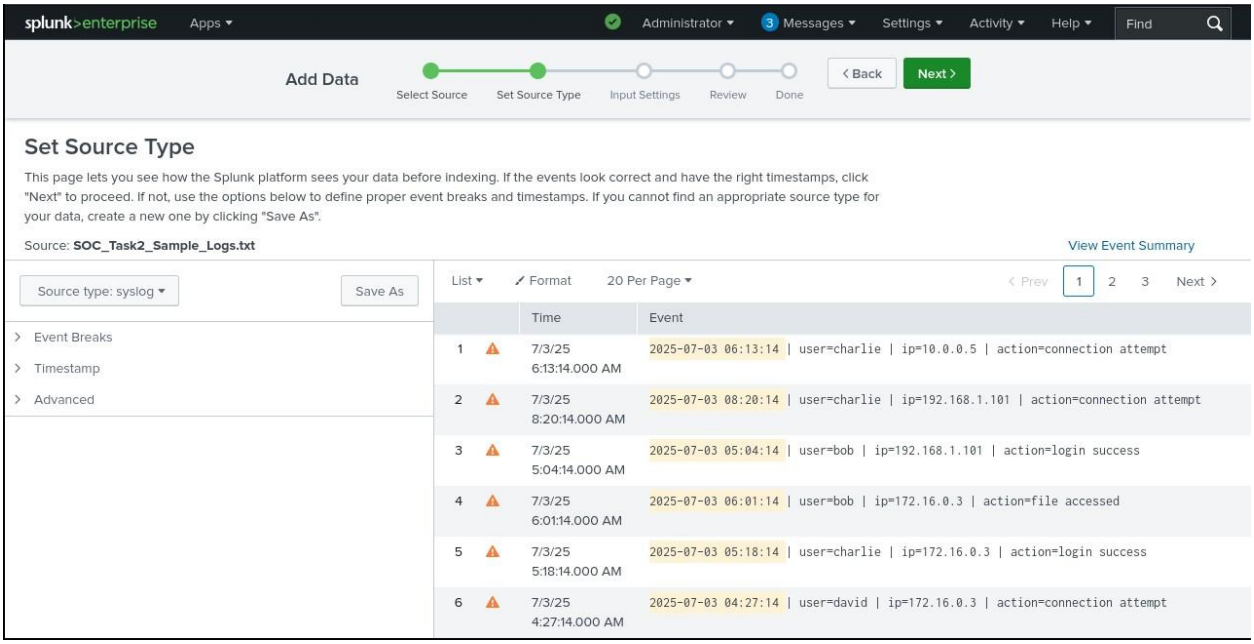


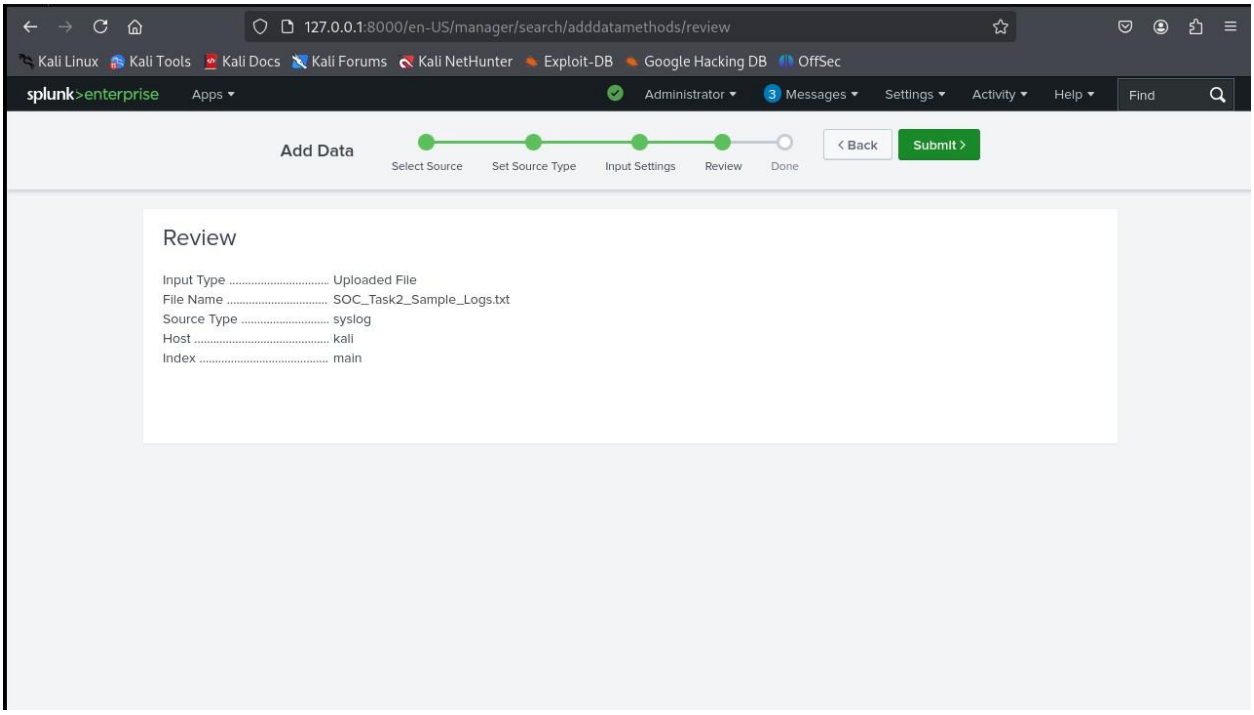


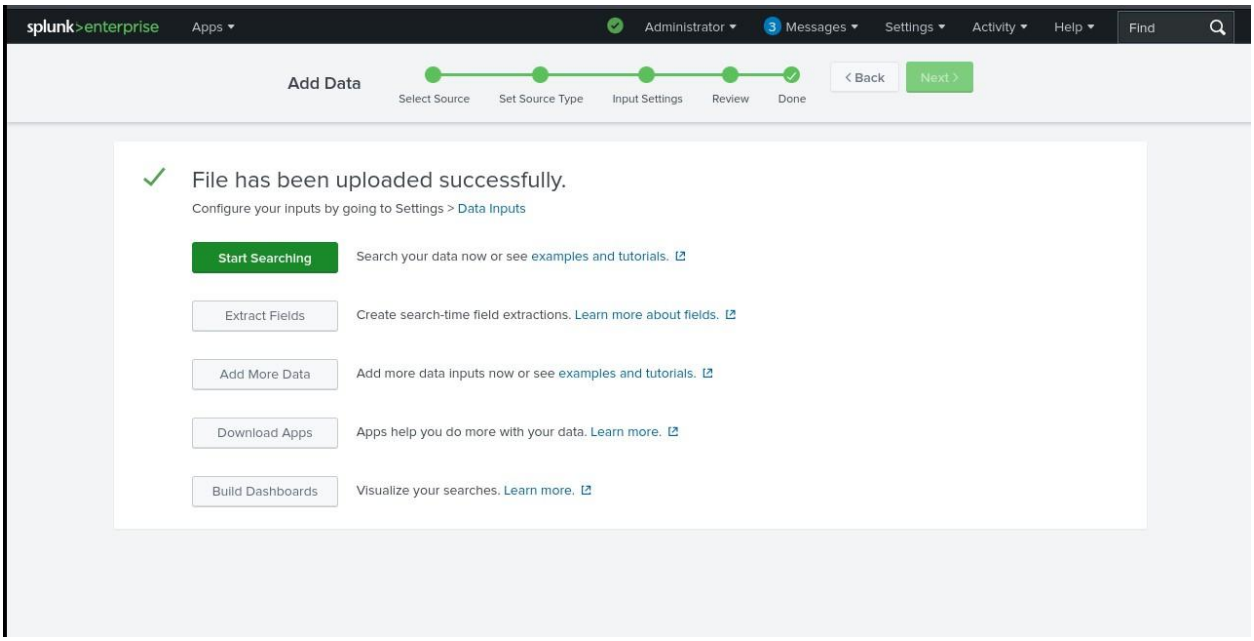

127.0.0.1:8000/en-US/account/login?return_to=%2Fen-US%2F
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
splunk>enterprise
Username
Password
Sign In
First time signing in?
If you installed this instance, use the username and password you created at installation. 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.

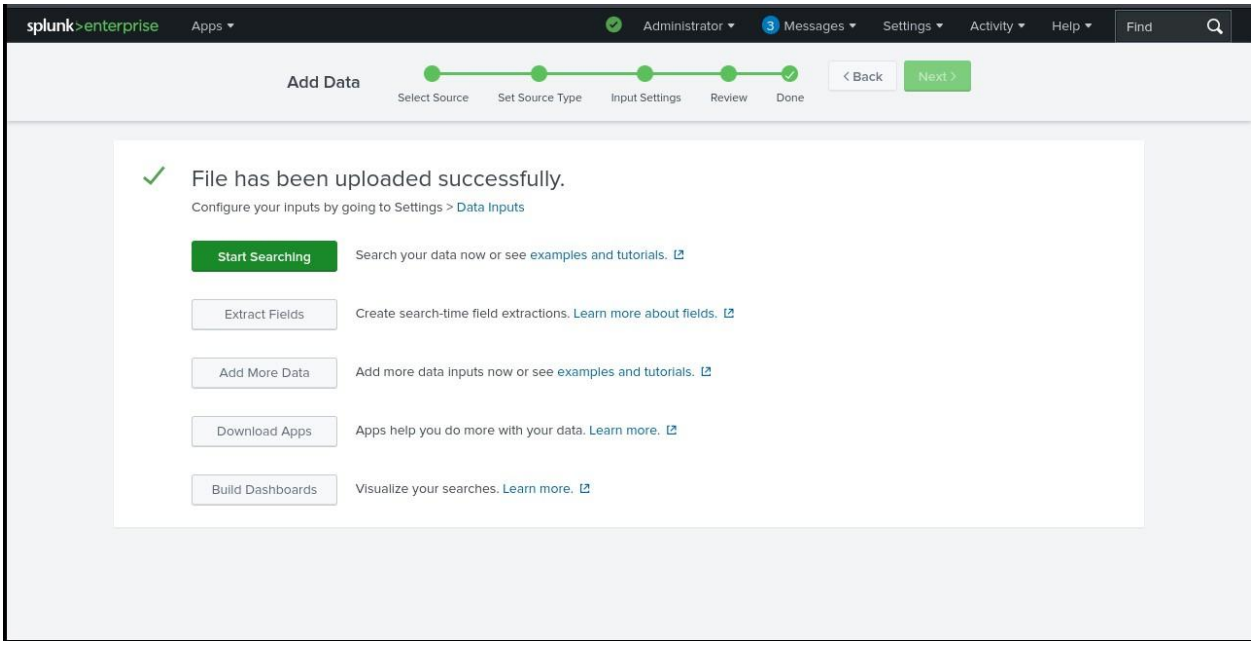

127.0.0.1:8000/en-US/app/launcher/home
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Manage
Search apps by name...
Search & Reporting
Splunk Secure Gateway
Upgrade Readiness App
Find more apps
Hello, Administrator
Home page settings
Bookmarks
Dashboard
Search history
Recently viewed
Created by you
Shared with you
My bookmarks (0)
Add bookmark
Shared with my organization (0)
Add bookmark
Shared by me
Shared by other administrators
Splunk recommended (14)
Common tasks
Hide for users
Add data
Add data from a variety of common sources.
Search your data
Turn data into doing with Splunk search.

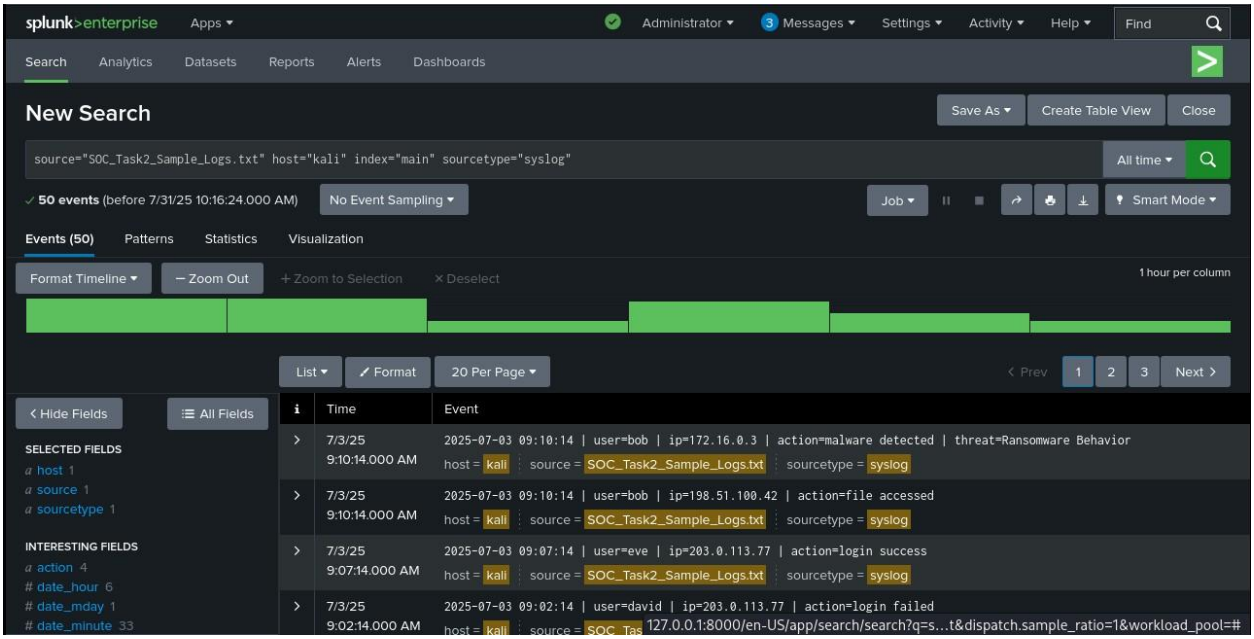

127.0.0.1:8000/en-US/manager/search/adddatamethods/selectsource?input_mode=0
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
splunk>enterprise
Apps
Administrator
3 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
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.txt
Select File
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?

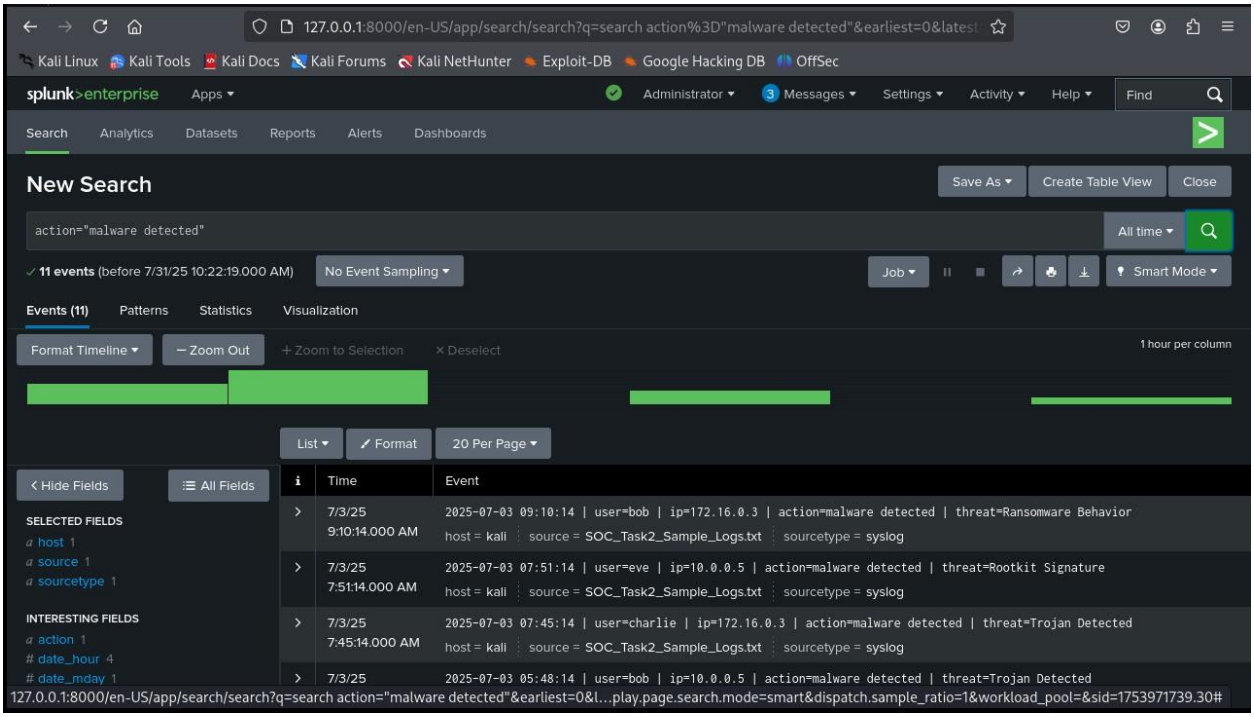

splunk>enterprise
Apps
Administrator
3 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
Set Source Type
This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".
Source: SOC_Task2_Sample_Logs.txt
View Event Summary
Source type: syslog
Save As
Event Breaks
Timestamp
Advanced
List
Format
20 Per Page
< Prev
1
2
3
Next >
Time
Event
1 7/3/25 6:13:14.000 AM 2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
2 7/3/25 8:20:14.000 AM 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
3 7/3/25 5:04:14.000 AM 2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success
4 7/3/25 6:01:14.000 AM 2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed
5 7/3/25 5:18:14.000 AM 2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
6 7/3/25 4:27:14.000 AM 2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt

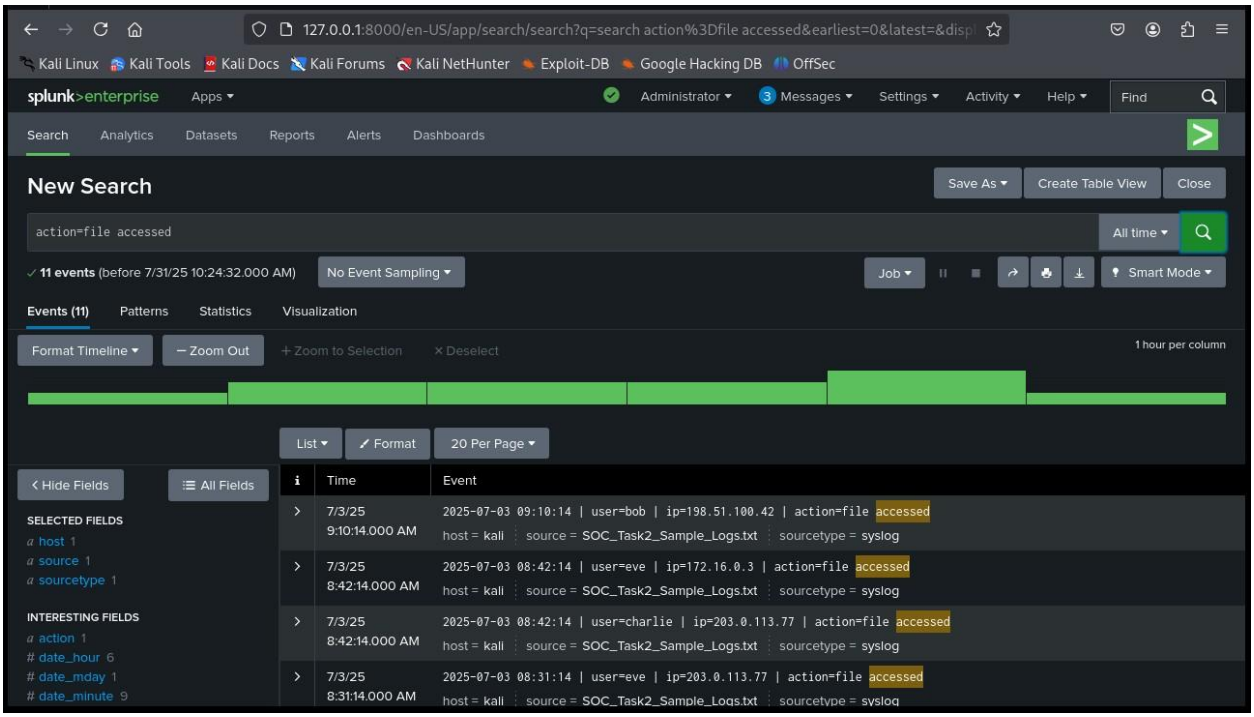

127.0.0.1:8000/en-US/manager/search/adddatamethods/review
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
splunk>enterprise
Apps
Administrator
3 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Submit >
Review
Input Type ..... Uploaded File
File Name ..... SOC_Task2_Sample_Logs.txt
Source Type ..... syslog
Host ..... kali
Index ..... main

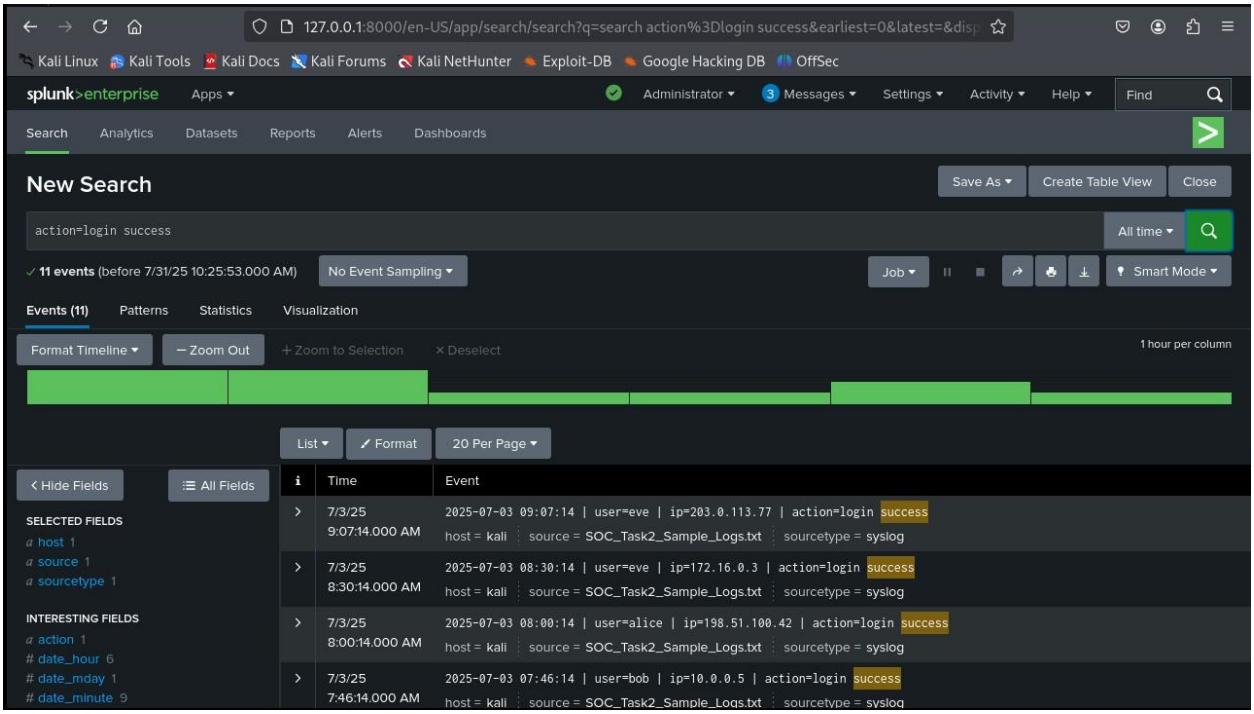

splunk>enterprise
Apps
Administrator
3 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
< Back
Next >
File has been uploaded successfully.
Configure your inputs by going to Settings > Data Inputs
Start Searching
Search your data now or see examples 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>enterprise
Apps
Administrator
3 Messages
Settings
Activity
Help
Find
Add Data
Select Source
Set Source Type
Input Settings
Review
Done
Back
Next
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>enterprise
Apps
Administrator
3 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
New Search
Save As
Create Table View
Close
source="SOC_Task2_Sample_Logs.txt" host="kali" index="main" sourcetype="syslog"
All time
50 events (before 7/31/25 10:16:24.000 AM)
No Event Sampling
Job
Smart Mode
Events (50)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
20 Per Page
Prev
1
2
3
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 4
date_hour 6
date_mday 1
date_minute 33
Time
Event
7/3/25 9:10:14.000 AM
2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
7/3/25 9:10:14.000 AM
2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
7/3/25 9:07:14.000 AM
2025-07-03 09:07:14 | user=eve | ip=203.0.113.77 | action=login success
host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
7/3/25 9:02:14.000 AM
2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed
host = kali source = SOC_Tas
127.0.0.1:8000/en-US/app/search/search?q=s...t&dispatch.sample_ratio=1&workload_pool=#


127.0.0.1:8000/en-US/app/search/search?q=search action%3D"malware detected"&earliest=0&latest
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
splunk>enterprise Apps Administrator 3 Messages Settings Activity Help Find
Search Analytics Datasets Reports Alerts Dashboards
New Search
Save As Create Table View Close
action="malware detected"
All time
11 events (before 7/31/25 10:22:19.000 AM) No Event Sampling Job Smart Mode
Events (11) Patterns Statistics Visualization
Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column
List Format 20 Per Page
Hide Fields All Fields
Time Event
7/3/25 9:10:14.000 AM 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior
host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
7/3/25 7:51:14.000 AM 2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature
host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
7/3/25 7:45:14.000 AM 2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected
host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
7/3/25 2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 1
date_hour 4
date_mday 1
127.0.0.1:8000/en-US/app/search/search?q=search action="malware detected"&earliest=0&l...play.page.search.mode=smart&dispatch.sample_ratio=1&workload_pool=&sid=1753971739.30#

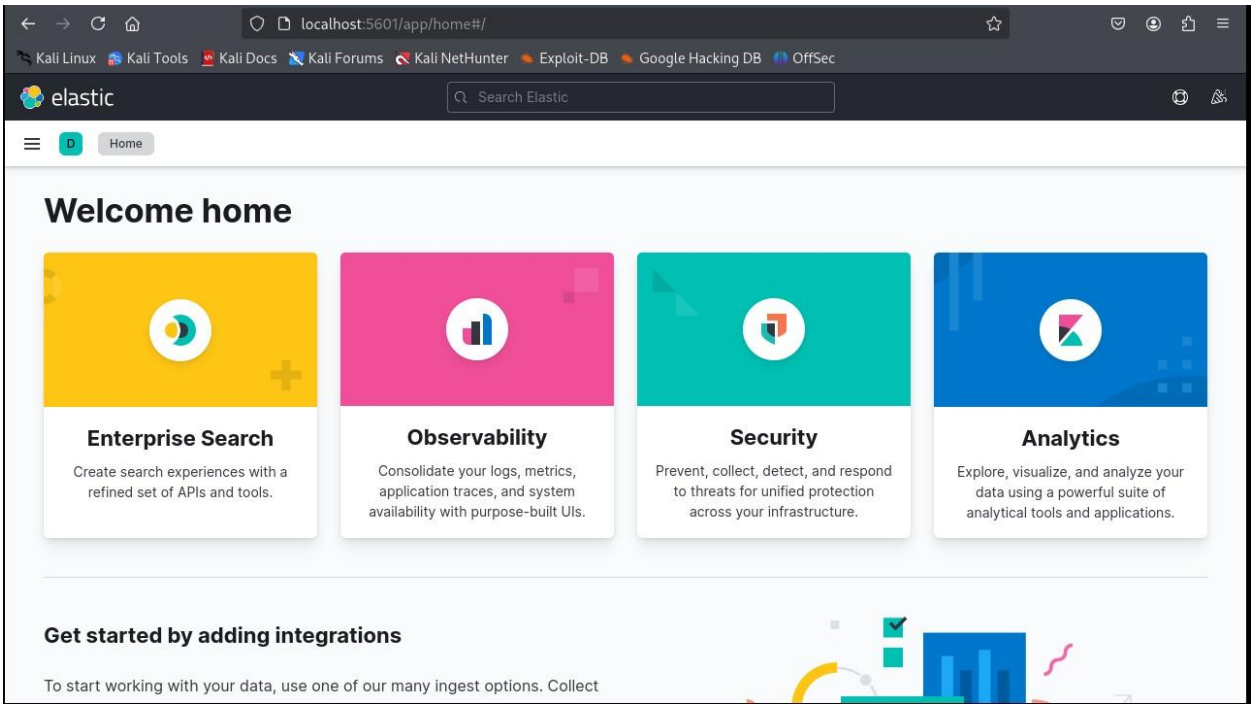

127.0.0.1:8000/en-US/app/search/search?q=search action%3Dfile accessed&earliest=0&latest=&disp
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
splunk>enterprise Apps Administrator 3 Messages Settings Activity Help Find
Search Analytics Datasets Reports Alerts Dashboards
New Search
Save As Create Table View Close
action=file accessed
All time
11 events (before 7/31/25 10:24:32.000 AM) No Event Sampling Job Smart Mode
Events (11) Patterns Statistics Visualization
Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column
List Format 20 Per Page
Hide Fields All Fields
Time Event
7/3/25 9:10:14.000 AM 2025-07-03 09:10:14 | user=bob | ip=198.51.100.42 | action=file accessed
host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
7/3/25 8:42:14.000 AM 2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accessed
host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
7/3/25 8:42:14.000 AM 2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accessed
host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
7/3/25 8:31:14.000 AM 2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accessed
host = kali source = SOC_Task2_Sample_Logs.txt sourcetype = syslog
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
a action 1
date_hour 6
date_mday 1
date_minute 9

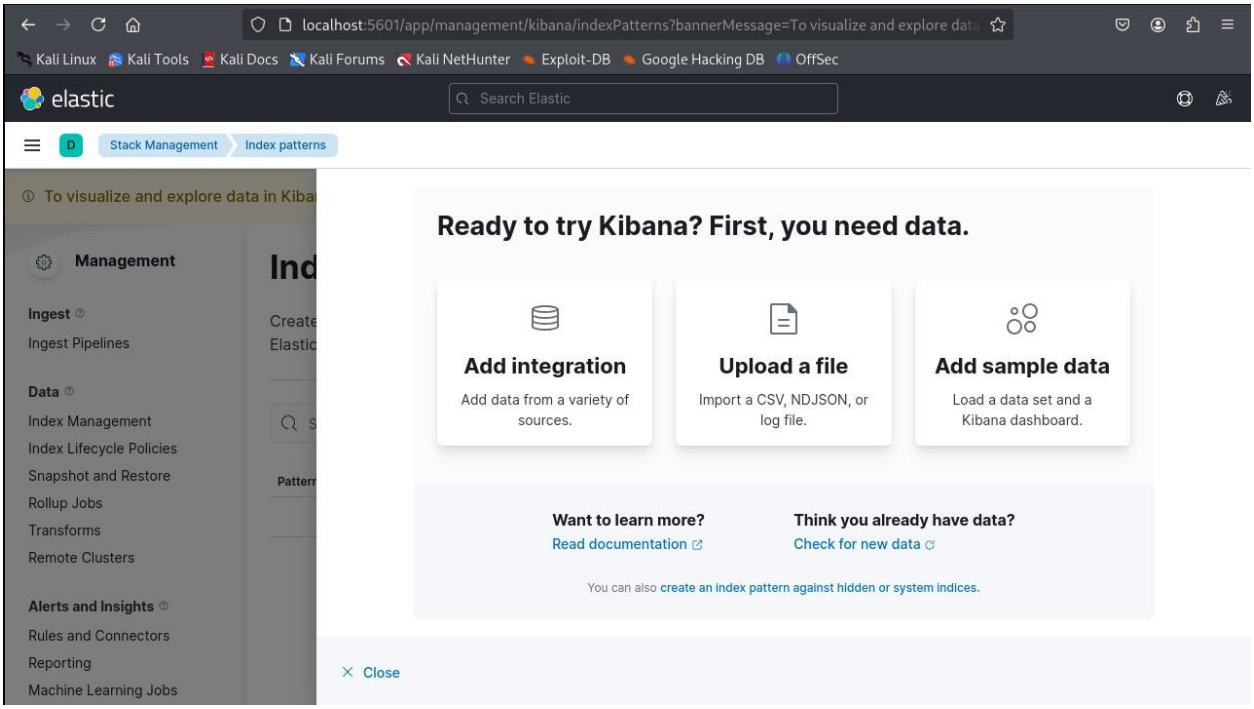


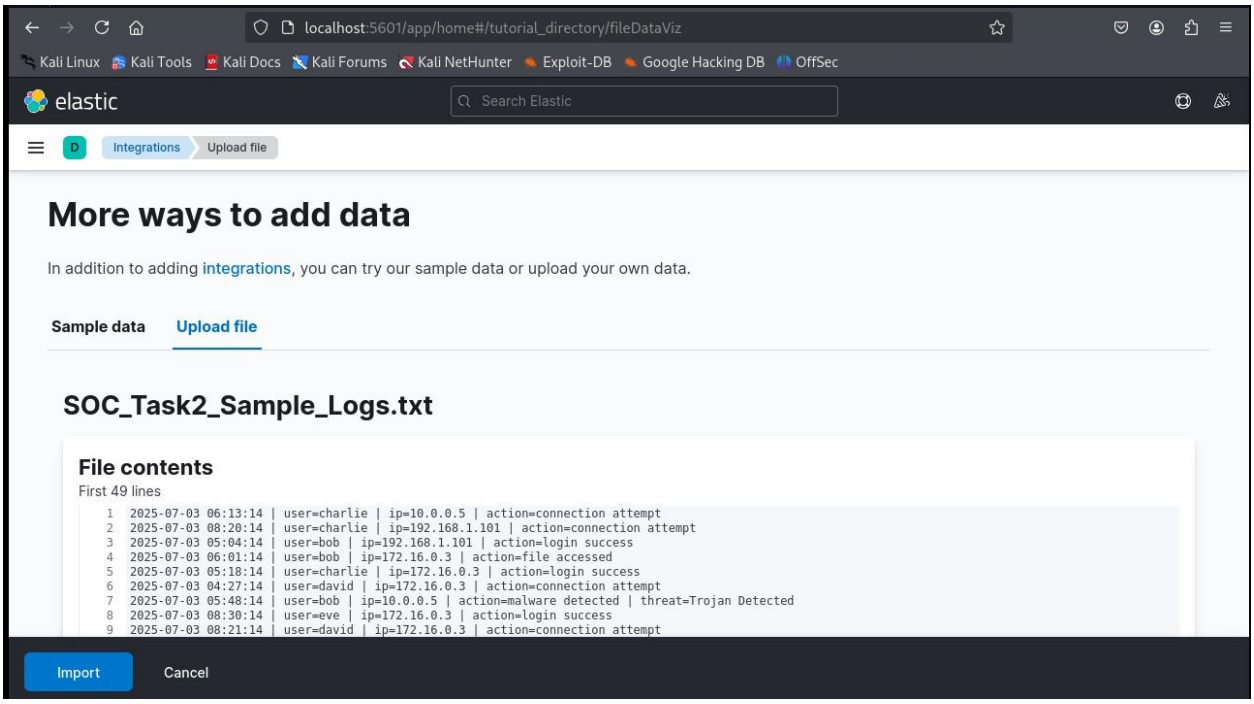
ELK Stack tools

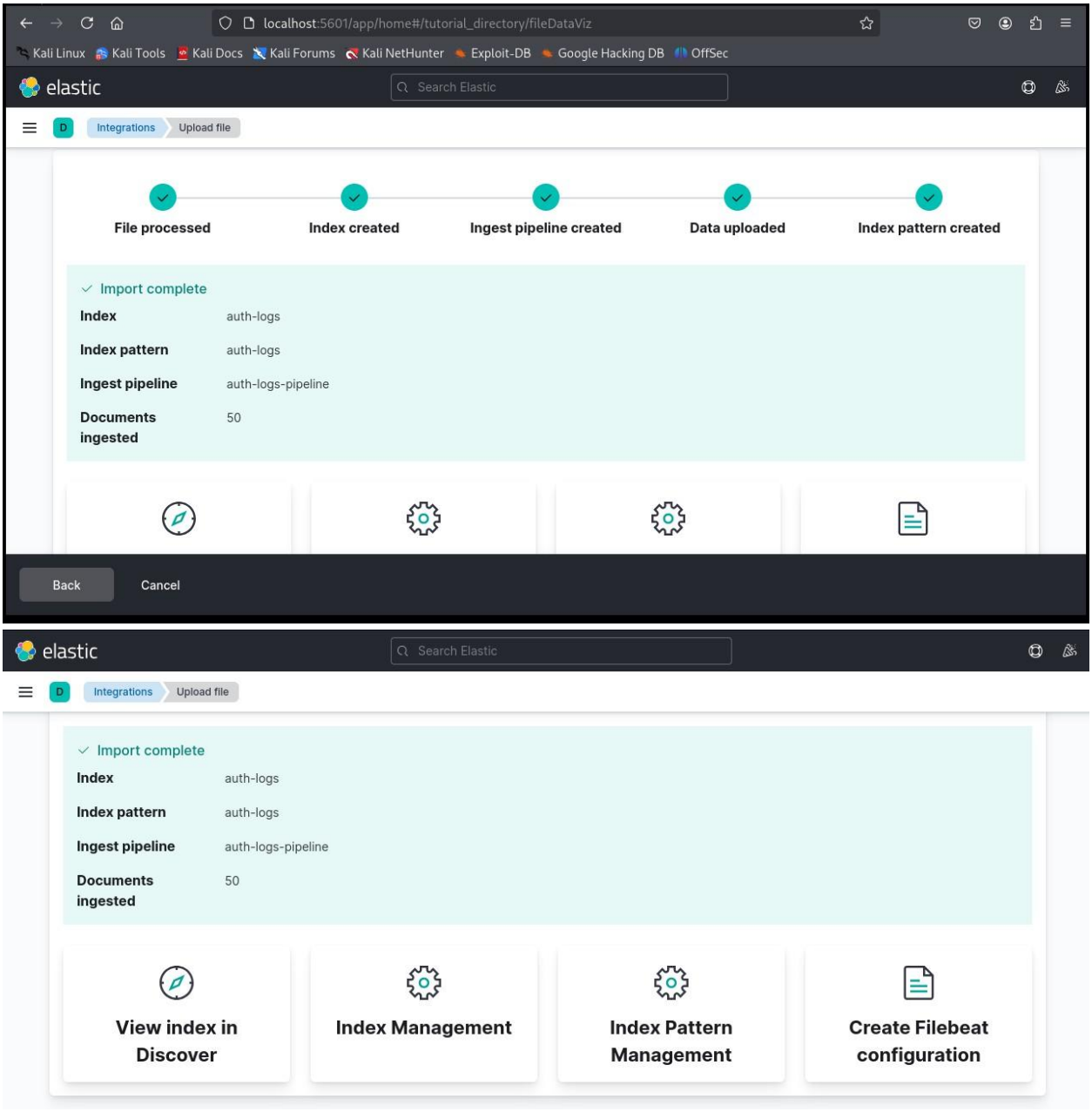
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable elasticsearch

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start elasticsearch

┌──(kali㉿kali)-[~]
└─$ sudo systemctl status elasticsearch
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: disabled)
     Active: active (running) since Thu 2025-07-31 13:18:18 EDT; 22s ago
 Invocation: 9d1854bdb70d413d8f527f52ab580887
       Docs: https://www.elastic.co
   Main PID: 10700 (java)
      Tasks: 78 (limit: 2199)
     Memory: 1G (peak: 1G)
        CPU: 44.428s
     CGroup: /system.slice/elasticsearch.service
             ├─10700 /usr/share/elasticsearch/jdk/bin/java -Xshare:auto -Des.networkaddress.cache.ttl=60 -Des.networkaddres
             └─10911 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller

Jul 31 13:18:01 kali systemd[1]: Starting elasticsearch.service - Elasticsearch...
Jul 31 13:18:05 kali systemd-entrypoint[10700]: Jul 31, 2025 1:18:05 PM sun.util.locale.provider.LocaleProviderAdapter <cli
Jul 31 13:18:05 kali systemd-entrypoint[10700]: WARNING: COMPAT locale provider will be removed in a future release
Jul 31 13:18:18 kali systemd[1]: Started elasticsearch.service - Elasticsearch.


┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable logstash

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start logstash

┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable kibana
Synchronizing state of kibana.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable kibana
```

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable logstash

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start logstash

┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable kibana
Synchronizing state of kibana.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable kibana

┌──(kali㉿kali)-[~]
└─$ sudo systemctl start kibana

┌──(kali㉿kali)-[~]
└─$ curl -X GET "localhost:9200"
{
  "name" : "kali",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "DKct8DfkTXKqF3UBoXMb4w",
  "version" : {
    "number" : "7.17.29",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "580aff1a0064ce4c93293aaab6fcc55e22c10d1c",
    "build_date" : "2025-06-19T01:37:57.847711500Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.3",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}

┌──(kali㉿kali)-[~]
└─$
```

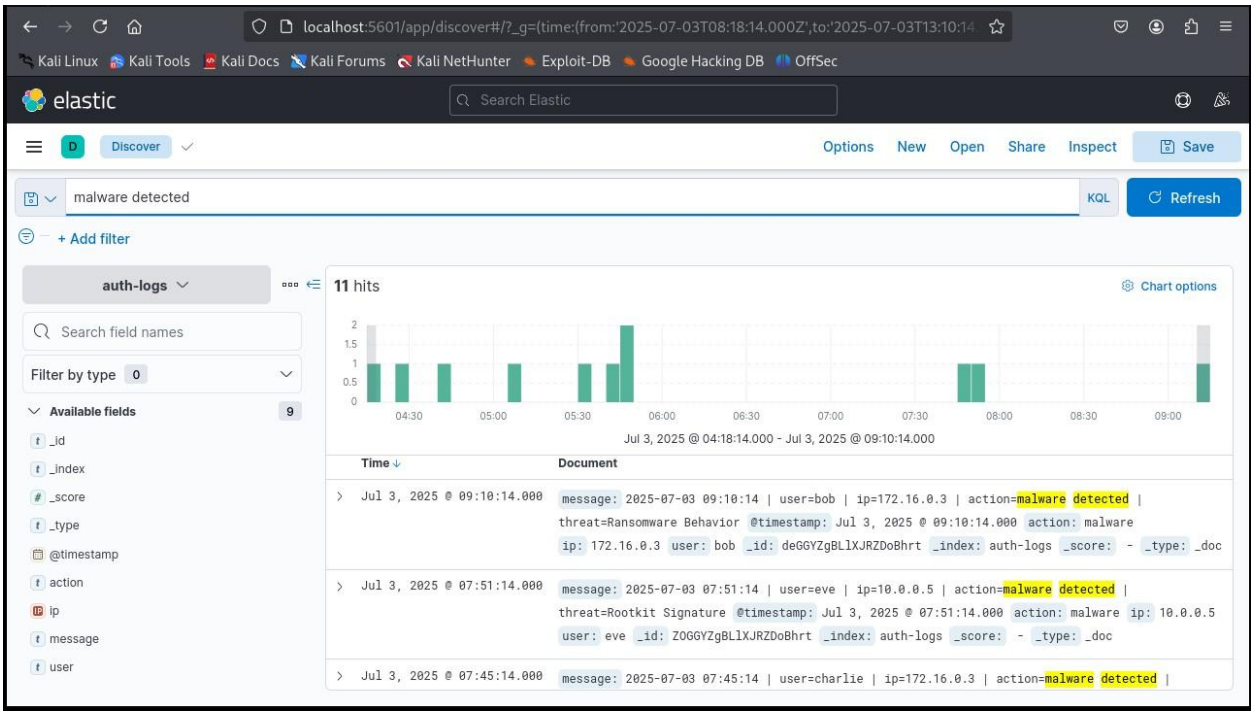


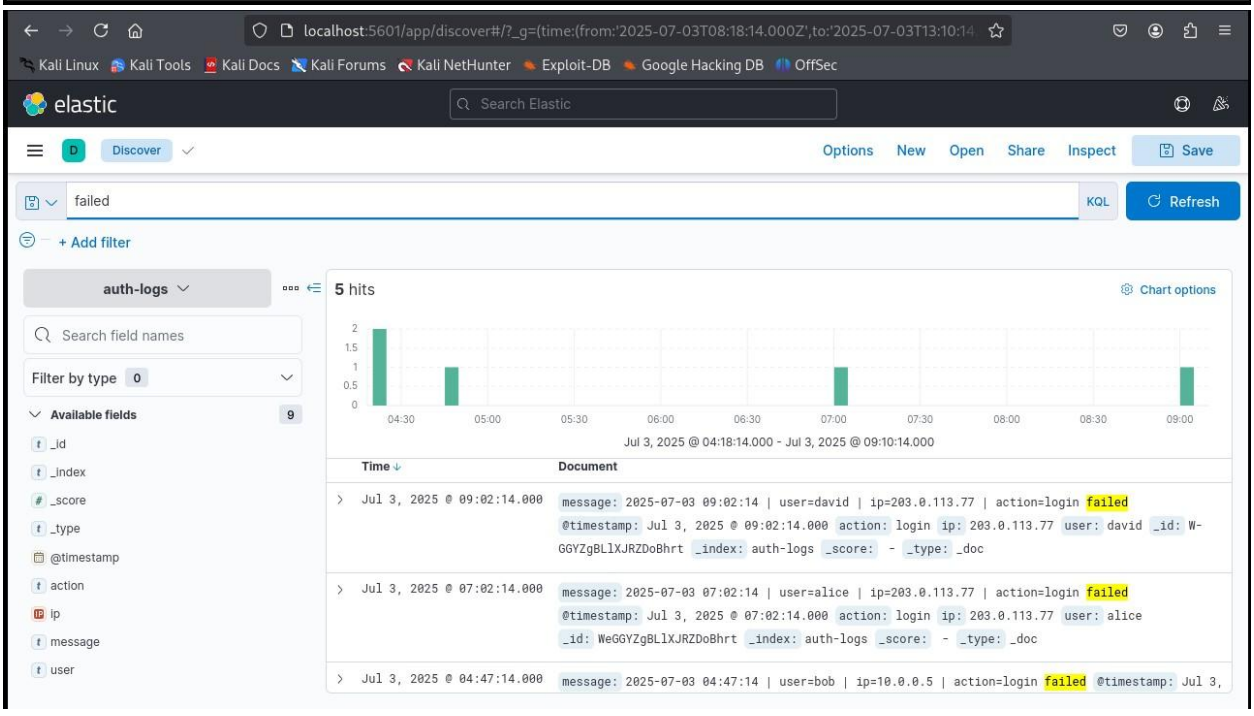

localhost:5601/app/management/kibana/indexPatterns?bannerMessage=To visualize and explore data
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
elastic
Search Elastic
Stack Management
Index patterns
To visualize and explore data in Kiba
Management
Ingest
Ingest Pipelines
Data
Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms
Remote Clusters
Alerts and Insights
Rules and Connectors
Reporting
Machine Learning Jobs
Ready to try Kibana? First, you need data.
Add integration
Add data from a variety of sources.
Upload a file
Import a CSV, NDJSON, or log file.
Add sample data
Load a data set and a Kibana dashboard.
Want to learn more?
Read documentation
Think you already have data?
Check for new data
You can also create an index pattern against hidden or system indices.
Close

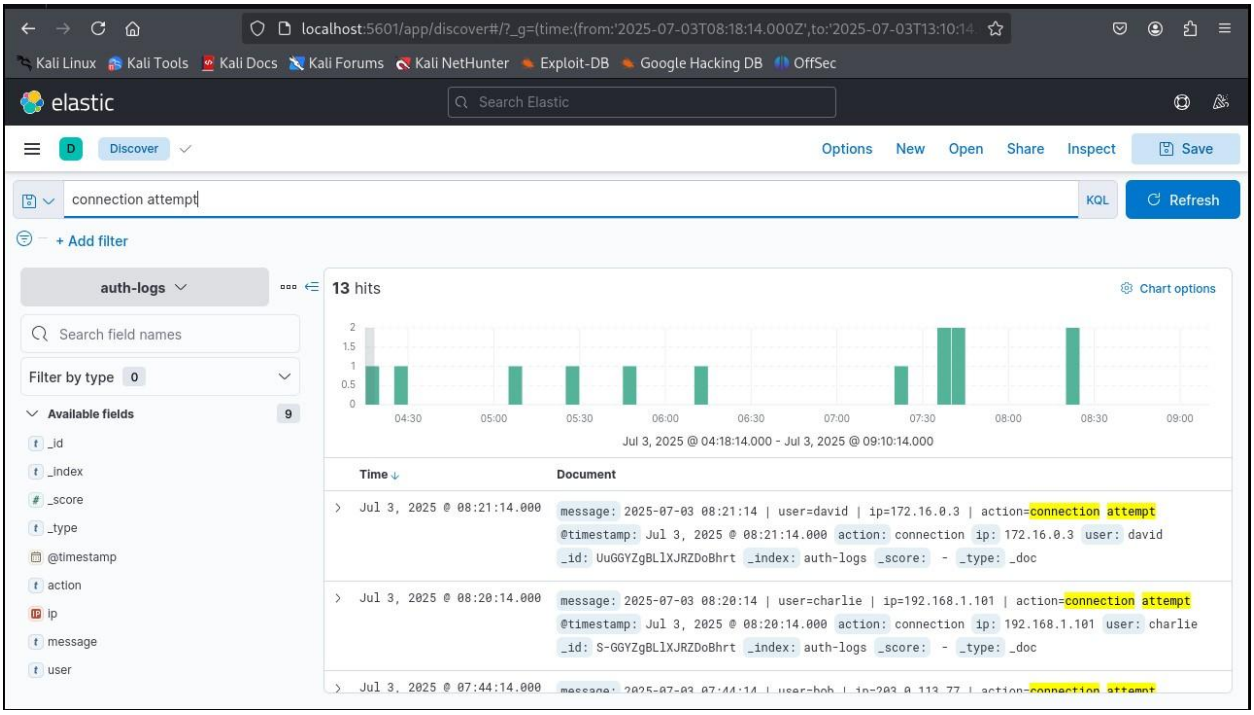

localhost:5601/app/home#/tutorial_directory/fileDataViz
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
elastic
Search Elastic
Integrations
Upload file
More ways to add data
In addition to adding integrations, you can try our sample data or upload your own data.
Sample data
Upload file
SOC_Task2_Sample_Logs.txt
File contents
First 49 lines
1 2025-07-03 06:13:14 | user=charlie | ip=10.0.0.5 | action=connection attempt
2 2025-07-03 08:20:14 | user=charlie | ip=192.168.1.101 | action=connection attempt
3 2025-07-03 05:04:14 | user=bob | ip=192.168.1.101 | action=login success
4 2025-07-03 06:01:14 | user=bob | ip=172.16.0.3 | action=file accessed
5 2025-07-03 05:18:14 | user=charlie | ip=172.16.0.3 | action=login success
6 2025-07-03 04:27:14 | user=david | ip=172.16.0.3 | action=connection attempt
7 2025-07-03 05:48:14 | user=bob | ip=10.0.0.5 | action=malware detected | threat=Trojan Detected
8 2025-07-03 08:30:14 | user=eve | ip=172.16.0.3 | action=login success
9 2025-07-03 08:21:14 | user=david | ip=172.16.0.3 | action=connection attempt
Import
Cancel


localhost:5601/app/home#/tutorial_directory/fileDataViz
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
elastic
Search Elastic
D
Integrations
Upload file
File processed
Index created
Ingest pipeline created
Data uploaded
Index pattern created
Import complete
Index
auth-logs
Index pattern
auth-logs
Ingest pipeline
auth-logs-pipeline
Documents ingested
50
Back
Cancel

elastic
Search Elastic
D
Integrations
Upload file
Import complete
Index
auth-logs
Index pattern
auth-logs
Ingest pipeline
auth-logs-pipeline
Documents ingested
50
View index in Discover
Index Management
Index Pattern Management
Create Filebeat configuration


localhost:5601/app/discover#/?_g=(time:(from:'2025-07-03T08:18:14.000Z',to:'2025-07-03T13:10:14
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
elastic
Search Elastic
Discover
Options New Open Share Inspect Save
malware detected
KQL
Refresh
+ Add filter
auth-logs
11 hits
Chart options
Search field names
Filter by type 0
Available fields 9
_id
_index
_score
_type
@timestamp
action
ip
message
user
Jul 3, 2025 @ 04:18:14.000 - Jul 3, 2025 @ 09:10:14.000
Time
Document
Jul 3, 2025 @ 09:10:14.000
message: 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior @timestamp: Jul 3, 2025 @ 09:10:14.000 action: malware ip: 172.16.0.3 user: bob _id: deGGYZgBLlXJRZDoBhrt _index: auth-logs _score: - _type: _doc
Jul 3, 2025 @ 07:51:14.000
message: 2025-07-03 07:51:14 | user=eve | ip=10.0.0.5 | action=malware detected | threat=Rootkit Signature @timestamp: Jul 3, 2025 @ 07:51:14.000 action: malware ip: 10.0.0.5 user: eve _id: ZOGGYZgBLlXJRZDoBhrt _index: auth-logs _score: - _type: _doc
Jul 3, 2025 @ 07:45:14.000
message: 2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected |


localhost:5601/app/discover#/?_g=(time:(from:'2025-07-03T08:18:14.000Z',to:'2025-07-03T13:10:14
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
elastic
Search Elastic
Discover
Options New Open Share Inspect Save
failed
KQL
Refresh
+ Add filter
auth-logs
5 hits
Chart options
Search field names
Filter by type 0
Available fields 9
_id
_index
_score
_type
@timestamp
action
ip
message
user
Jul 3, 2025 @ 04:18:14.000 - Jul 3, 2025 @ 09:10:14.000
Time
Document
Jul 3, 2025 @ 09:02:14.000
message: 2025-07-03 09:02:14 | user=david | ip=203.0.113.77 | action=login failed @timestamp: Jul 3, 2025 @ 09:02:14.000 action: login ip: 203.0.113.77 user: david _id: W-GGYZgBLlXJRZDoBhrt _index: auth-logs _score: - _type: _doc
Jul 3, 2025 @ 07:02:14.000
message: 2025-07-03 07:02:14 | user=alice | ip=203.0.113.77 | action=login failed @timestamp: Jul 3, 2025 @ 07:02:14.000 action: login ip: 203.0.113.77 user: alice _id: WeGGYZgBLlXJRZDoBhrt _index: auth-logs _score: - _type: _doc
Jul 3, 2025 @ 04:47:14.000
message: 2025-07-03 04:47:14 | user=bob | ip=10.0.0.5 | action=login failed @timestamp: Jul 3,



Sample Email to Future Interns

Subject: Security Incident Notification - Malware and Unauthorized Access

To Future Interns,

We have identified a security incident involving malware detection and multiple unauthorized access attempts. The issue has been contained and remediation is underway. A full report is attached for your review.

Regards,
Vivek Yadav
Cybersecurity Intern

Final Notes

This task helped me build practical understanding of how SOC teams operate, investigate incidents, and coordinate response. I gained exposure to SIEM tools and learned how to convert logs into actionable intelligence.