

SSH Log Analysis using Splunk Project

By Gaurav Ghandat

Project Overview

This project focuses on analyzing **SSH authentication logs** using **Splunk** to detect suspicious activities such as brute-force attacks, failed login attempts, unauthorized connections, and successful logins from unknown sources.

The project demonstrates **real-world SOC analyst skills**, including log ingestion, searching, visualization, dashboard creation, and alert configuration.

Objective

The primary goals of this project are to analyze SSH logs to detect:

-  **Successful SSH logins** (who connected and from where)
-  **Failed login attempts** (possible brute-force or password spraying)
-  **Multiple failed authentication attempts** (brute-force indicators)
-  **Connections without authentication** (scanning or incomplete sessions)

By completing this project, you will learn how to:

- Ingest SSH logs into Splunk
 - Write SPL queries for log analysis
 - Build dashboards and visualizations
 - Configure alerts for suspicious behavior
-

Lab Setup & Prerequisites

Prerequisites

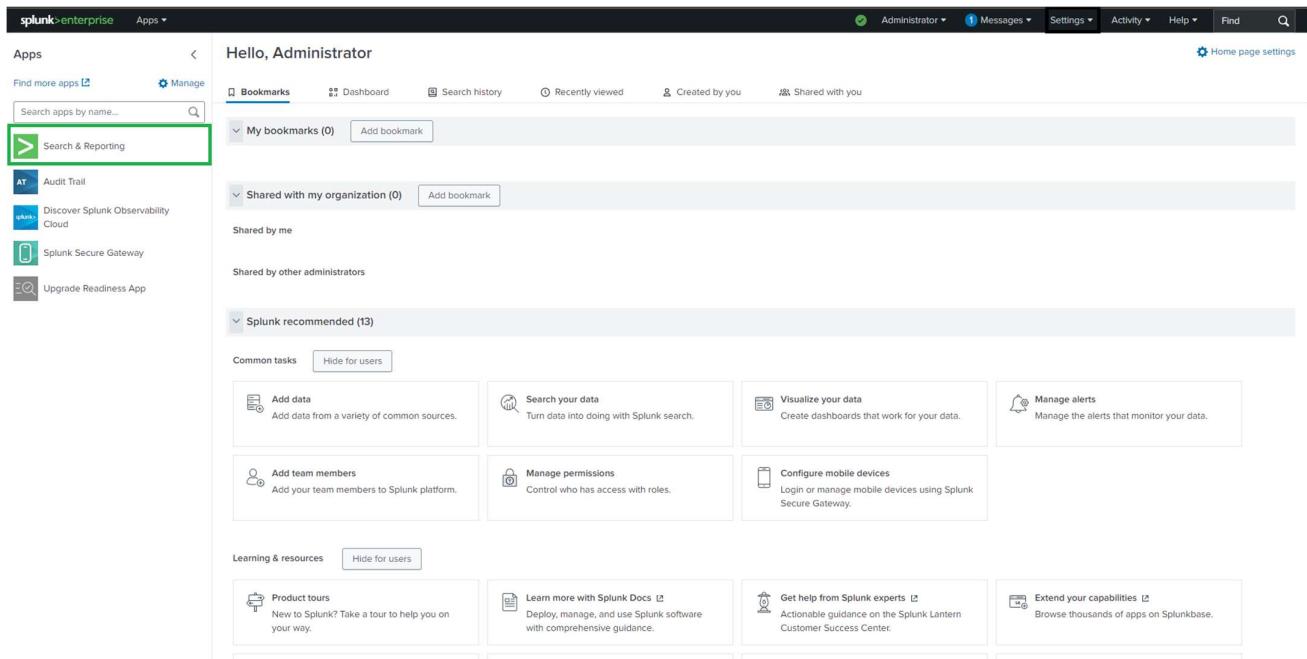
- Splunk Enterprise or Splunk Free installed
- Basic understanding of SPL (Search Processing Language)

Files Required

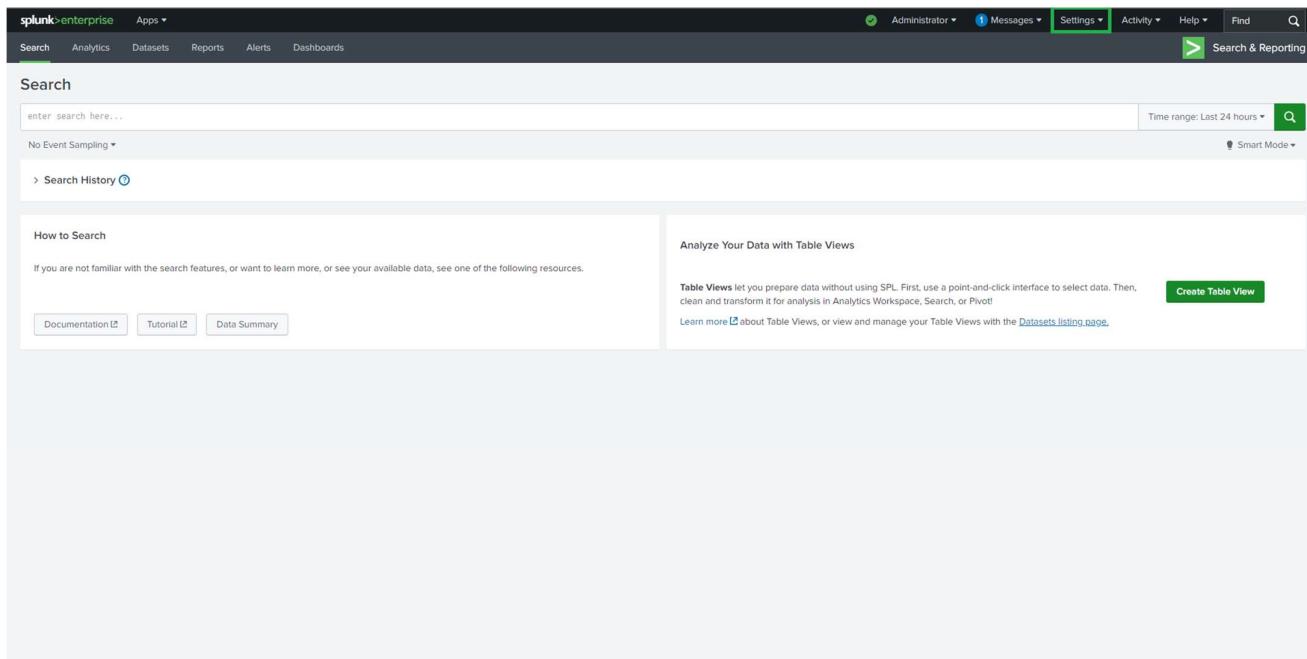
- ssh_log.json (SSH authentication logs)
-

Preparation Steps

1. Log in to your **Splunk Web Interface**
2. Navigate to: Apps → Search & Reporting



The screenshot shows the Splunk Web Interface with the 'Search & Reporting' app bookmarked. The top navigation bar includes links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. The main content area is titled 'Hello, Administrator' and displays a 'Bookmarks' section with a list of bookmarked items. One item, 'Search & Reporting', is highlighted with a green border. Other bookmarked items include 'Audit Trail', 'Discover Splunk Observability Cloud', 'Splunk Secure Gateway', and 'Upgrade Readiness App'. Below the bookmarks, there are sections for 'Shared with my organization', 'Shared by me', and 'Shared by other administrators'. A 'Splunk recommended (13)' section is also present, featuring various common tasks like 'Add data', 'Search your data', 'Visualize your data', 'Manage alerts', 'Add team members', 'Manage permissions', 'Configure mobile devices', 'Product tours', 'Learn more with Splunk Docs', 'Get help from Splunk experts', and 'Extend your capabilities'.



The screenshot shows the Splunk Web Interface with the 'Search & Reporting' app open. The top navigation bar includes links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. The main content area is titled 'Search' and features a search bar with placeholder text 'enter search here...'. Below the search bar are buttons for 'Time range: Last 24 hours', 'Smart Mode', and a magnifying glass icon. On the left, there's a 'How to Search' section with links for 'Documentation', 'Tutorial', and 'Data Summary'. On the right, there's a 'Analyze Your Data with Table Views' section with a 'Create Table View' button. The bottom of the page has a footer with links for 'Documentation', 'Tutorial', 'Data Summary', 'Feedback', and 'Help'.

3. Click: Add Data → Upload

The screenshot shows the Splunk Enterprise search interface. At the top, there's a navigation bar with 'splunk enterprise' and various links like 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. On the left, there's a 'Search' section with a search bar and some links for 'Documentation', 'Tutorial', and 'Data Summary'. In the center, there's a 'How to Search' section and a 'Analyze Your Data with Table Views' section. On the right, there's a sidebar with a 'Monitoring Console' icon and a search bar. The main content area has a green box highlighting the 'Add Data' button.

The screenshot shows the 'Add Data' page. At the top, there's a header with 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a 'Find' bar. Below it, there's a search bar and a sidebar with categories like 'KNOWLEDGE', 'DATA', 'SYSTEM', 'DISTRIBUTED ENVIRONMENT', 'USERS AND AUTHENTICATION', and 'FEDERATION'. The main content area has a heading 'What data do you want to send to the Splunk platform?'. It shows four data source categories: 'Cloud computing' (10 sources), 'Networking' (2 sources), 'Operating System' (1 source), and 'Security' (3 sources). Below this, there's a section titled 'Or get data in with the following methods' with three options: 'Upload' (highlighted with a green box), 'Monitor', and 'Forward'.

4. Upload the file: ssh_log.json

The screenshot shows the Splunk Add Data interface at the 'Select Source' step. The top navigation bar includes 'splunk enterprise', 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the navigation is a progress bar with five steps: 'Select Source' (green dot), 'Set Source Type' (white circle), 'Input Settings' (white circle), 'Review' (white circle), and 'Done' (white circle). The 'Next >' button is highlighted in green. The main area is titled 'Select Source' with the sub-instruction 'Choose a file to upload to the Splunk platform, either by browsing your computer or by dropping a file into the target box below.' A message 'Selected File: No file selected' is displayed above a 'Select File' button. A large input field labeled 'Drop your data file here' is present, with the note 'The maximum file upload size is 500 Mb'. Below this is a 'FAQ' section with links to various help topics. In the foreground, a Windows 'Open' file dialog is overlaid on the interface. It shows a file named 'ssh_logs' located in the 'Downloads' folder. The 'Open' button in the dialog is highlighted with a green box. The file dialog has standard Windows UI elements like 'File name:', 'All Files', 'Open', and 'Cancel'.

127.0.0.1:8000/en-USmanager/search/adddatamethods/selectsource?input_mode=0#

The screenshot shows the 'Select Source' step of the 'Add Data' wizard. The progress bar at the top is at the second step, 'Select Source'. The main area shows a file named 'ssh_logs.json' has been selected and uploaded successfully. A message says 'File Successfully Uploaded'. Below this, there's an FAQ section with links to common questions about file types and sources.

5. Set:

- **Source type: _json**
- **Index: ssh_logs (create a new index)**

The screenshot shows the 'Set Source Type' page. It displays a table of events from the 'ssh_logs.json' file. The table includes columns for timestamp, authentication attempts, success status, connection state, event type, history, and various ID and byte counts. The first few rows show successful logins and failed attempts.

	_time	auth_attempts	auth_success	conn_state	event_type	history	id.orig_h	id.orig_p	id.resp_h	id.resp_p	missed_bytes	orig_ip_bytes	orig_pkts
1	4/24/25 3:50:09.508 PM	1	true	SF	Successful SSH Login	ShADadF	10.0.0.43	58221	10.0.1.6	22	0	3234	49
2	4/24/25 3:50:09.508 PM	1	false	SF	Failed SSH Login	ShADadF	10.0.0.36	26957	10.0.1.12	22	0	1197	21
3	4/24/25 3:50:09.508 PM	8	false	SF	Multiple Failed Authentication Attempts	ShADadF	10.0.0.44	42848	10.0.1.10	22	0	702	13
4	4/24/25 3:50:09.508 PM	1	false	SF	Failed SSH Login	ShADadF	10.0.0.20	47789	10.0.1.2	22	0	1168	16
5	4/24/25 3:50:09.508 PM	1	true	SF	Successful SSH Login	ShADadF	10.0.0.37	30192	10.0.1.1	22	0	876	12
6	4/24/25 3:50:09.508 PM	6	false	SF	Multiple Failed Authentication Attempts	ShADadF	10.0.0.42	32500	10.0.1.10	22	0	1848	28
7	4/24/25 3:50:09.508 PM	0	null	SF	Connection Without Authentication	ShADadF	10.0.0.10	47980	10.0.1.5	22	0	3150	42
8	4/24/25 3:50:09.508 PM	1	false	SF	Failed SSH Login	ShADadF	10.0.0.21	34955	10.0.1.12	22	0	2350	50
9	4/24/25 3:50:09.508 PM	4	false	SF	Multiple Failed Authentication Attempts	ShADadF	10.0.0.21	20693	10.0.1.1	22	0	2262	29

splunk enterprise Apps ▾

Administrator ▾ i Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Add Data

Select Source Set Source Type Input Settings Review Done < Back Review >

Input Settings

Optional set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More ⓘ

Constant value
 Regular expression on path
 Segment in path

Host field value: LAPTOP-EHJ3QFJI

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More ⓘ

Index: Default ▾ **Create a new index**

FAQ

> How do Indexes work?
> How do I know when to create or use multiple indexes?

splunk enterprise Apps ▾

Administrator ▾ i Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

New Index

General Settings

Index Name:

Set index name (e.g., INDEX_NAME). Search using index:INDEX_NAME.

Index Data Type: Events Metrics

The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/its).

Cold Path: optional
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional
Thawed/restricted db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable Disable

Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB ▾

Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto GB ▾

Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path: optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App:

Storage Optimization

Save **Cancel**

New Index

General Settings

Index Name: ssh_logs
Set index name (e.g., INDEX_NAME). Search using index:INDEX_NAME.

Index Data Type: Events Metrics
The type of data to store (event-based or metrics).

Home Path: optional
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/0).

Cold Path: optional
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed Path: optional
Thawed/restricted db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check: Enable Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: 500 GB
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: auto GB
Maximum target size of buckets. Enter 'auto_high_volume' for high-volume indexes.

Frozen Path: optional
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App: Search & Reporting

Storage Optimization

Save **Cancel**

Add Data

Select Source **Set Source Type** Input Settings Review Done **< Back** **Review >**

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

The Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More 

Constant value
 Regular expression on path
 Segment in path

Host field value: LAPTOP-EHJ3QFJI

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More 

Index: Default Create a new index

✓ Default

- dns_lab
- history
- http_lab
- main
- ssh_logs
- summary

127.0.0.1:8000/en-USmanager/search/adddatamethods/inputsettings#

splunk enterprise Apps ▾

Administrator ▾ i Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Add Data Select Source Set Source Type Input Settings Review Done < Back Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. Learn More ⓘ

Constant value
 Regular expression on path
 Segment in path

Host field value: LAPTOP-EHJ3QFJI

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. Learn More ⓘ

Index: ssh_logs Create a new Index

FAQ

> How do Indexes work?
> [How do I know when to create or use multiple indexes?](#)

splunk enterprise Apps ▾

Administrator ▾ i Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Add Data Select Source Set Source Type Input Settings Review Done < Back Submit >

Review

Input Type: Uploaded File
File Name: ssh_logs.json
Source Type: json
Host: LAPTOP-EHJ3QFJI
Index: ssh_logs

6. Review settings and click **Start Searching**

The screenshot shows the Splunk Add Data interface. At the top, there's a navigation bar with 'splunk-enterprise' and 'Apps'. On the right, there are links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the navigation is a progress bar titled 'Add Data' with five steps: 'Select Source', 'Set Source Type', 'Input Settings', 'Review', and 'Done'. The 'Review' step is highlighted with a green circle. To the right of the progress bar are '< Back' and 'Next >' buttons. The main content area has a success message: '✓ File has been uploaded successfully.' followed by 'Configure your inputs by going to Settings > Data Inputs'. Below this is a large green button labeled 'Start Searching'. To the right of the button is the text 'Search your data now or see examples and tutorials.' with a link icon. There are also four other buttons: '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.', and 'Build Dashboards', 'Visualize your searches. Learn more.'.

Step-by-Step Implementation

◆ Task 1: Ingest and Parse SSH Logs

Validate Field Extraction

Ensure the following fields are extracted correctly:

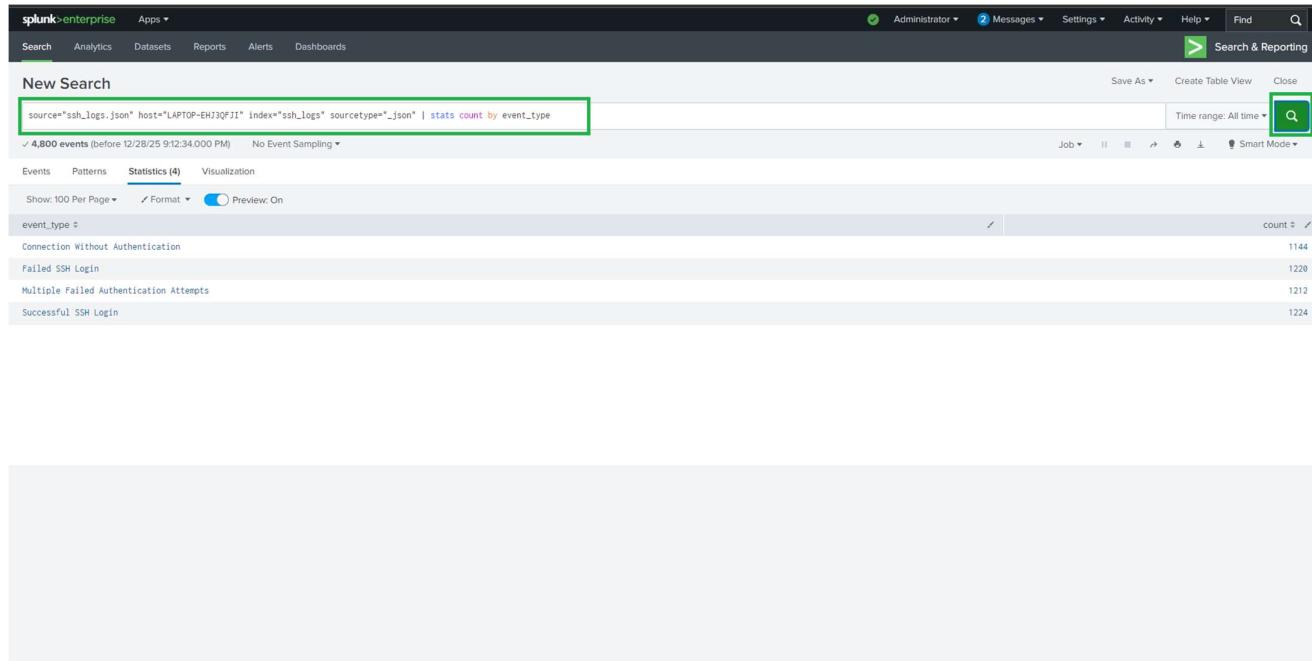
- event_type
- auth_success
- auth_attempts
- id.orig_h (Source IP)
- id.resp_h (Destination Host)

Validation Query

```
index=ssh_logs
```

```
| stats count by event_type
```

This confirms that logs are ingested and parsed successfully.



The screenshot shows the Splunk Enterprise search interface. The search bar contains the command: `source="ssh_logs.json" host="LAPTOP-ENJ3QFJ1" index="ssh_logs" sourcetype=".json" | stats count by event_type`. Below the search bar, it says "4,800 events (before 12/28/25 9:12:34.000 PM) No Event Sampling". The results table has a single row with the following data:

event_type	count
Connection Without Authentication	1144
Failed SSH Login	1220
Multiple Failed Authentication Attempts	1212
Successful SSH Login	1224

◆ Task 2: Analyze Failed Login Attempts

Identify Failed SSH Logins

```
index=ssh_logs event_type="Failed SSH Login"
```

```
| stats count by id.orig_h
```

```
| sort - count
```

```
| head 10
```

The screenshot shows a Splunk search interface with the following search command:

```
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype=".json" event_type="Failed SSH Login"
| stats count by id.orig_h
```

Results summary: 1,220 events (before 12/28/25 9:13:08.000 PM) No Event Sampling.

Statistics (50) view is selected. The results table shows the following data:

id.orig_h	count
10.0.0.10	16
10.0.0.11	12
10.0.0.12	32
10.0.0.13	28
10.0.0.14	28
10.0.0.15	16
10.0.0.16	36
10.0.0.17	38
10.0.0.18	28
10.0.0.19	12
10.0.0.20	16
10.0.0.21	40
10.0.0.22	24
10.0.0.23	24
10.0.0.24	28
10.0.0.25	36
10.0.0.26	24
10.0.0.27	28
10.0.0.28	12

The screenshot shows a Splunk search interface with the same search command and results as the previous screenshot. The Statistics (50) view is selected. The results table shows the following data:

id.orig_h	count
10.0.0.10	16
10.0.0.11	12
10.0.0.12	32
10.0.0.13	28
10.0.0.14	28
10.0.0.15	16
10.0.0.16	36
10.0.0.17	38
10.0.0.18	28
10.0.0.19	12
10.0.0.20	16
10.0.0.21	40
10.0.0.22	24
10.0.0.23	24
10.0.0.24	28
10.0.0.25	36
10.0.0.26	24
10.0.0.27	28
10.0.0.28	12

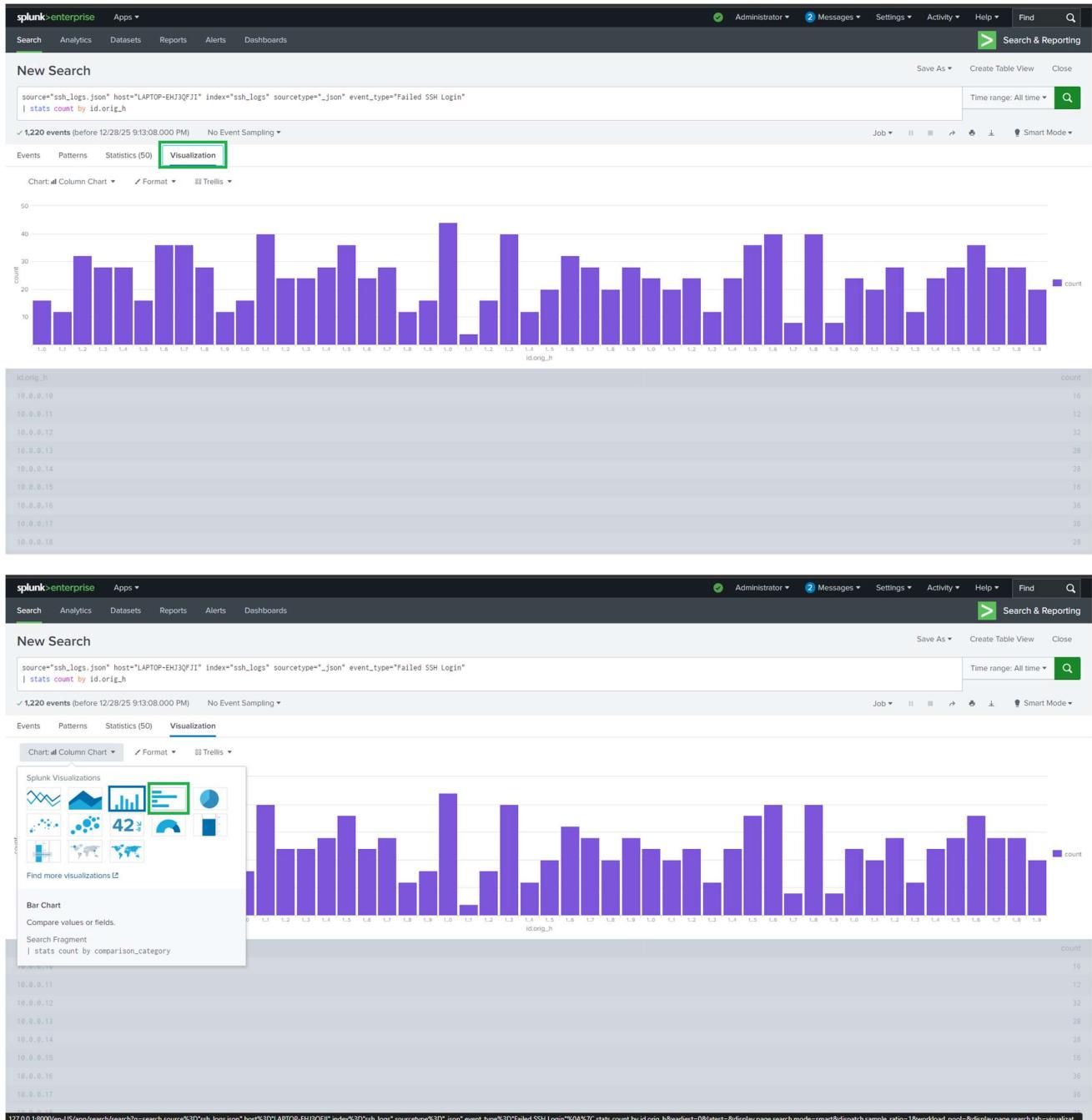
The screenshot shows a Splunk search interface with the same search command and results as the previous screenshots. The Statistics (50) view is selected. The results table shows the following data:

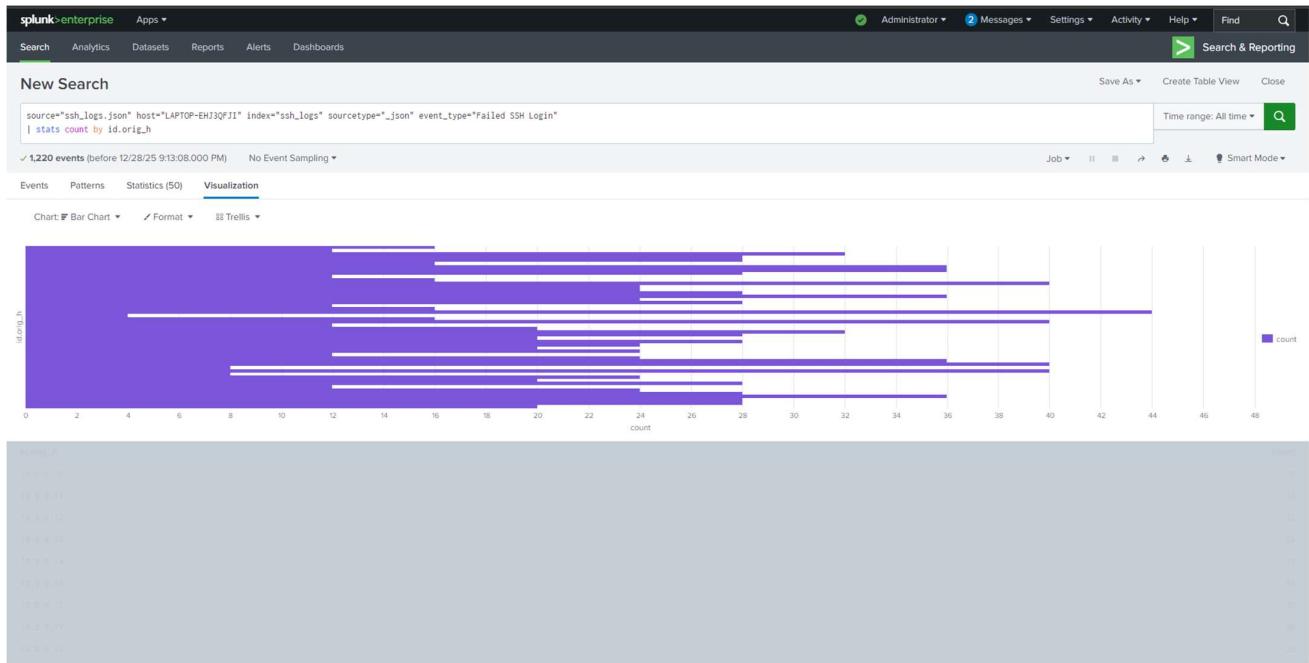
id.orig_h	count
10.0.0.10	16
10.0.0.11	12
10.0.0.12	32
10.0.0.13	28
10.0.0.14	28
10.0.0.15	16
10.0.0.16	36
10.0.0.17	36
10.0.0.18	28
10.0.0.19	12

Visualization

- Create a **Bar Chart**
- X-axis: id.orig_h
- Y-axis: Count of failed logins

📌 **Purpose:** Identify IPs generating excessive failed login attempts.





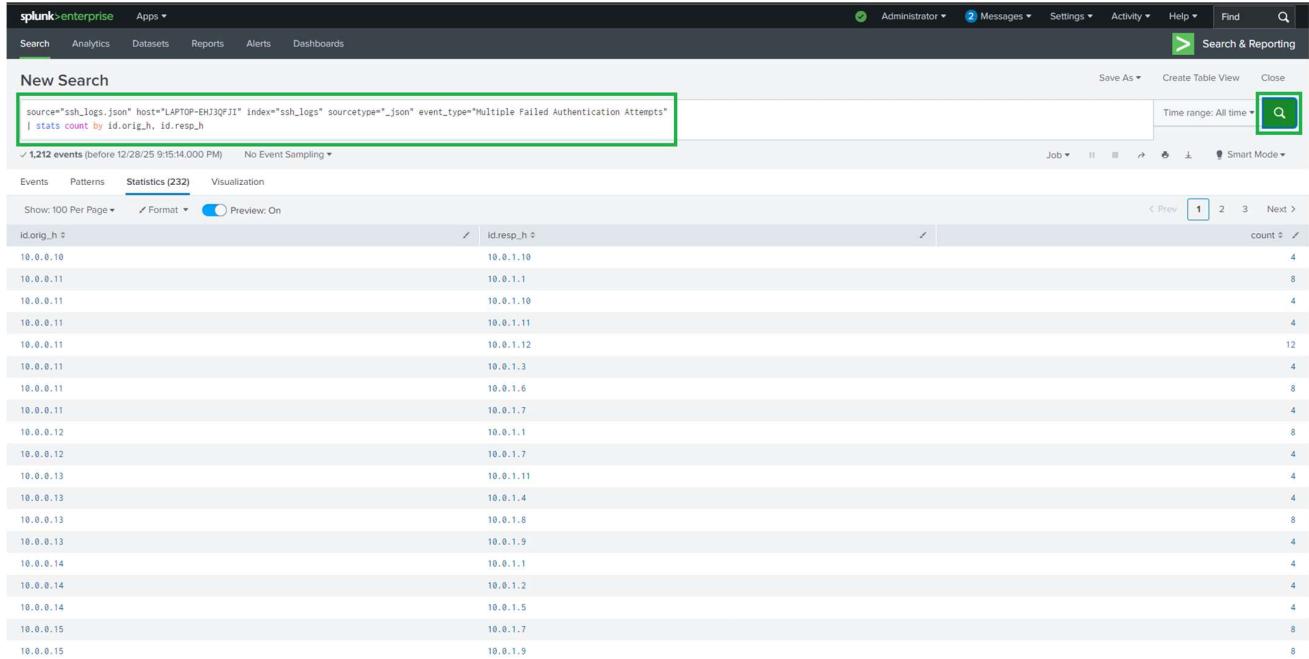
◆ Task 3: Detect Multiple Failed Authentication Attempts (Brute Force)

Search for Multiple Failed Attempts

index=ssh_logs event_type="Multiple Failed Authentication Attempts"

| stats count by id.orig_h, id.resp_h

| where count > 5



Alert Configuration

- **Trigger condition:** More than 5 failed attempts
- **Time window:** 10 minutes
- **Alert type:** Real-time or Scheduled
- **Action:** Email / SOC notification

⚠ **Purpose:** Detect brute-force attacks early.

The screenshot shows the Splunk Enterprise interface. At the top, there's a search bar with the query: `source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype=".json" event_type="Multiple Failed Authentication Attempts" | stats count by id.orig_h, id.resp_h`. Below the search bar, a table displays 1,212 events. The table has two columns: 'id.orig_h' and 'count'. The 'id.resp_h' column is currently sorted, with the top item, '10.0.1.10', highlighted with a green border. The 'count' column shows values ranging from 4 to 12. In the bottom right corner of the table area, a context menu is open, listing options: 'Save As', 'Report', 'Alert' (which is highlighted with a green border), 'Existing Dashboard', 'New Dashboard', and 'Event Type'. The 'Alert' option is selected. The URL at the bottom of the page is: `127.0.0.1:8000/_app/search/search?q=search source%3D"ssh_logs.json" host%3D"LAPTOP-EHJ3QFJI" index%3D"ssh_logs" sourcetype%3D".json" event_type%3D"Multiple Failed Authentication Attempts"%0A%7C stats count by id.orig_h%2C id.resp_h&earliest=-30s&latest=&display=page&search_mode=smart&dispatch.sample_ratio=1&workload_pool...`.

The screenshot shows the Splunk Enterprise interface with a search results page on the left and a 'Save As Alert' dialog box on the right.

Search Results (Left):

- Source: `source="ssh_logs.json" host="APTOP-EN3QJII" index="ssh_logs" sourcetype=""`
- Count: 1,212 events (before 12/28/25 9:15:00 AM)
- Events: Patterns, Statistics (232), Visualization
- Show 100 Per Page, Format, Preview On
- Hosts: id.orig_h, id.resp_h
- IP Addresses: 10.0.0.10, 10.0.0.11, 10.0.0.11, 10.0.0.11, 10.0.0.11, 10.0.0.11, 10.0.0.11, 10.0.0.11, 10.0.0.11, 10.0.0.12, 10.0.0.12, 10.0.0.13, 10.0.0.13, 10.0.0.13, 10.0.0.14, 10.0.0.14, 10.0.0.15, 10.0.0.15

Save As Alert Dialog (Right):

Settings

- Title: (highlighted with a green box)
- Description: Optional
- Permissions: Private (selected) / Shared in App
- Alert type: Scheduled (selected) / Real-time
- Run every week: at
- Expires: hour(s)

Trigger Conditions

- Trigger alert when: Number of Results
- Trigger: Once / For each result
- Throttle?

Trigger Actions

- + Add Actions

Buttons: Cancel, Save

New Search

```
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="stats count by id.orig_h, id.resp_h"
```

1,212 events (before 12/28/25 9:15:14,000 PM) No Event Sampling ▾

Events Patterns Statistics (232) Visualization

Show: 100 Per Page ▾ Format ▾ Preview: On

id.orig_h ▾

- 10.0.0.10
- 10.0.0.11
- 10.0.0.11
- 10.0.0.11
- 10.0.0.11
- 10.0.0.11
- 10.0.0.11
- 10.0.0.11
- 10.0.0.12
- 10.0.0.12
- 10.0.0.13
- 10.0.0.13
- 10.0.0.13
- 10.0.0.14
- 10.0.0.14
- 10.0.0.15
- 10.0.0.15

10.0.1.7

10.0.1.8

Save As Alert

Title: brute_force

Description: Optional

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Run every week ▾

On: Monday at: 6:00

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Number of Results ▾

is greater than: 0

Trigger

Once For each result

Throttle? □

Trigger Actions

+ Add Actions ▾

When triggered: Add to Triggered Alerts Remove

Severity: Medium

Cancel Save

New Search

```
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype="stats count by id.orig_h, id.resp_h"
```

1,212 events (before 12/28/25 9:15:14,000 PM) No Event Sampling ▾

Events Patterns Statistics (232) Visualization

Show: 100 Per Page ▾ Format ▾ Preview: On

id.orig_h ▾

- 10.0.0.10
- 10.0.0.11
- 10.0.0.11
- 10.0.0.11
- 10.0.0.11
- 10.0.0.11
- 10.0.0.11
- 10.0.0.11
- 10.0.0.12
- 10.0.0.12
- 10.0.0.13
- 10.0.0.13
- 10.0.0.13
- 10.0.0.14
- 10.0.0.14
- 10.0.0.15
- 10.0.0.15

10.0.1.10

10.0.1.11

10.0.1.10

10.0.1.11

10.0.1.12

10.0.1.13

10.0.1.6

10.0.1.7

10.0.1.1

10.0.1.7

10.0.1.11

10.0.1.4

10.0.1.6

10.0.1.9

10.0.1.1

10.0.1.2

10.0.1.5

10.0.1.7

10.0.1.9

Alert has been saved

This scheduled search will not run after the Splunk Enterprise Trial License expires.

You can view your alert, change additional settings, or continue editing it.

Additional Settings:

- Permissions

Continue Editing View Alert

splunk enterprise Apps ▾

Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Search Analytics Datasets Reports Alerts Dashboards

brute_force

Enabled: Yes. Disable

App: search

Permissions: Private. Owned by gaurav23. Edit

Modified: Dec 28, 2025 9:18:30 PM

Alert Type: Scheduled. Weekly, Monday at 6:00. Edit

Trigger Condition: Number of Results is > 0. Edit

Actions: 1 Action Edit

Add to Triggered Alerts

Info There are no fired events for this alert.

◆ Task 4: Track Successful SSH Logins

Successful Login Query

```
index=ssh_logs event_type="Successful SSH Login"  
| stats count by id.orig_h, id.resp_h
```

Correlation Use Case

Compare:

- IPs with multiple failed logins
- IPs that later successfully authenticate

📌 Purpose: Detect potential compromised credentials.

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query: `source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype=".json" event_type="Successful SSH Login" | stats count by id.orig_h, id.resp_h`. A green box highlights this query. The results table shows 1,224 events. The columns are `id.orig_h`, `id.resp_h`, and `count`. The data is as follows:

<code>id.orig_h</code>	<code>id.resp_h</code>	<code>count</code>
10.0.0.10	10.0.1.1	4
10.0.0.10	10.0.1.12	8
10.0.0.10	10.0.1.5	4
10.0.0.10	10.0.1.6	4
10.0.0.10	10.0.1.8	4
10.0.0.11	10.0.1.11	4
10.0.0.11	10.0.1.3	4
10.0.0.11	10.0.1.6	4
10.0.0.11	10.0.1.8	4
10.0.0.11	10.0.1.9	4
10.0.0.12	10.0.1.11	4
10.0.0.12	10.0.1.12	4
10.0.0.12	10.0.1.6	4
10.0.0.12	10.0.1.7	4
10.0.0.12	10.0.1.8	4
10.0.0.13	10.0.1.1	12
10.0.0.13	10.0.1.5	4
10.0.0.13	10.0.1.6	4
10.0.0.14	10.0.1.1	4

Dashboard Panel

- Visualization: Bar Chart or Table
- Metric: Top source IPs with successful SSH logins

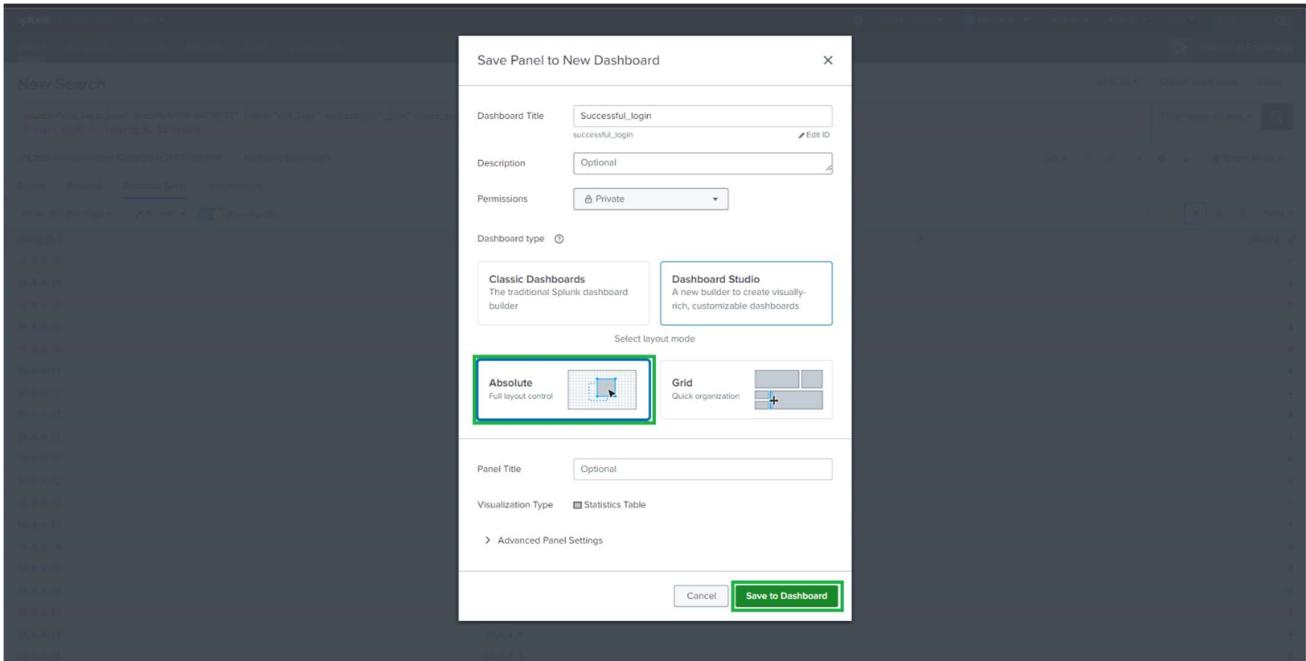
The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk-enterprise', 'Apps', and various system links like 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search bar. Below the navigation is a 'New Search' bar containing a search command:

```
source="ssh_logs.json" host="LAPTOP-EHJ3QFJI" index="ssh_logs" sourcetype=".json" event_type="Successful SSH Login"
| stats count by id.orig_h, id.resp_h
```

The search results table shows 1,224 events from before 12/28/25 9:21:57.000 PM. The table has columns for 'id.orig_h' and 'id.resp_h'. A context menu is open over the table, with 'New Dashboard' highlighted.

id.orig_h	id.resp_h	count
10.0.0.10	10.0.1.1	4
10.0.0.10	10.0.1.12	8
10.0.0.10	10.0.1.5	4
10.0.0.10	10.0.1.6	4
10.0.0.10	10.0.1.8	4
10.0.0.11	10.0.1.11	4
10.0.0.11	10.0.1.3	4
10.0.0.11	10.0.1.6	4
10.0.0.11	10.0.1.8	4
10.0.0.11	10.0.1.9	4
10.0.0.12	10.0.1.11	4
10.0.0.12	10.0.1.12	4
10.0.0.12	10.0.1.6	4
10.0.0.12	10.0.1.7	4
10.0.0.12	10.0.1.8	4
10.0.0.13	10.0.1.1	12
10.0.0.13	10.0.1.5	4
10.0.0.13	10.0.1.6	4

Below the search results, a modal dialog titled 'Save Panel to New Dashboard' is open. It asks for a 'Dashboard Title' (Required), a 'Description' (Optional), and 'Permissions' (Private). It also includes a section for 'Dashboard type' with two options: 'Classic Dashboards' (The traditional Splunk dashboard builder) and 'Dashboard Studio' (A new builder to create visually-rich, customizable dashboards). The 'Dashboard Studio' option is highlighted with a green box. At the bottom of the dialog are 'Panel Title' (Optional), 'Visualization Type' (Statistics Table), and 'Advanced Panel Settings' buttons, along with 'Cancel' and 'Save to Dashboard' buttons.



The screenshot shows the Splunk interface with a search results page in the background. A modal dialog box titled "Your Dashboard Panel Has Been Created" is open, stating "The panel has been created and added to successful_login. You may now view the dashboard." At the bottom right of this dialog is a "View Dashboard" button. The background search results show a table with columns "id.org.b" and "id.resp.h". The data in the table is as follows:

id.org.b	id.resp.h	count
10.0.0.10	10.0.1.1	4
10.0.0.10	10.0.1.12	8
10.0.0.10	10.0.1.5	4
10.0.0.10	10.0.1.6	4
10.0.0.10	10.0.1.8	4
10.0.0.11	10.0.1.11	4
10.0.0.11	10.0.1.3	4
10.0.0.11	10.0.1.6	4
10.0.0.11	10.0.1.9	4
10.0.0.11	10.0.1.9	4
10.0.0.12	10.0.1.11	4
10.0.0.12	10.0.1.12	4
10.0.0.12	10.0.1.6	4
10.0.0.12	10.0.1.7	4
10.0.0.12	10.0.1.8	4
10.0.0.13	10.0.1.1	12
10.0.0.13	10.0.1.5	4
10.0.0.13	10.0.1.6	4
10.0.0.14	10.0.1.1	4

id.orig_h	id.resp_h	count
10.0.0.10	10.0.11	4
10.0.0.10	10.0.12	8
10.0.0.10	10.0.15	4
10.0.0.10	10.0.16	4
10.0.0.10	10.0.18	4

◆ Task 5: Detect Connections Without Authentication

Search Unauthenticated Connections

index=ssh_logs event_type="Connection Without Authentication"

| stats count by id.orig_h

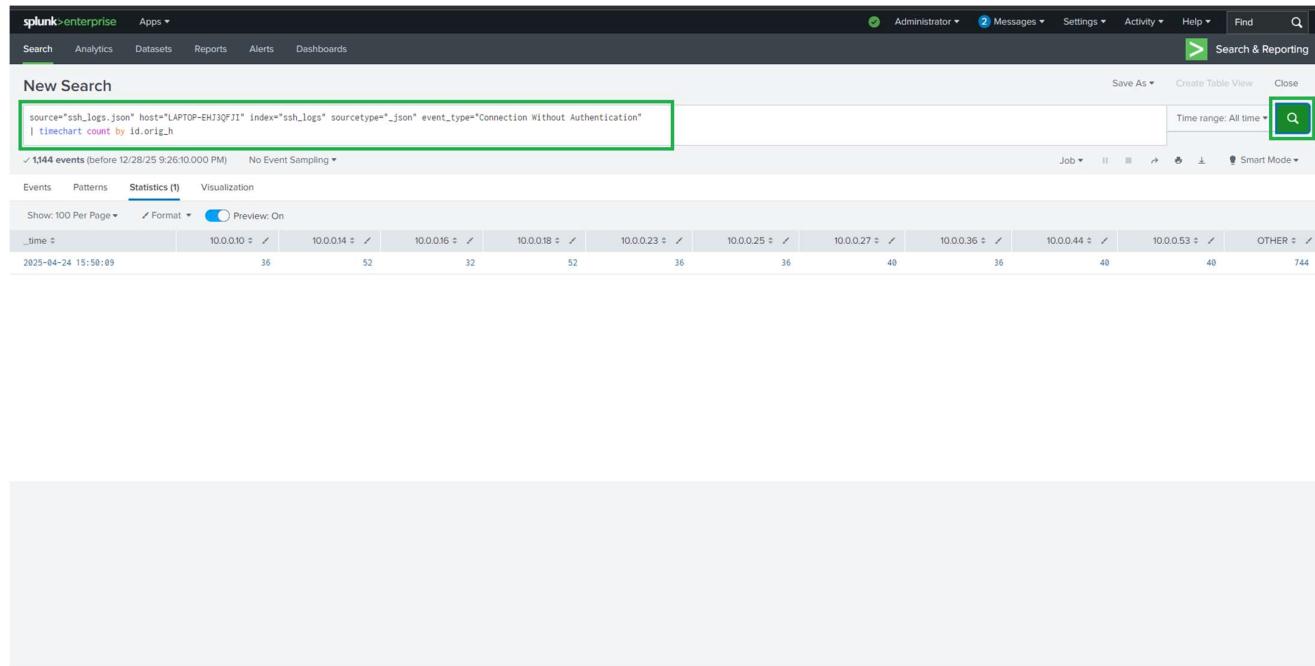
id.orig_h	id.resp_h	count
10.0.0.10		36
10.0.0.11		28
10.0.0.12		8
10.0.0.13		12
10.0.0.14		52
10.0.0.15		8
10.0.0.16		32
10.0.0.17		8
10.0.0.18		52
10.0.0.19		8
10.0.0.20		16
10.0.0.21		24
10.0.0.22		28
10.0.0.23		36
10.0.0.24		12
10.0.0.25		36
10.0.0.26		28
10.0.0.27		40
10.0.0.28		12

Time-Based Monitoring

```
index=ssh_logs event_type="Connection Without Authentication"
| timechart count by id.orig_h
```

📌 Purpose:

- Identify SSH probing
- Detect port scanning or reconnaissance activity



📊 Dashboards Created

- 🔒 SSH Successful Login Monitoring
- ✗ Failed Login Attempts per IP
- 💡 Brute Force Detection
- 🔎 Unauthenticated SSH Connection Trends

⚠️ Alerts Configured

- **Brute-force detection alert**
- Triggered on multiple failed authentication attempts
- Time-based correlation (10-minute window)

Conclusion

By completing this project, you have:

- ✓ Ingested and parsed SSH logs in Splunk
- ✓ Written SPL queries for threat detection
- ✓ Built SOC-style dashboards
- ✓ Configured alerts for high-risk activity
- ✓ Gained hands-on **SOC Analyst-level log analysis experience**