

# Home Lab Setup & SIEM Implementation Using Splunk



**Prepared by:**

Kripesh Acharya  
[Kripeshacharya2025@gmail.com](mailto:Kripeshacharya2025@gmail.com)

September 2024

## Table of Contents

Abstract.....	3
1. Introduction.....	4
2. Project Implementation.....	5
2.2 Log Collection and Integration .....	12
2.3 Data Parsing and Security Analysis .....	16
2.4 Dashboard Creation .....	25
2.5 Reporting, Scheduling and Alerting.....	26
2.6     Continuous Monitoring.....	28
3.Learning Resources.....	28
4. Conclusion .....	28

## **Abstract**

This report outlines the implementation of a Security Information and Event Management (SIEM) system using Splunk in a home lab environment. The project involved installing Splunk Enterprise, integrating and parsing various log files, and conducting security analysis. Key activities included monitoring logs, detecting suspicious events using Search Processing Language (SPL), and creating dashboards and alerts to enhance security visibility and response.

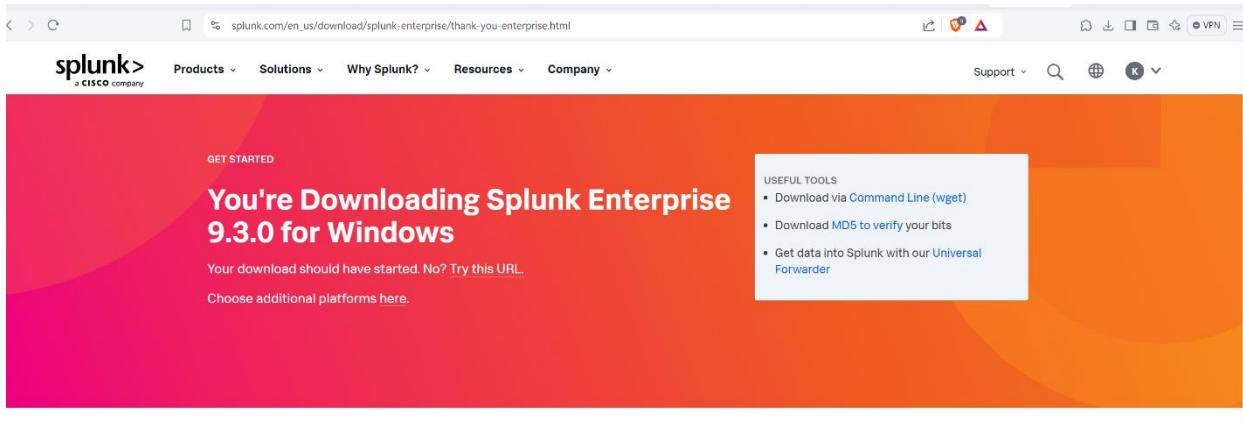
## 1. Introduction

With the increasing complexity of security threats, effective monitoring and analysis of log data are crucial. This project focuses on setting up a SIEM solution using Splunk, a leading platform for handling large volumes of machine-generated data. The goal was to gain practical experience in log management, data integration, and security analysis within a controlled home lab environment.

## 2. Project Implementation

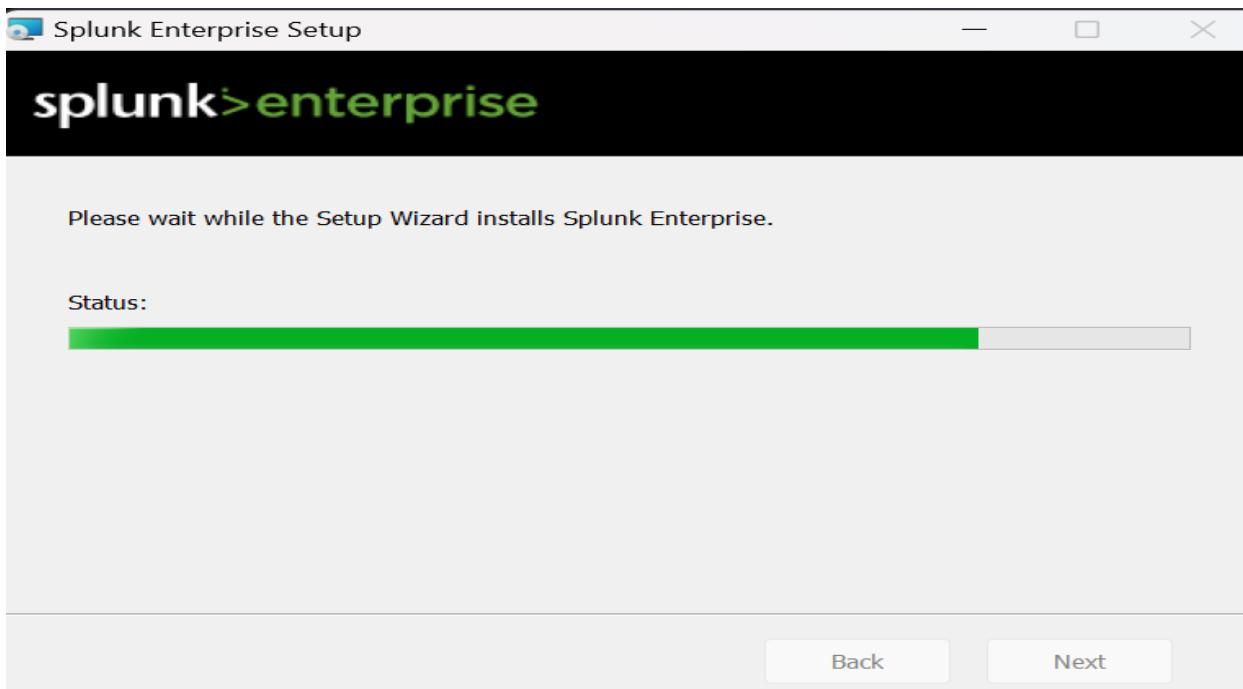
### 2.1 Installation and Initial Setup

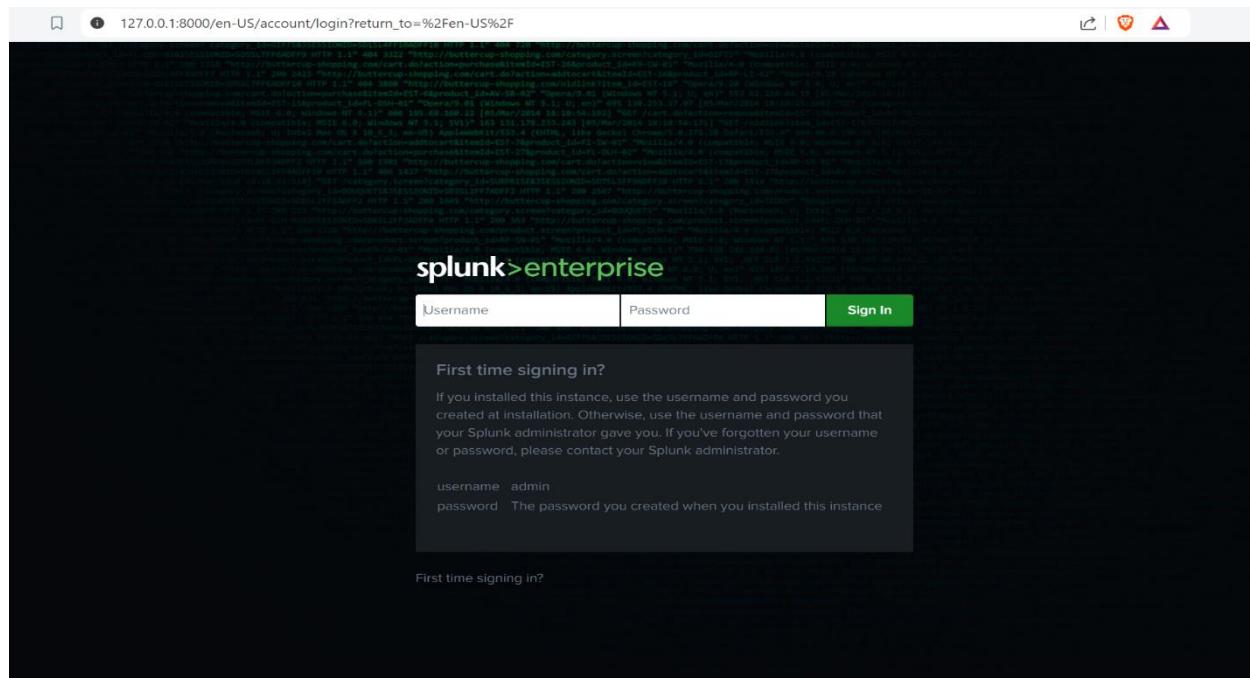
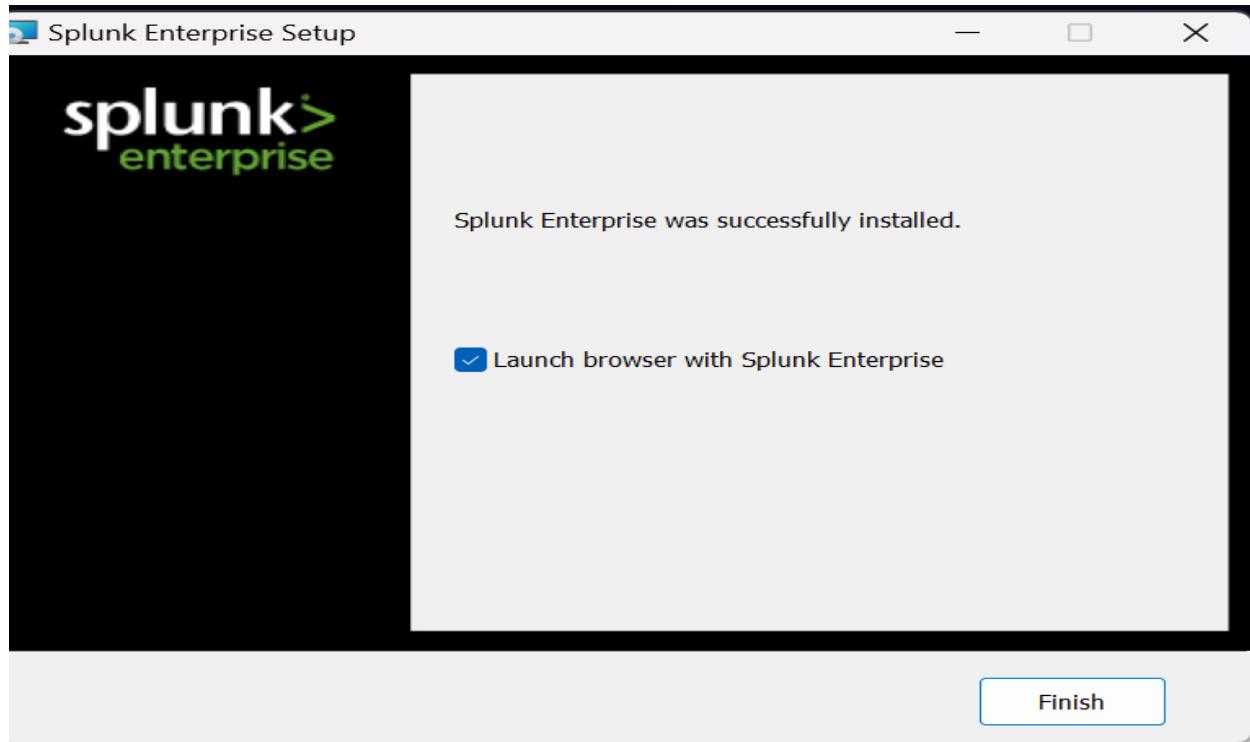
The project began with the download and installation of Splunk Enterprise from the official website. The setup was performed on a Windows system.



Getting Data In    Search and Alerts    Reports and Dashboards    Learning Splunk

Getting Data In — Windows (4:07)    Getting Data In — Linux (4:47)    Getting Data In — Forwarders (4:34)





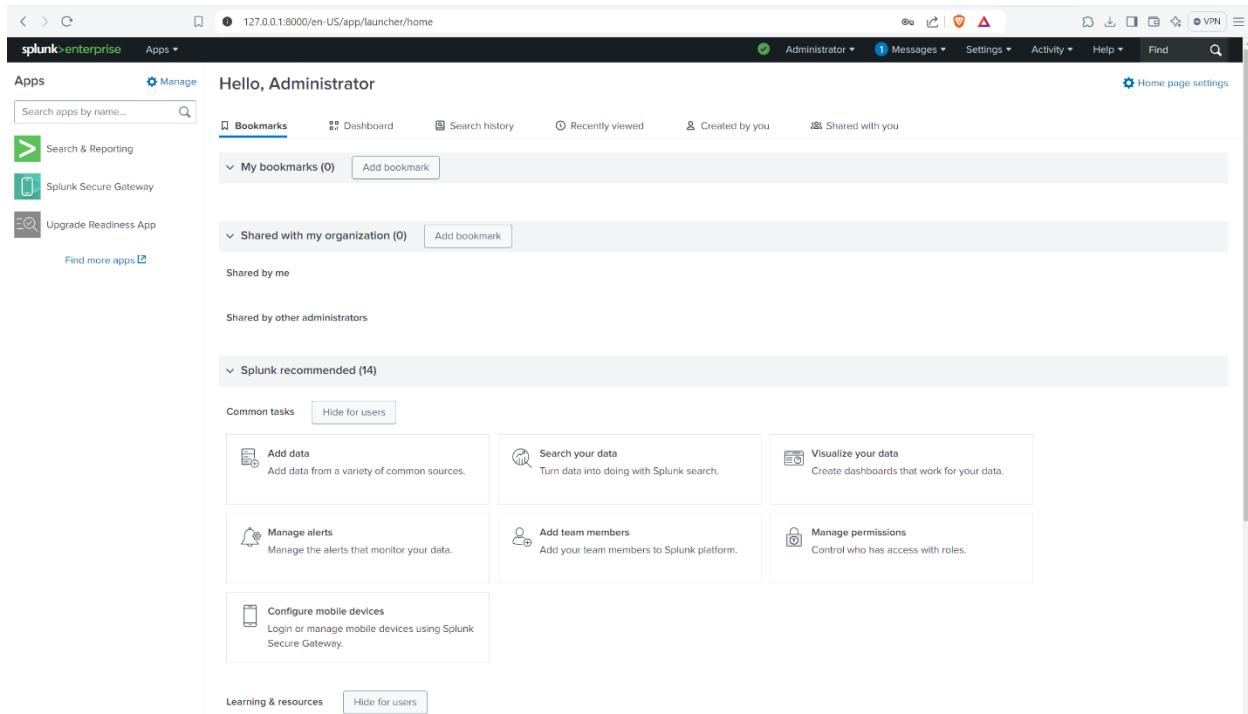


Fig: Splunk Enterprise Initial Setup

After the initial setup, it's important to ensure that Splunk is configured to start automatically and continues to monitor data without interruption.

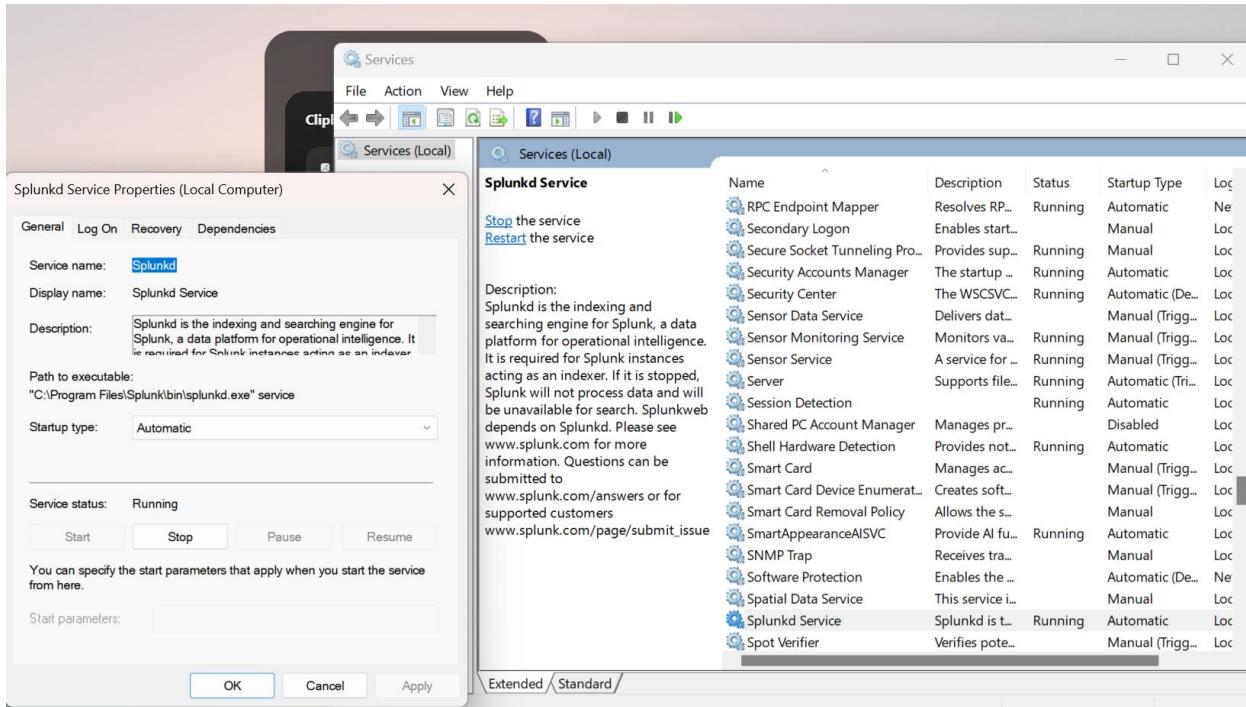


Fig: Verify Application Startup Status

After verifying that Splunk is starting up correctly, the next step involves configuring and selecting the appropriate log collections. In this case only Application, Security and System was selected.

The screenshot shows the 'Event Log Collections' configuration page in Splunk Enterprise. The top navigation bar includes 'splunk>enterprise', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search icon. The main title is 'Event Log Collections' under 'Data Inputs > Event Log Collections'. A sub-header 'Logs' is followed by a table with two columns: 'Available log(s)' and 'Selected log(s)'. The 'Available log(s)' column lists 'Intel-iaLPSS2-I2C/Debug', 'Intel-iaLPSS2-I2C/Performance', 'Security', 'Setup', and 'System'. The 'Selected log(s)' column contains 'Application', 'Security', and 'System'. Below the table is a note: 'Select the Windows Event Logs you want to index from the list.' At the bottom left is an 'Index' section with a dropdown set to 'default'. At the bottom right are 'Cancel' and 'Save' buttons.

Fig: Log Collection Selection

To test its detection capabilities, the Windows Event Security logs were cleared and Splunk was checked to see if it generated an alert for this action.

The screenshot shows a 'New Search' page in Splunk Enterprise. The top navigation bar is identical to the previous screenshot. The main search bar contains the query 'index = \_internal'. Below the search bar, it says '179,340 events (9/11/24 10:00:00.000 AM to 9/12/24 10:30:18.000 AM)'. The search results are displayed under the 'Events (179,340)' tab, which is currently selected. Other tabs include 'Patterns', 'Statistics', and 'Visualization'. At the bottom, there are buttons for 'Format Timeline', 'Zoom Out', 'Zoom to Selection', and 'Deselect'.

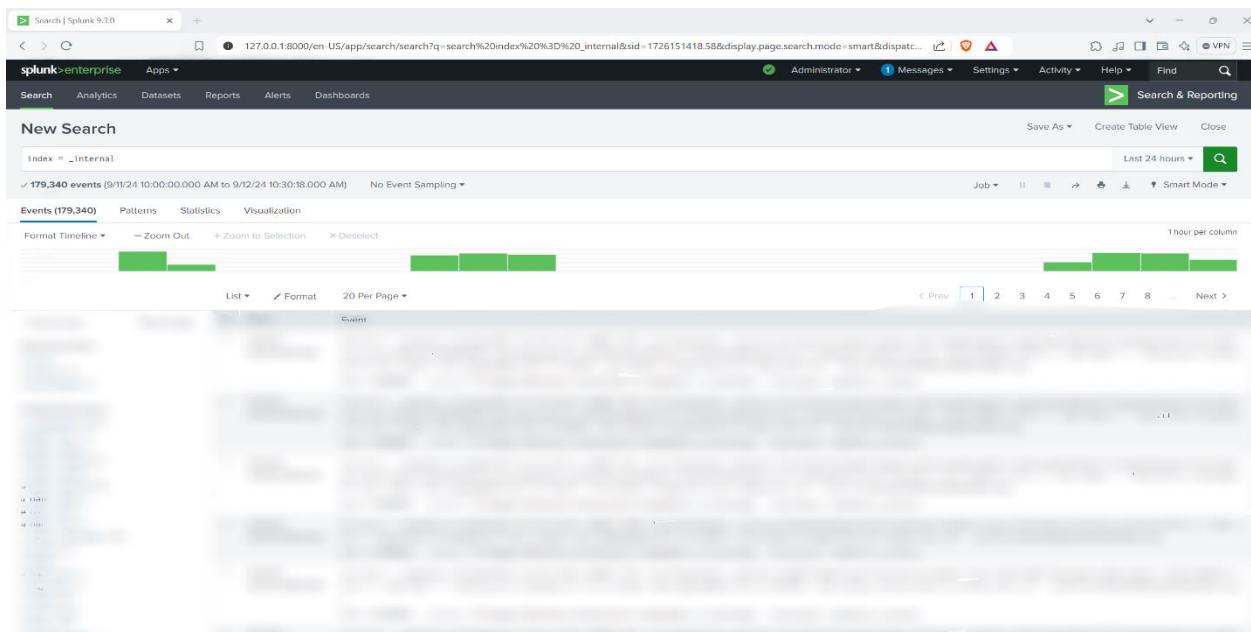


Fig: Internal System Alerts

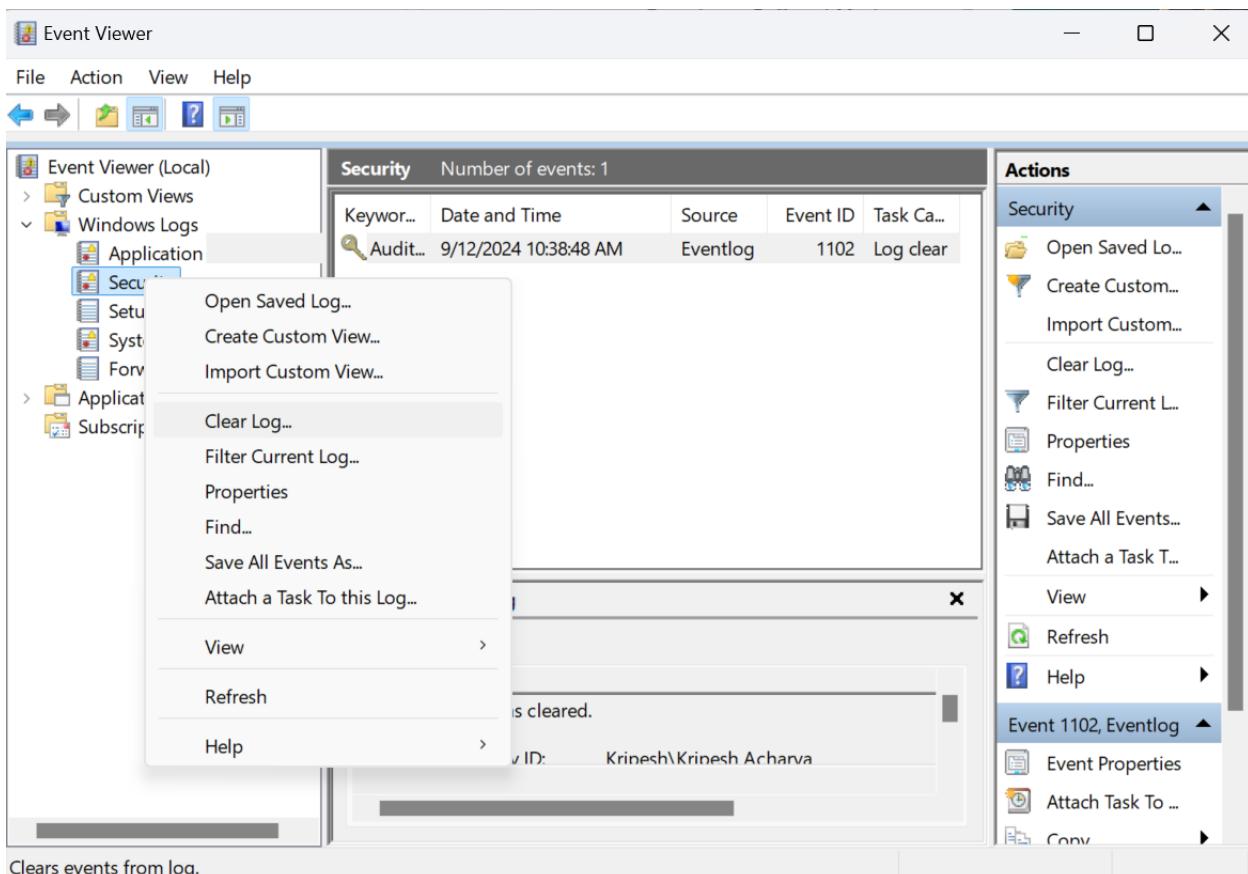


Fig: Security Log Cleared

**New Search**

\* host="KRIPESH"

✓ 89 events (9/12/24 10:28:24.000 AM to 9/12/24 10:43:24.000 AM) No Event Sampling

Events (89) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect

Show Fields List ▾ Format 20 Per Page ▾

i	Time	Event
>	9/12/24 10:38:48.000 AM	09/12/2024 10:38:48 AM LogName=Security EventCode=1102 EventType=4 ComputerName=Kripesh Show all 17 lines host = KRIPESH   source = WinEventLog:Security   sourcetype = WinEventLog:Security
>	9/12/24 10:36:14.000 AM	09/12/2024 10:3 Add to search 81 events LogName=Applica... EventCode=1001 EventType=4 ComputerName=Kr... Show all 52 lines

127.0.0.1:8000/en-US/app/search/search?q=search%20%20host%3D"KRIPESH"%20source%3D"Wi...

\* host="KRIPESH" source="WinEventLog:Security" EventCode="1102"

✓ 1 event (9/12/24 10:29:25.000 AM to 9/12/24 10:44:25.000 AM) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect

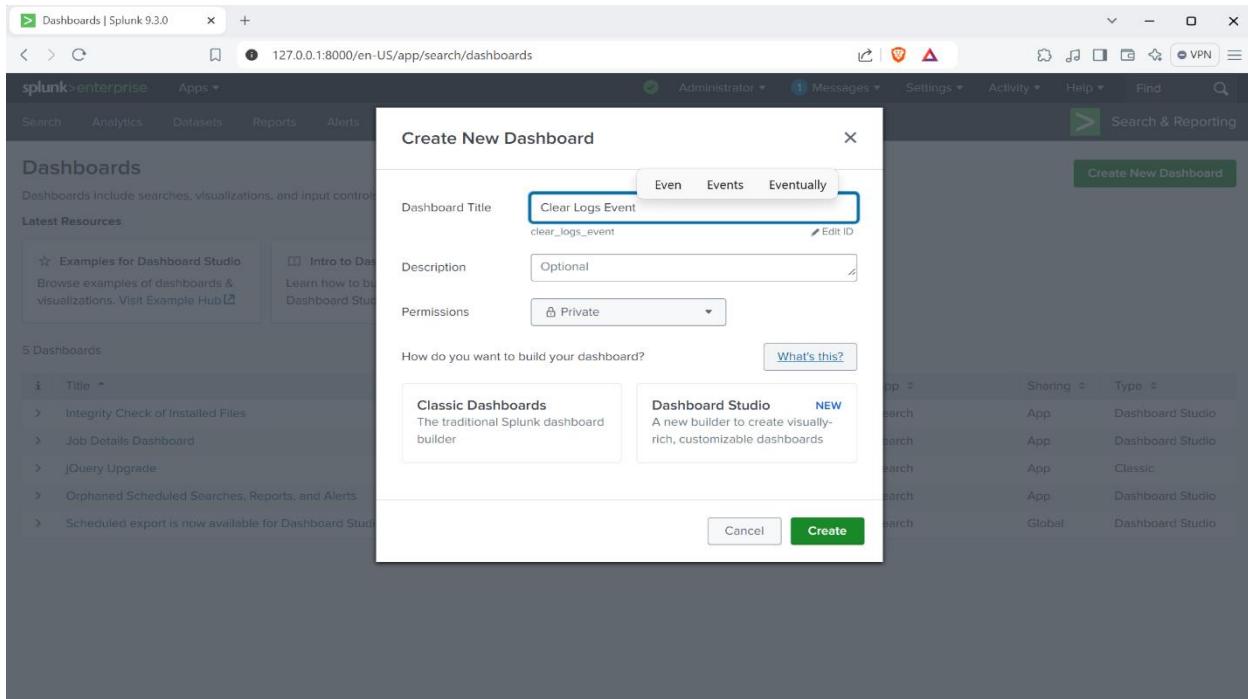
Show Fields List ▾ Format 20 Per Page ▾

i	Time	Event
>	9/12/24 10:38:48.000 AM	09/12/2024 10:38:48 AM LogName=Security EventCode=1102 EventType=4 ComputerName=Kripesh SourceName=Microsoft-Windows-Eventlog Type=Information RecordNumber=150546 Keywords=Audit Success TaskCategory=Log clear OpCode=Info Message=The audit log was cleared. Subject: Security ID: [REDACTED] Account Name: Kripesh Acharya Domain Name: Kripesh Logon ID: [REDACTED]

Event Actions ▾

Fig: Windows Event Security Log Detected

After successfully detecting the log-cleared alert, a new dashboard was created to facilitate easy viewing of similar alerts in the future.



Title	Actions	Owner	App	Sharing	Type
Clear Logs Event	Edit	kacharya	search	Private	Dashboard Studio
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

Fig: Dashboard Created

UltimateWindowsSecurity.com can be referred to for details on event log IDs and other important information related to Windows security events.

The screenshot shows a web browser window with the URL [ultimatewindowssecurity.com/securitylog/encyclopedia/](http://ultimatewindowssecurity.com/securitylog/encyclopedia/). The page title is "Windows Security Log Events". On the left, there's a sidebar with links like "Event IDs", "All Event IDs", and "Audit Policy". Below that is a search bar with "Go To Event ID:" and a "Go" button. Further down is a "Quick Reference Chart" button. The main content area has several filter dropdowns: "All Sources" (with "Windows Audit" selected), "Windows Audit Categories" (with "All categories" selected), "Subcategories" (with "All subcategories" selected), "Windows Versions" (with "Win2008, Win2012R2, Win2016 and Win10+, Win2019" selected), and a "Category: All" dropdown. The main list of events includes:

- Windows 1100 The event logging service has shut down
- Windows 1101 Audit events have been dropped by the transport
- Windows 1102 The audit log was cleared
- Windows 1104 The security Log is now full
- Windows 1105 Event log automatic backup
- Windows 1108 The event logging service encountered an error
- Windows 4608 Windows is starting up
- Windows 4609 Windows is shutting down
- Windows 4610 An authentication package has been loaded by the Local Security Authority
- Windows 4611 A trusted logon process has been registered with the Local Security Authority
- Windows 4612 Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits.
- Windows 4614 A notification package has been loaded by the Security Account Manager.
- Windows 4615 Invalid use of LPC port
- Windows 4616 The system time was changed.
- Windows 4618 A monitored security event pattern has occurred
- Windows 4621 Administrator recovered system from CrashOnAuditFail
- Windows 4622 A security package has been loaded by the Local Security Authority.

## 2.2 Log Collection and Integration

Logs from various sources, including DNS, FTP, and SSH, were collected and integrated into Splunk. This involved adding log files to the system and ensuring they were correctly indexed and searchable. The next step involves adding log files into Splunk for security analysis. The first log data imported into the application is the DNS log. This includes configuring the data input, ensuring proper indexing, and setting up necessary parsing rules to facilitate effective analysis and detection of security events.

The screenshot shows the Splunk 9.3.0 interface. The top navigation bar includes links for Dashboards, Clear Logs Event, Add Data, and the current page, 127.0.0.1:8000/en-US/manager/Splunk\_Security\_Essentials/adddata. The main content area displays a form titled "What data do you want to send to the Splunk platform?" with two sections: "Upload files from my computer" (with options for Local log files, Local structured files (e.g. CSV), and a Tutorial for adding data) and "Monitor files and ports on this Splunk instance" (with options for Files - HTTP - WMI - TCP, Modular inputs for external sources, and a Tutorial for adding data). A sidebar menu is open, showing categories like KNOWLEDGE, DATA, SYSTEM, and USERS AND AUTHENTICATION, each with sub-options such as Searches, reports, and alerts; Data inputs; and Roles.

The screenshot shows the 'Add Data' wizard in Splunk, specifically the 'Select Source' step. The interface includes a progress bar with five steps: 'Select Source' (green dot), 'Set Source Type' (white dot), 'Input Settings' (white dot), 'Review' (white dot), and 'Done' (white dot). Below the progress bar are 'Back' and 'Next' buttons. The main area is titled 'Select Source' and contains instructions: '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 'Learn More' link is provided. A 'Selected File: No file selected' message is displayed above a 'Select File' button. To the right of the file selection area is a file explorer window titled 'Sample data' showing a directory structure. The 'dns.log.gz' file is selected, with details like 'Name: dns.log.gz', 'Date modified: 9/12/2024 1:38 PM', and 'Type: Compressed'. The file explorer also lists other folders and files such as Desktop, Downloads, Documents, Pictures, Music, Videos, job certificates, Applications, and Certificates.

Dashboard | Splunk 9.3.0 | Clear Logs Event | Splunk 9.3.0 | Add Data - Set Sourcetype | Splunk 9.3.0

127.0.0.1:8000/en-US/manager/Splunk\_Security\_Essentials/adddatamethods/datapreview

splunk>enterprise Apps ▾ Administrator ▾ 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: dns.log.gz

View Event Summary

Source type: Select Source Type ▾		List ▾ Format 20 Per Page ▾									
		Time			Event						
> Event Breaks	Save As	1	9/12/24	1:42:17.000 PM	1331901005.510000	CWGTk431H9XuaTN4fi	192.168.202.100	45658	192.168.27.203	137	
> Timestamp		2	9/12/24	1:42:17.000 PM	1331901015.070000	C36a282Jljjz7BsbGH	192.168.202.76	137	192.168.202.255	137	
> Advanced		3	9/12/24	1:42:17.000 PM	1331901015.820000	C36a282Jljjz7BsbGH	192.168.202.76	137	192.168.202.255	137	
		4	9/12/24	1:42:17.000 PM	1331901016.570000	C36a282Jljjz7BsbGH	192.168.202.76	137	192.168.202.255	137	
		5	9/12/24	1:42:17.000 PM	1331901005.860000	C36a282Jljjz7BsbGH	192.168.202.76	137	192.168.202.255	137	

## Save Source Type

**Name** DNS\_Logs

**Description**

**Category** Custom ▾

**App** Search & Reporting ▾

**Cancel** **Save**

**Add Data**

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: Kripesh

**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?

127.0.0.1:8000/en-US/manager/Splunk\_Security\_Essentials/adddatamethods/inputsettings#

**Add Data**

**Uploading File**  
Processing...

**Review**

Input Type ..... Uploaded File  
File Name ..... dns.log.gz

**Submit >**

**New Search**

source=dns.log.gz host="Kripesh" sourcetype=DNS\_Logs

✓ 422,130 events (before 9/12/24 1:46:14.000 PM) No Event Sampling

Events (422,130) Patterns Statistics Visualization

Format, Timeline | Zoom Out | + Zoom to Selection | X Deselect

100 milliseconds per column

List | Format | 20 Per Page | C Prev | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | ... | Next |

< Hide Fields		i	Time	Event
SELECTED FIELDS	a host 1 a source 1 a sourcetype 1	>	9/12/24 1:46:00.000 PM	1332817991.830000 C05001GM#5211C8 192.168.292.122.137 192.168.207.255.137 udp 33/87 1ABADIN:941491 1 C_INTERNET 32 NB -
INTERESTING FIELDS	a index 1 # linecount 10 a punct 100+ a splunk.server 1 a timestamp 1	>	9/12/24 1:46:00.000 PM	1332817991.830000 C05001GM#5211C8 192.168.292.83.456519 192.168.207.4 53 udp 125/72 44.206.168.192.in-addr.arpa 1 C_INTERNET 12
11 more fields	+ Extract New Fields	>	9/12/24 1:46:00.000 PM	1332817991.830000 C05001GM#5211C8 192.168.292.88.60538 192.168.206.44.53 udp 36843 dr..dns-sd..udp.0.48.16.172.in-addr.arpa 1 C_INTERNET
		>	9/12/24 1:46:00.000 PM	1332817991.830000 C05001GM#5211C8 192.168.292.88.65208 192.168.206.44.53 udp 30842 dr..dns-sd..udp.0.202.168.192.in-addr.arpa 1 C_INTERNET
		>	9/12/24 1:46:00.000 PM	1332817991.830000 C05001GM#5211C8 192.168.292.88.65208 192.168.206.44.53 udp 28561 b..dns_sd..udp.0.48.16.172.in-addr.arpa 1 C_INTERNET
		>	9/12/24 1:46:00.000 PM	1332817991.830000 C05001GM#5211C8 192.168.292.88.65208 192.168.206.44.53 udp 58/91 1b..dns_sd..udp.0.48.16.172.in-addr.arpa 1 C_INTERNET
		>	9/12/24 1:46:00.000 PM	1332817991.830000 C05001GM#5211C8 192.168.292.88.65208 192.168.206.44.53 udp 63787 44.206.168.192.in-addr.arpa 1 C_INTERNET 12

Fig: DNS Log File Uploaded Successfully

### 2.3 Data Parsing and Security Analysis

Data parsing was performed to structure the logs appropriately. Security analysis was conducted using Splunk's Search Processing Language (SPL) to identify and investigate suspicious events. This process included filtering and querying the log data to uncover potential security issues. The next step after uploading the log file is to select a sample event and parse the data. This ensures that the data is structured appropriately, making it easier to use later in Search Processing Language (SPL) queries for effective analysis and reporting.

## Select Method

Indicate the method you want to use to extract your field(s). Learn more [»](#)

[I prefer to write the regular expression myself >](#)

Source type  
**DNS\_Logs**

1332017958.990000	CDP8CAi82kvSsJat8	192.168.202.83	35036	192.168.207.4	53	udp	63787	44.206.168.192.in-addr.arpa	1	C_INTERNET	12	PTR
3	NXDOMAIN	F	F	T	F	0	-	-	F			F

(.\*?)

Regular Expression

Splunk Enterprise will extract fields using a Regular Expression.

x|y|z

Delimiters

Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

## Select Fields

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist in an event for the regular expression sample event to modify them. To highlight text that is already part of an existing extraction, first turn off the existing extractions. [Learn more »](#)

1332017958.990000	CDP8CAi82kvSsJat8	192.168.202.83	35036	192.168.207.4	53	udp	63787	44.206.168.192.in-addr.arpa				
3	NXDOMAIN	F	F						F			

Extracted Fields

Ip    I    if

Field Name: **Src\_ip**

Sample Value: **192.168.202.83**

**Add Extraction**

## Extract Fields

Select Sample    Select Method    Select Fields    Validate    Save    [< Back](#)    **Finish >**

## Save

Name the extraction and set permissions.

Extractions Name: **EXTRACT- Src\_ip**

Owner: **kacharya**

App: **Splunk\_Security\_Essentials**

Permissions:

Owner     App     All apps

Source type: **DNS\_Logs**

Sample event: 1332017958.990000    CDP8CAi82kvSsJat8    192.168.202.83    35036    192.168.207.4    53    udp  
63787    44.206.168.192.in-addr.arpa    1    C\_INTERNET    12    PTR    3    NXDOMAIN    F  
F    T    F    0    -    -    F

Fields: **Src\_ip**

Regular Expression: **^(?:[^t\n]\*\t){2}(?P<Src\_ip>[^t]+)**

Fig: Data Parsed from the Log Event Sample

After the data is parsed, it is analyzed for further investigation using Search Processing Language and commands. This step helps in querying the data to identify and investigate security events and anomalies.

Fig: Looking For top 20 Domain mostly visited

index=\_\* OR index=\*\_ sourcetype=DNS\_Logs domain="tools.google.com"

✓ 14,051 events (9/11/24 2:00:00.000 PM to 9/12/24 2:16:34.000 PM) No Event Sampling ▾

**Events (14,051)** Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect

List ▾ ✎ Format 20 Per Page ▾

◀ Hide Fields : All Fields

**SELECTED FIELDS**

- a host 1
- a index 1
- # linecount 2
- a punct 3
- a source 1
- a sourcetype 1
- a splunk\_server 1
- a timestamp 1

**INTERESTING FIELDS**

- a domain 1
- a Dst\_ip 7
- # Dst\_port 1
- a Src\_ip 32
- # Src\_port 100+

+ Extract New Fields

i	Time	Event	
<b>Src_ip</b>			
32 Values, 100% of events		Selected Yes No	
<b>Reports</b>			
<a href="#">Top values</a>	<a href="#">Top values by time</a>	<a href="#">Rare values</a>	
<a href="#">Events with this field</a>			
<b>Top 10 Values</b>		Count	%
10.10.117.210		10,179	72.443%
10.10.117.209		1,644	11.7%
192.168.202.106		326	2.32%
192.168.229.252		280	1.993%
192.168.202.76		208	1.48%
192.168.202.85		207	1.473%
192.168.202.91		201	1.43%
192.168.202.80		132	0.939%
192.168.28.25		128	0.911%
192.168.203.63		117	0.833%

In the above figure, to determine which users visited a particular site the most, a query was executed to identify and list the top users based on their visit frequency to the specified site.

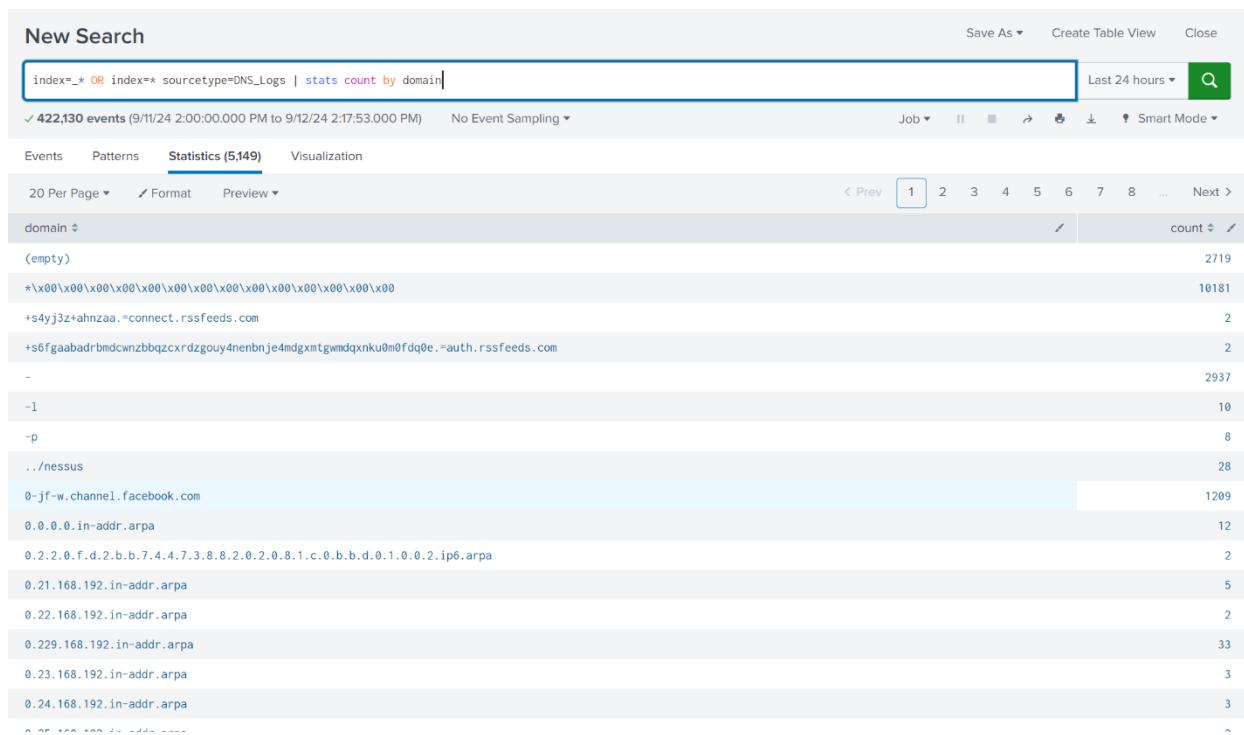


Fig: Query Executed to View Total Statistics Number of Domain

Similarly, the analysis was also conducted on the FTP log data to identify key patterns and user activity, using similar queries to extract valuable insights for further investigation.

## Save Source Type

X

---

Name	FTP_logs
Description	
Category	Custom ▾
App	Search & Reporting ▾

Fig: FTP Log data Uploaded

The user "anonymous" had attempted to send files multiple times, raising suspicion. The username was filtered, and the status of each attempt was checked based on the server logs to determine if any of the file transfers were successful.

In the same way, the SSH log file was analyzed to investigate user activity and identify any potential security issues, focusing on suspicious login attempts and unusual behavior patterns.

Splunk > enterprise Apps ▾

Administrator 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Q

Home Content ▾ Analytics Advisor ▾ Security Operations ▾ Data ▾ Advanced ▾ Documentation ▾ Setup ▾ Splunk Security Essentials

New Search

source="ssh.log.gz" host="Kripesh" sourcetype="SSH\_Log"

7,143 events (before 9/12/24 2:55:44.000 PM) No Event Sampling ▾

Events (7,143) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect 1 millisecond per column

List ▾ ✓ Format 20 Per Page ▾

< Hide Fields All Fields

	i	Time	Event
SELECTED FIELDS			
a host 1		9/12/24 2:55:39.000 PM	1332016697.210000 CyEd9z3v2QM9a1Bfbfd 192.168.202.69 37012 192.168.28.253 22 undetermined INBOUND SSH-2.0-OpenSSH_5.0 SSH-2.0-OpenSSH_4.5 - - - - - host = Kripesh   index = main   linecount = 1   punct = .tt...tt...ttt...t-.-t-t-t-t-   source = ssh.log.gz   sourcetype = SSH_Log   splunk_server = Kripesh   timestamp = none
a index 1			
# linecount 1			
a punct 19			
a source 1			
a sourcetype 1			
a splunk_server 1			
a timestamp 1			
+ Extract New Fields			

Dashboards | Splunk 9.3.0 Search | Splunk 9.3.0 ChatGPT

New Search

index=\_\* OR sourcetype=SSH\_Log

7,143 events (9/11/24 3:00:00.000 PM to 9/12/24 3:02:46.000 PM) No Event Sampling ▾

Events (7,143) Patterns Statistics Visualization

Format Timeline ▾ – Zoom Out + Zoom to Selection X Deselect 1 hour per column

List ▾ ✓ Format 20 Per Page ▾

< Hide Fields All Fields

	i	Time	Event
SELECTED FIELDS			
a host 1		9/12/24 2:55:39.000 PM	1332016697.210000 CyEd9z3v2QM9a1Bfbfd 192.168.202.69 37012 192.168.28.253 22 undetermined INBOUND SSH-2.0-OpenSSH_5.0 SSH-2.0-OpenSSH_4.5 - - - - - host = Kripesh   index = main   linecount = 1   punct = .tt...tt...ttt...t-.-t-t-t-t-   source = ssh.log.gz   sourcetype = SSH_Log   splunk_server = Kripesh   timestamp = none
a index 1			
# linecount 1			
a punct 19			
a source 1			
a sourcetype 1			
a splunk_server 1			
a timestamp 1			
INTERESTING FIELDS			
a direction 1			
a dst_ip 58			
# dst_port 1			
a result 3			
a src_ip 49			
# src_port 100+			
+ Extract New Fields			

Fig: SSH Log after applying Data Parsing

**New Search**

index=\_\* OR index=\_\* sourcetype=SSH\_Log | command = ssh.py

✓ 1 event (9/11/24 3:00:00.000 PM to 9/12/24 3:14:26.000 PM) No Event Sampling ▾ Job ▾ II ■ ▾ Smart Mode ▾

Events (1) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ Format 20 Per Page ▾

Time	Event
9/12/24 2:55:39.000 PM	1332014883.950000 C8Bw6F2JD1ASztOZh 192.168.202.102 4380 192.168.21.253 22 undetermined INBOUND SSH-1.5-ssh.py SSH-1.99-OpenSSH_4.5 - - - - - - command = ssh.py   host = Kripesh   index = main   linecount = 1   punct = .tt...ttt...t-.-t-t-t-t-   source = ssh.log.gz   sourcetype = SSH_Log   splunk_server = Kripesh   timestamp = none

◀ Hide Fields ▶ All Fields

**SELECTED FIELDS**

- a command 1
- a host 1
- a index 1
- # linecount 1
- a punct 1
- a source 1
- a sourcetype 1
- a splunk\_server 1
- a timestamp 1

**INTERESTING FIELDS**

- a direction 1
- a dst\_ip 1
- # dst\_port 1
- a result 1
- a src\_ip 1
- # src\_port 1

index=\_\* OR index=\_\* sourcetype=SSH\_Log result=failure "SSH-2.0-Nmap-SSH2"

✓ 487 events (9/11/24 3:00:00.000 PM to 9/12/24 3:18:58.000 PM) No Event Sampling ▾ Job ▾ II ■ ▾ Smart Mode ▾

Events (487) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ Format 20 Per Page ▾

Time	Event
9/12/24 2:55:39.000 PM	1332014961.000000 C9Xd7rlrqMvxdE7h 192.168.202.136 56568 192.168.21.203 22 failure INBOUND SSH-2.0-Nmap-SSH2-Hostkey SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - - - host = Kripesh   index = main   linecount = 1   punct = .tt...ttt...t-.-t-t-t-t-   source = ssh.log.gz   sourcetype = SSH_Log   splunk_server = Kripesh   timestamp = none
9/12/24 2:55:39.000 PM	1332014961.040000 ChSj9guzUhPolkCa6 192.168.202.136 60076 192.168.21.102 22 failure INBOUND SSH-2.0-Nmap-SSH2-Hostkey SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - - - host = Kripesh   index = main   linecount = 1   punct = .tt...ttt...t-.-t-.-t-t-t-t-   source = ssh.log.gz   sourcetype = SSH_Log   splunk_server = Kripesh   timestamp = none
9/12/24 2:55:39.000 PM	1332014960.620000 C4wXMJ3QXdi8LqQZZc 192.168.202.136 56543 192.168.21.203 22 failure INBOUND SSH-2.0-Nmap-SSH2-Hostkey SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - - - host = Kripesh   index = main   linecount = 1   punct = .tt...ttt...t-.-t-.-t-t-t-t-   source = ssh.log.gz   sourcetype = SSH_Log   splunk_server = Kripesh   timestamp = none
9/12/24 2:55:39.000 PM	1332014960.630000 CmS3YU3t21Hb2B7Bfc 192.168.202.136 60051 192.168.21.102 22 failure INBOUND SSH-2.0-Nmap-SSH2-Hostkey SSH-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - - - host = Kripesh   index = main   linecount = 1   punct = .tt...ttt...t-.-t-.-t-t-t-t-   source = ssh.log.gz   sourcetype = SSH_Log   splunk_server = Kripesh   timestamp = none
9/12/24 2:55:39.000 PM	1332013311.980000 Cas6HxImtj5RYZk56 192.168.202.141 5738 192.168.229.101 22 failure INBOUND SSH-2.0-Nmap-SSH2-Hostkey SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1 - - - - - - host = Kripesh   index = main   linecount = 1   punct = .tt...ttt...t-.-t-.-t-t-t-t-   source = ssh.log.gz   sourcetype = SSH_Log

◀ Hide Fields ▶ All Fields

**SELECTED FIELDS**

- a host 1
- a index 1
- # linecount 1
- a punct 7
- a source 1
- a sourcetype 1
- a splunk\_server 1
- a timestamp 1

**INTERESTING FIELDS**

- a direction 1
- a dst\_ip 54
- # dst\_port 1
- a result 1
- a src\_ip 12
- # src\_port 100+

+ Extract New Fields

Fig: Investigating suspicious Events

## 2.4 Dashboard Creation

A custom dashboard was created in Splunk to provide a visual representation of the collected log data. This dashboard facilitated easy access to critical information and trends.

The screenshot shows the Splunk search interface with a search bar at the top containing the query: `index=_* OR index=_source sourcetype=SSHLog _resultFailure`. Below the search bar, there are tabs for Events (487), Patterns, Statistics, and Visualization. A modal window titled "Your Dashboard Panel Has Been Created" is displayed, stating: "The panel has been created and added to ssh\_attempt\_suspicious. You may now view the dashboard." At the bottom of the modal is a green "View Dashboard" button. The main search results table shows several log entries with columns for Time, Event, and various log fields like host, index, source, and source type.

The screenshot shows the Splunk Apps page with a search bar and a sidebar listing various apps: Search & Reporting, Splunk Secure Gateway, Splunk Security Essentials, Upgrade Readiness App, and a link to Find more apps. The main content area displays a list of dashboards under the heading "Recently viewed". The "SSH Attempt Suspicious" dashboard is listed first, along with other dashboards like Home, Data Inventory, Simple Search, Clear Logs Event, and Secure Gateway Status Dashboard. Each dashboard entry includes columns for Name, Owner, Updated, App, and Sharing.

The screenshot shows the "SSH Attempt Suspicious" dashboard with a title bar and a search bar. The main content area is a table with columns for Time, Event, and various log fields. The table lists multiple log entries from different dates and times, each detailing an SSH attempt event with details like host, source, and source type. The table includes buttons for Edit, Export, and three dots.

Fig: Dashboard Created

## 2.5 Reporting, Scheduling and Alerting

After Dashboard creation, the next step involved creating a comprehensive report based on the analysis, scheduling regular reports for continuous monitoring, and setting up alerts to notify of any suspicious activities or security events in real-time.

The screenshot shows two interface components related to report creation and management.

**Save As Report Dialog:**

- Title:** SSH Failure Attempts Several Times
- Description:** optional
- Content:** Events
- Time Range Picker:** Yes (selected)
- Buttons:** Cancel, Save

**Reports List:**

- Header:** Reports, 13 Reports, Filter, Search icon
- Table Headers:** Title, Actions, Next Scheduled Time, Owner, App, Sharing
- Items:**
  - Generate Data Availability ML Model for Latency
  - Generate Datamodels Lookup
  - Generate Local Saved Search Lookup
  - Generate MITRE Data Source Lookup
  - Generate MITRE Detections Lookup
  - Generate MITRE Enterprise List
  - Generate MITRE Environment Count
  - Generate MITRE Threat Group Lookup
  - Generate STRT Macros to Data Source Categories Lookup
  - Generate STRT Macros to Data Source Categories Lookup - Backup
  - Products and the Content Mapped to Them
  - SSH Attempt Failed** (selected item, highlighted with a blue border)
- Details for SSH Attempt Failed:**
  - List of all failed SSH Attempt
  - Creator ..... Created by Search.
  - App ..... Splunk\_Security\_Essentials
  - Schedule ..... Not scheduled. Edit
  - Actions ..... 0 Actions
  - Acceleration ..... Disabled. Edit
  - Permissions ..... Private. Owned by kacharya. Edit
  - Modified ..... Sep 12, 2024 3:36:14 PM
  - Embedding ..... Disabled. Edit

Fig: Report Created

**Edit Schedule**

**⚠ Scheduling this report results in removal of the time picker from the report display.**

Report	SSH Attempt Failed
Schedule Report	<input checked="" type="checkbox"/> <a href="#">Learn More</a>
Schedule	Run every week ▾
On	Monday ▾ at 6:00 ▾
Time Range	Yesterday ▶
Schedule Priority ?	Default ▾
Schedule Window ?	No window ▾
<b>Trigger Actions</b>	
<a href="#">+ Add Actions ▾</a>	

---

✓ **SSH Attempt Failed**

Open In Search Edit ▾ None kacharya Splunk\_Security\_Essentials Private

List of all failed SSH Attempt

Creator ..... Created by Search.  
App ..... Splunk\_Security\_Essentials  
Schedule ..... Weekly, Monday at 6:00. Edit  
Actions ..... 0 Actions  
Acceleration ..... Disabled. Edit  
Permissions ..... Private. Owned by kacharya. Edit  
Modified ..... Sep 12, 2024 3:43:38 PM  
Embedding ..... Disabled. Edit

Fig: Scheduling a Report

**Save As Alert**

**Settings**

Title	SSH failed Attempt Multiple Times	frames framed framework
Description	List of all failed SSH Attempt in same time frame	
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 ?	<input type="checkbox"/>	

Fig: Creating an Alert

## 2.6 Continuous Monitoring

The last step is to implement continuous monitoring, ensuring that logs are regularly analyzed, reports are generated, and alerts are triggered automatically to detect and respond to any ongoing or emerging security threats.

## 3.Learning Resources

- **LetsDefend Learning Platform:** Provided hands-on training and practical knowledge on using Splunk for SIEM.
- **Rajneesh Gupta YouTube Channel:** Offered tutorials and insights into Splunk functionalities and best practices.

## 4. Conclusion

The project successfully demonstrated the capabilities of Splunk as a SIEM tool in a home lab setting. Through installation, log management, data analysis, and dashboard creation, valuable insights into security monitoring and incident response were gained. The use of SPL and alerting mechanisms enhanced the ability to detect and address suspicious activities effectively.