Implementation of Windows Log Monitoring using Splunk & VirusTotal

Learning - Outcomes

Introduction

- Splunk overview
- Virus Total overview
- Purpose of integration

Objectives

- Collect Windows logs
- Detect malicious hashes
- Integrate Virus Total lookup

Setup

- Install & access Splunk
- Add Windows Event Logs (Application & System)
- Install Virus Total app & API key

What is Splunk

Splunk is a powerful platform used to collect, index, and analyze machine-generated data from various sources in real time. It helps organizations monitor, search, and visualize logs to identify errors, security threats, and operational issues quickly. By turning raw log data into actionable insights, Splunk improves visibility, decision-making, and overall system performance.

What is Virus Total

Virus Total is an online service that analyzes files, URLs, and hashes to detect viruses, malware, and other security threats. It uses multiple antivirus engines and threat intelligence tools to check if a file or link is malicious. Security analysts use it to verify and investigate suspicious files or activities.

Purpose of Integration

The purpose of integrating Virus Total with Splunk is to enhance threat detection by identifying malicious hashes in log data. Splunk collects and indexes system logs, while Virus Total provides verdicts (malicious, clean, suspicious) for file hashes. This integration helps security analysts quickly detect and investigate potential threats within their environment using real-time log data combined with threat intelligence.

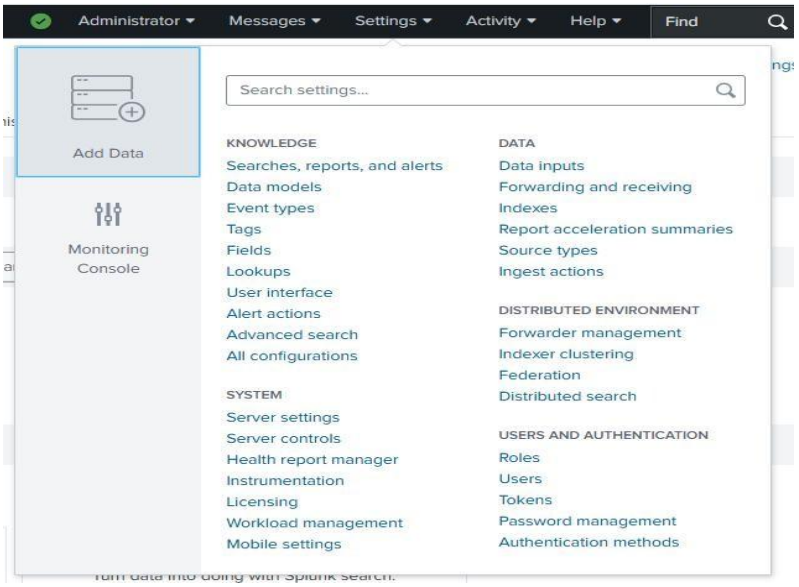
Setup Guide:

Step No. 1:

First download the Splunk SIEM Tool from the main page of Splunk and assign your credentials. Then a interface would appear **"Enter Username"** and **"Password"** that you had assigned earlier. Press Enter to proceed.

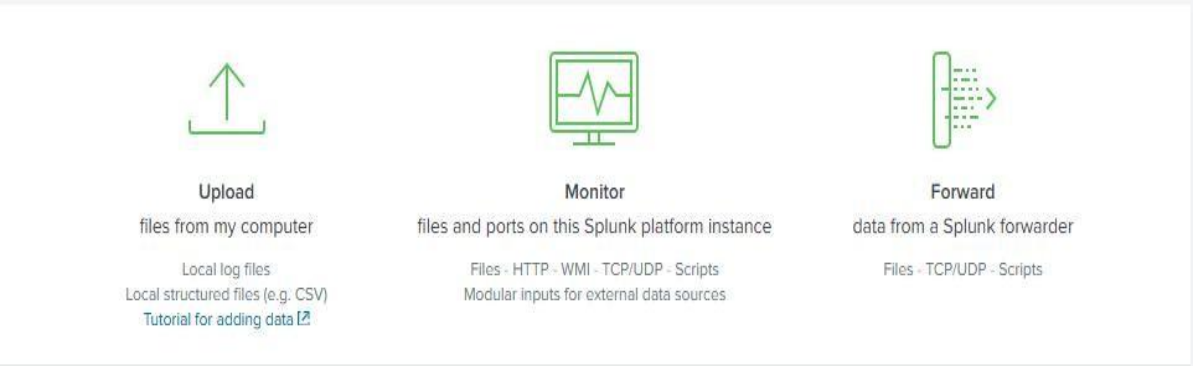
Step No. 2:

Click the Settings Option then "Add Data" option will appear select it.



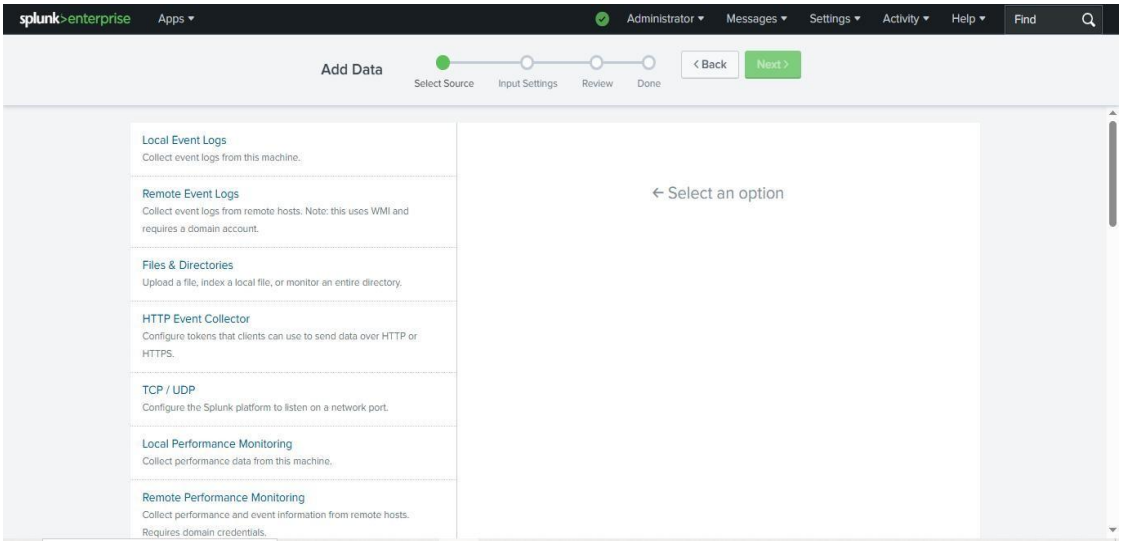
Step No. 3:

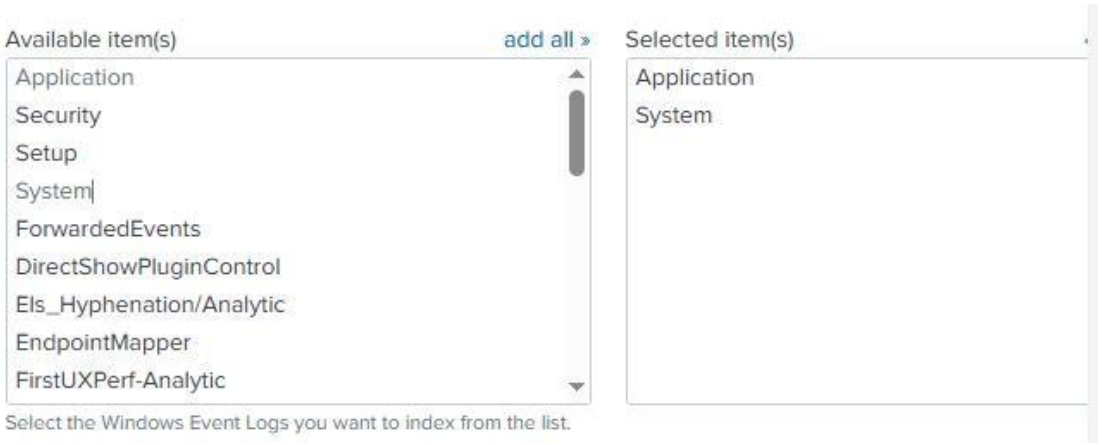
Scroll down and choose the Monitor Option.



Step No. 4:

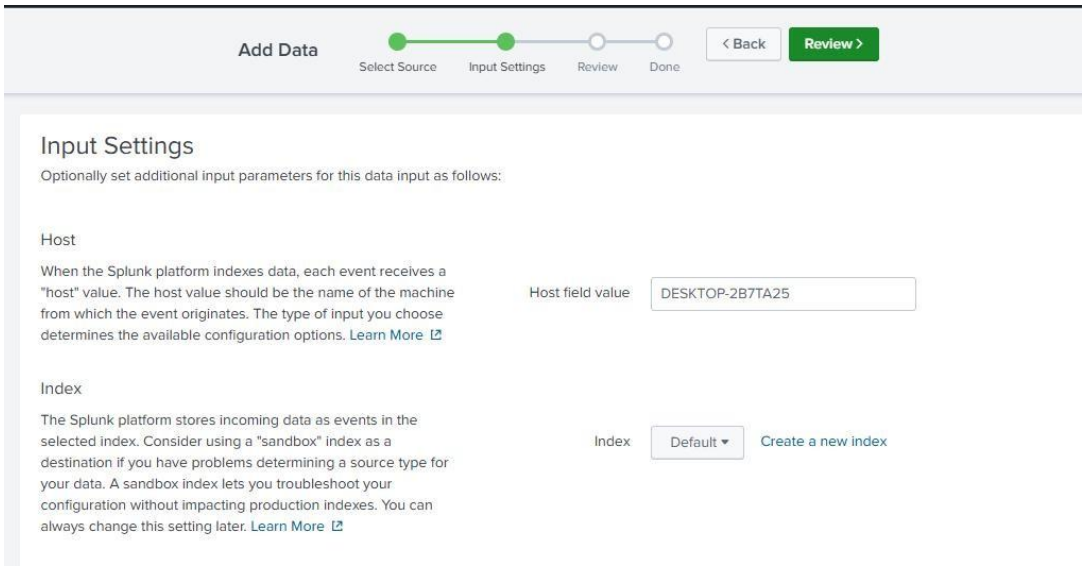
From the sidebar, select the "Event Logs" option and choose the two logs: System and Application, as we aim to monitor these logs.





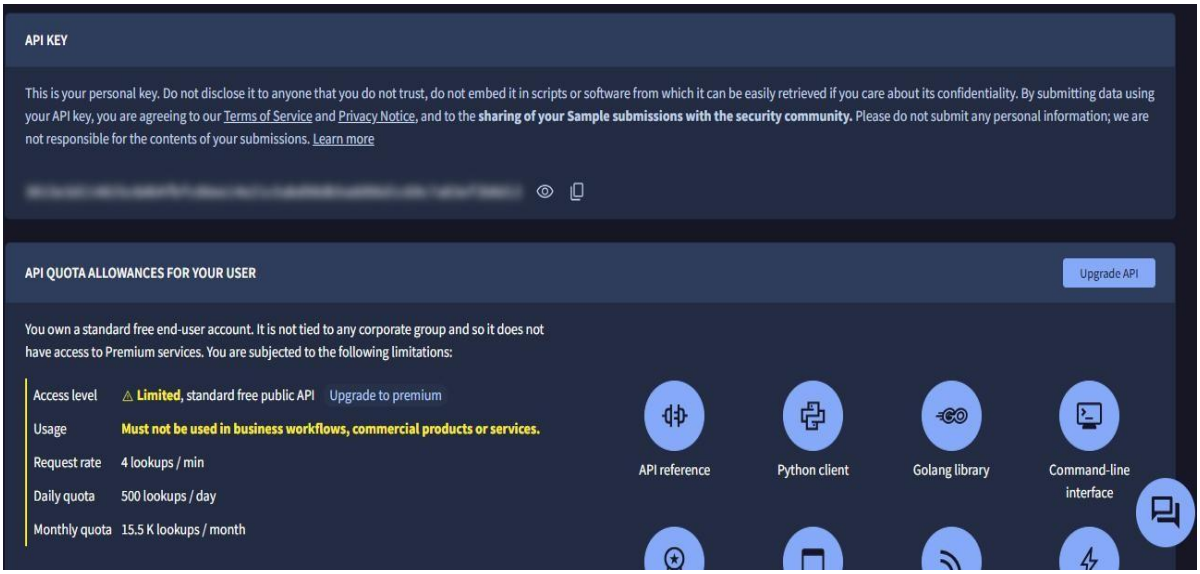
Step No. 5:

Click Next. The Host field value and Index options will appear. Splunk automatically assigns a default host and index at this step, so you usually don't need to change them manually.



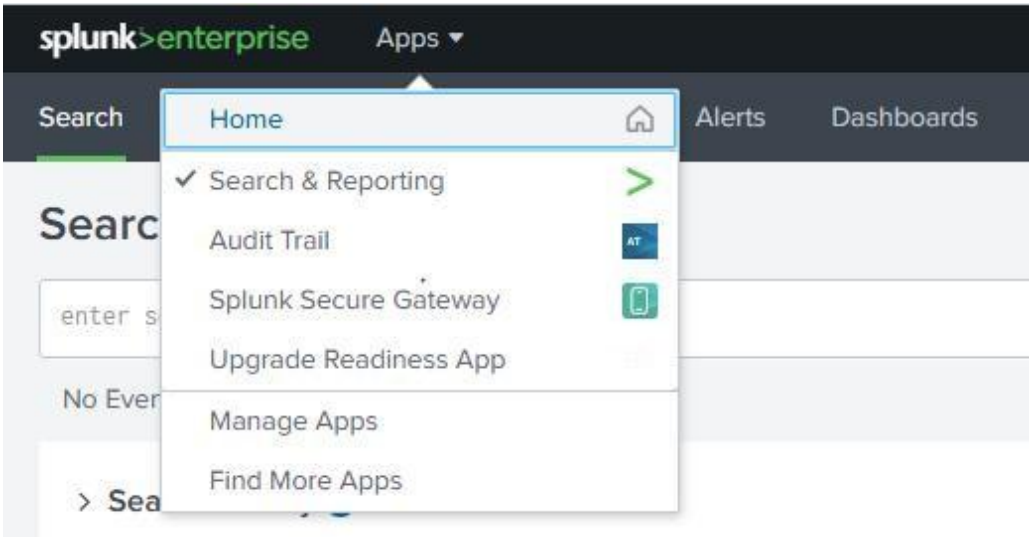
Step No. 6:

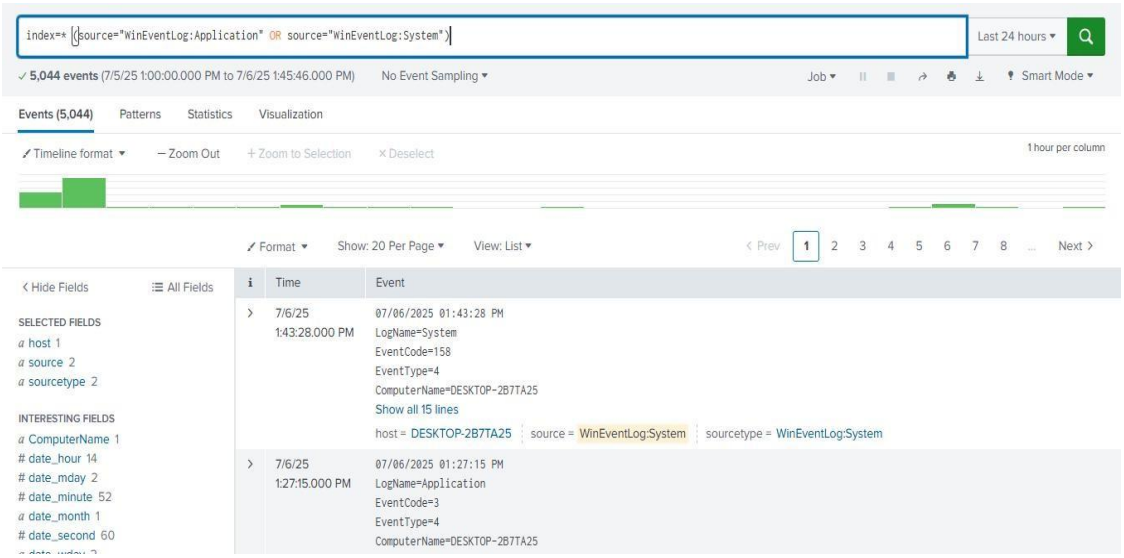
The next step is to open VirusTotal in your browser and sign in to your account. Then, click on your profile icon at the top-right corner to open the menu. From the menu, select the **API Key** option and copy your API key, as it is required to integrate the Virus Total app with Splunk.



Step No. 7:

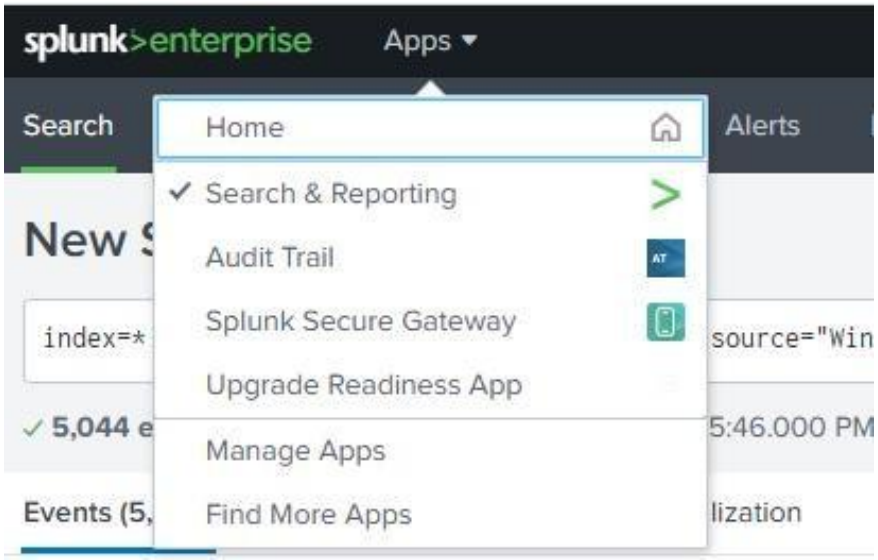
After saving the API key in the Virus Total app setup, go to the Apps menu and open the Search & Reporting app. In the search bar, run a query **(e.g., index=* sourcetype=WinEventLog:*)** to view your Windows logs in the results panel.

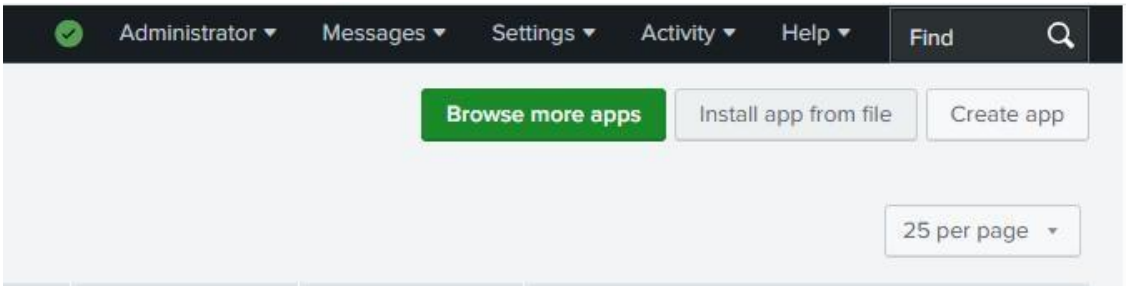




Step No. 8:

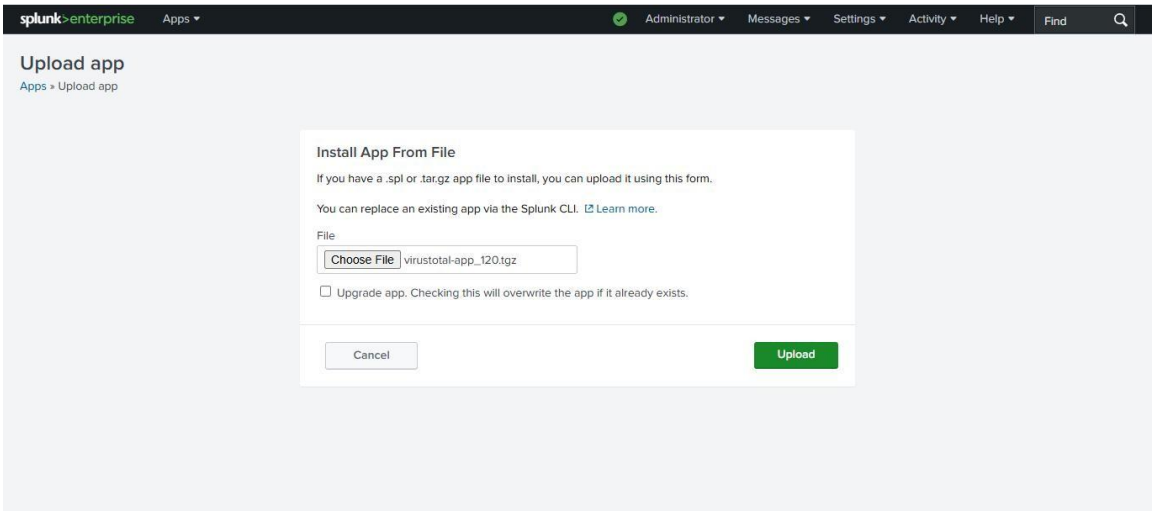
Go to Apps > Manage Apps > Install app from file, upload the downloaded Virus Total app file from Splunk-base, and complete the setup by saving your API key.





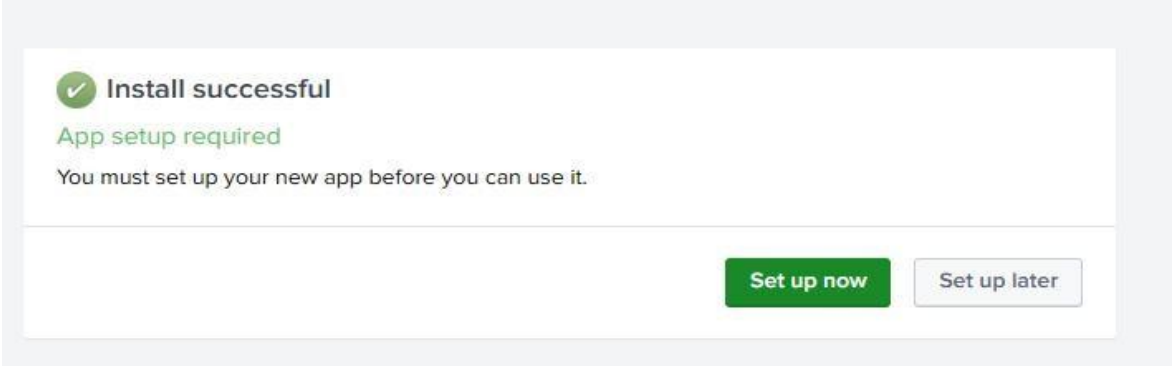
Step No. 9:

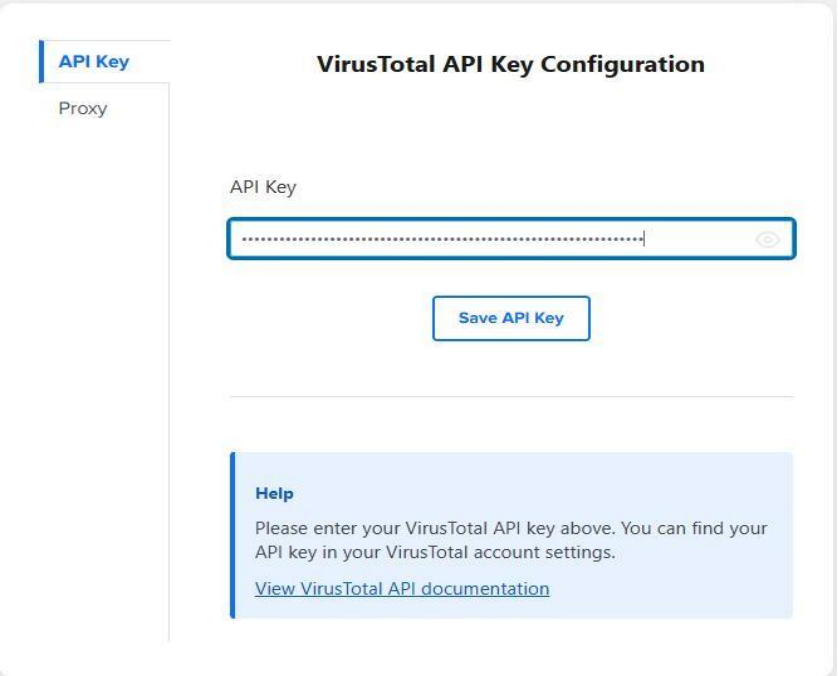
Browse & select the downloaded Virus Total app file. Click **Upload**.After install completes → If it says “App setup required”, click **Set up now**. Enter your Virus Total API key there & save.



Step No. 10:

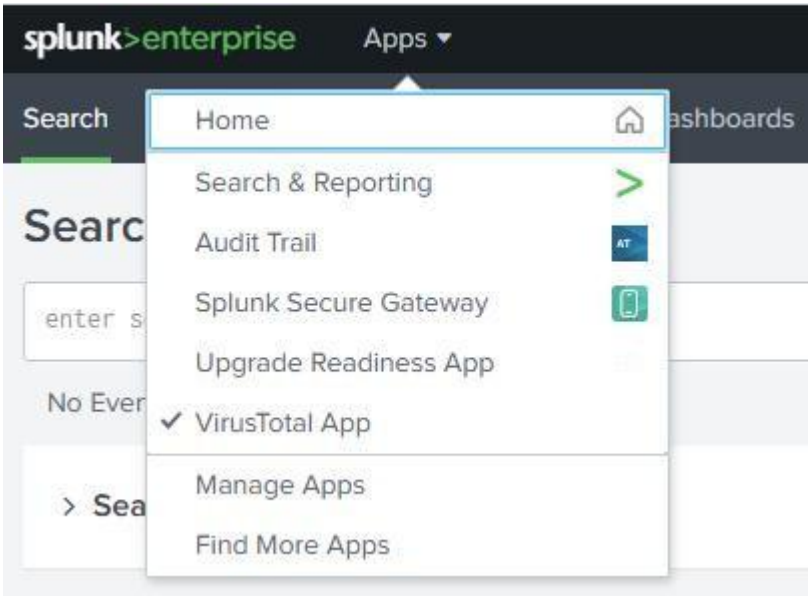
Click **Set up now**. Enter your Virus Total API key there & save.





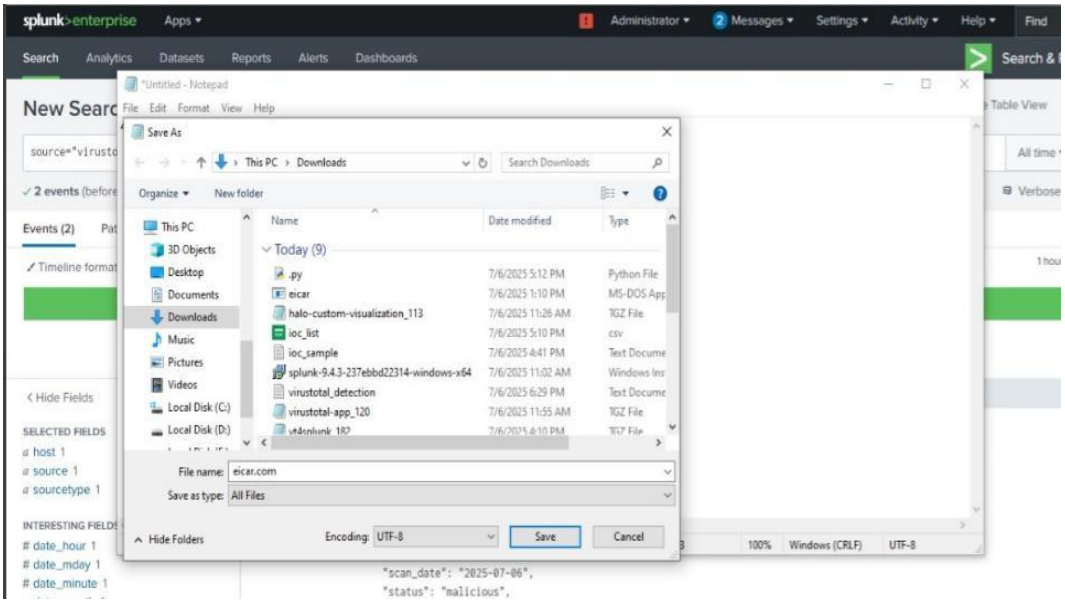
Step No. 11:

Virus Total has been successfully integrated into Splunk.



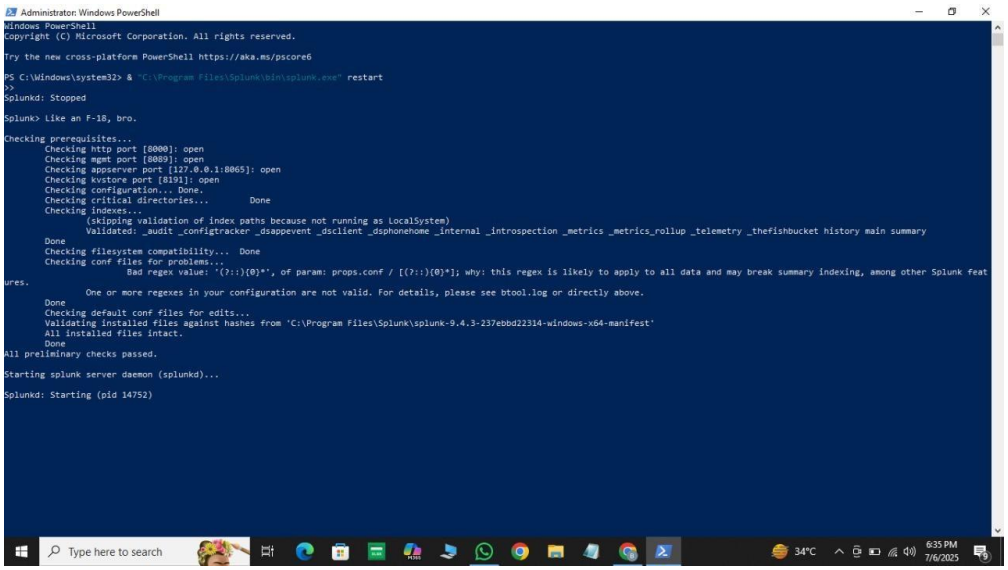
Step No. 12:

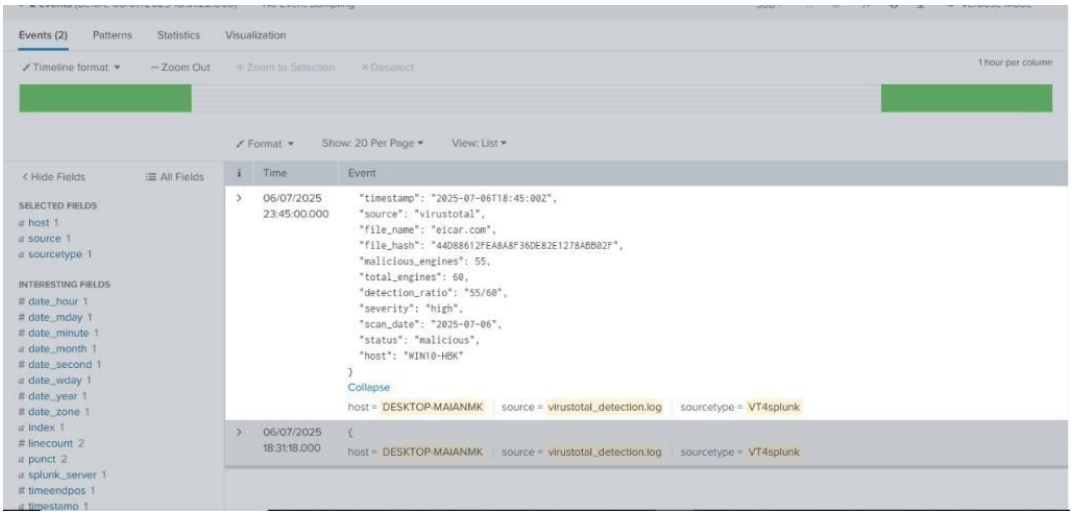
Now we are going to try a sample Malware file on Splunk Virus Total.And we have saved this file with the name **eicar.com** in the bin section of Splunk.



Step No. 13:

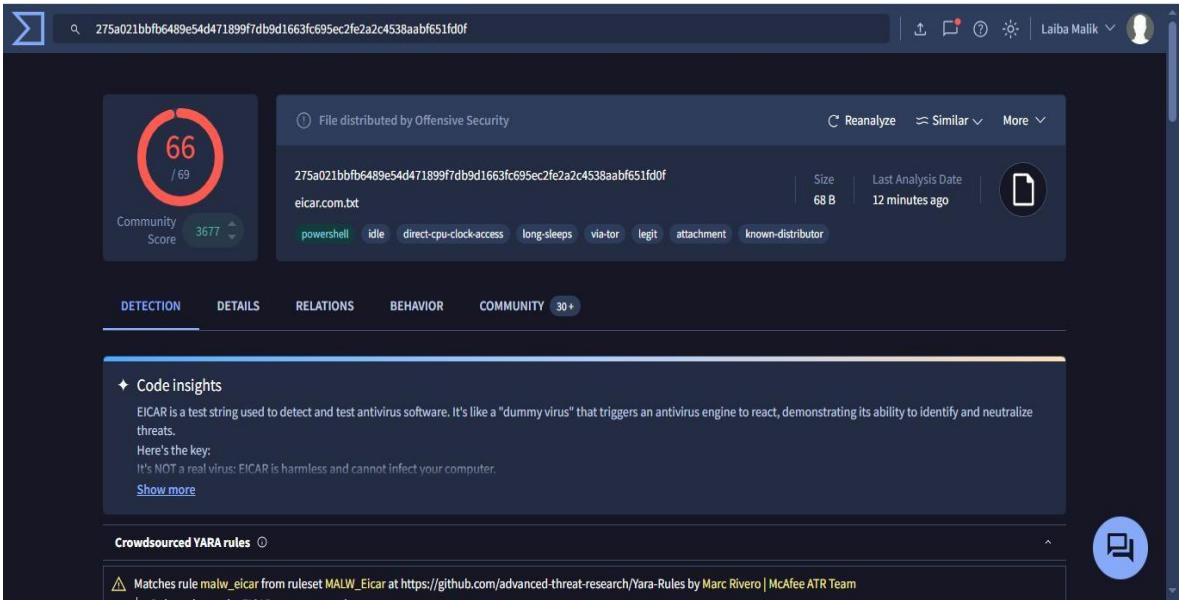
Restart Splunk using Power-shell, and the Virus Total app will display the results in Splunk.





Step No. 14:

For additional verification, the hash was also queried directly on VirusTotal, and the corresponding results are presented below.



---------- THE END----------