o

Virus Total Integration with Splunk

Collection of Window logs.

Report Made by:

Arshman Abbas

Linkdin Profile link:

www.linkedin.com/in/arshman-abbas-89a95732a

Learning Objectives

Introduction :

- Splunk
- Virus Total
- Why we Integrated (Purpose)

Objectives :

- Collect Windows logs
- Detect malicious hashes
- Integrate Virus Total lookup
- Install & access Splunk
- Add Windows Event Logs (Application,System)
- Install Virus Total app and upload in Splunk for Integration.
- Monitor Results

What is Splunk?

Splunk is a powerful tool that collects, processes, and analyzes machine-generated data in real time. It helps organizations monitor systems, troubleshoot issues, detect security threats, and improve performance by turning raw log data into useful insights. With its search and visualization features, Splunk enables faster decision-making and greater visibility into IT environments.

What is VirusTotal?

VirusTotal is an online platform that scans files, URLs, and file hashes to detect malware and other threats. It checks the input against a wide range of antivirus engines and threat intelligence sources to determine if it's safe or harmful. Cybersecurity professionals use VirusTotal to investigate and confirm whether a file or activity is potentially malicious**.**

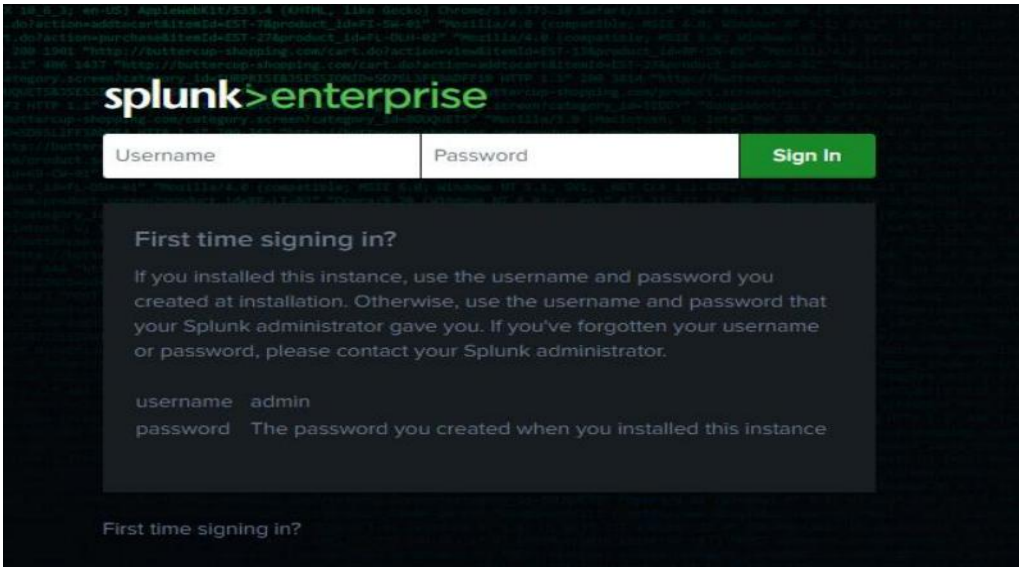
Purpose of Integrating Virus Total with Splunk

Integrating VirusTotal with Splunk strengthens threat detection by automatically checking file hashes found in log data. While Splunk collects and indexes log information, VirusTotal adds threat intelligence by labeling those hashes as safe, suspicious, or malicious. This combination enables security analysts to quickly spot and investigate threats in real time using enriched, actionable data.

WORK SET UP

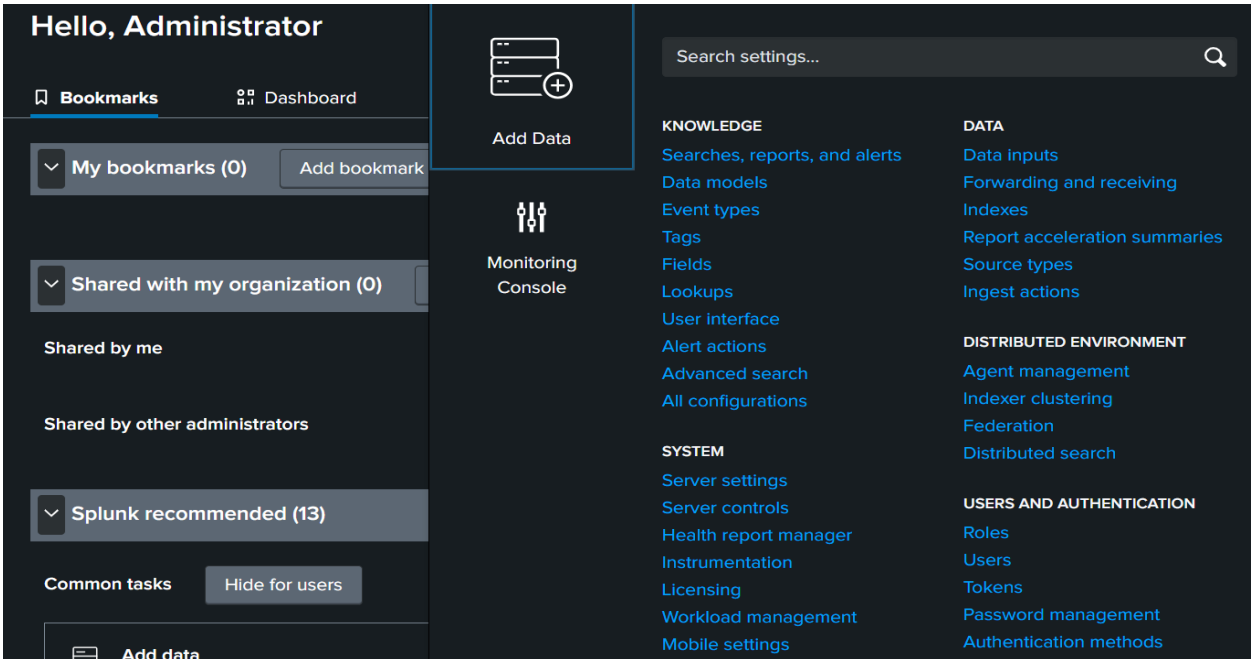
Step 1:

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



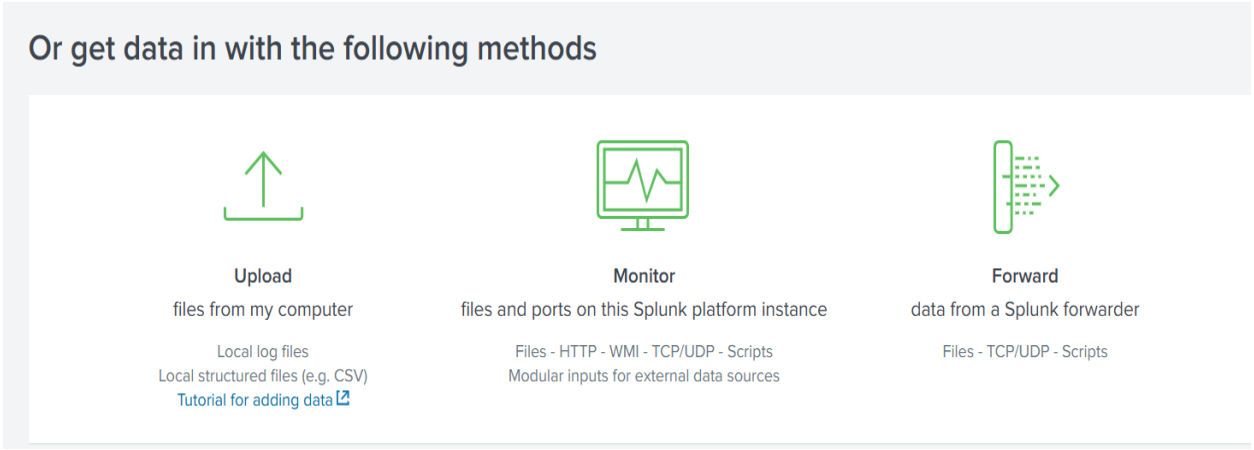
Step 2:

Now click the Settings Option in Splunk then "**Add Data"** option will appear select this.



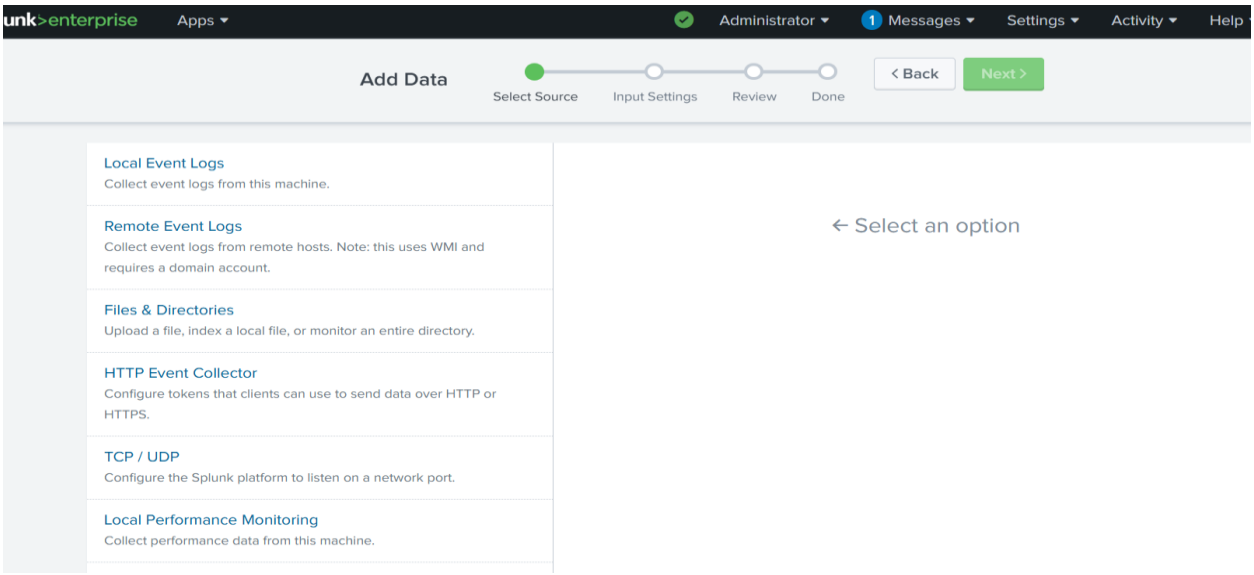
Step 3:

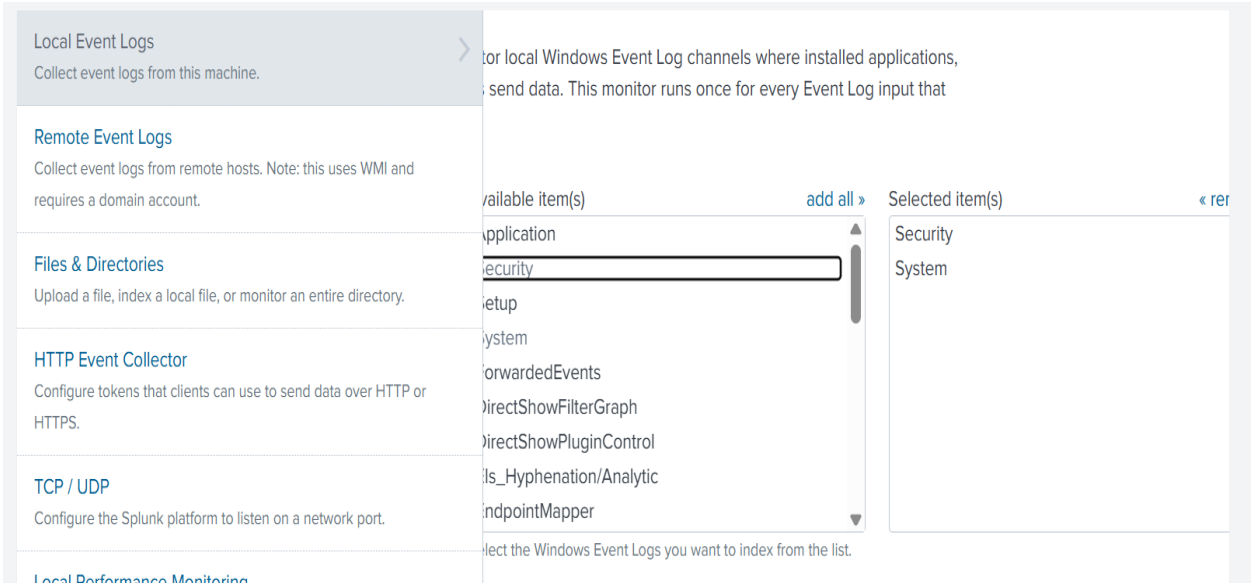
Scroll down and choose the **Monitor**.



Step 4:

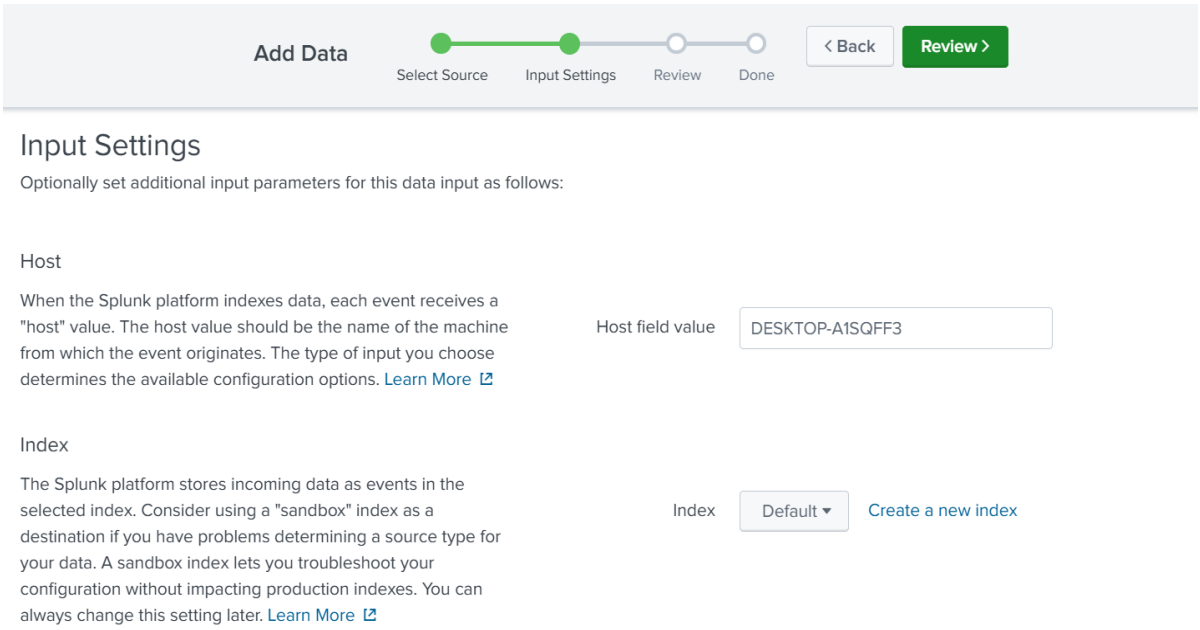
From the sidebar, select the " **Local Event Logs"** option and choose two logs: System and Application logs.





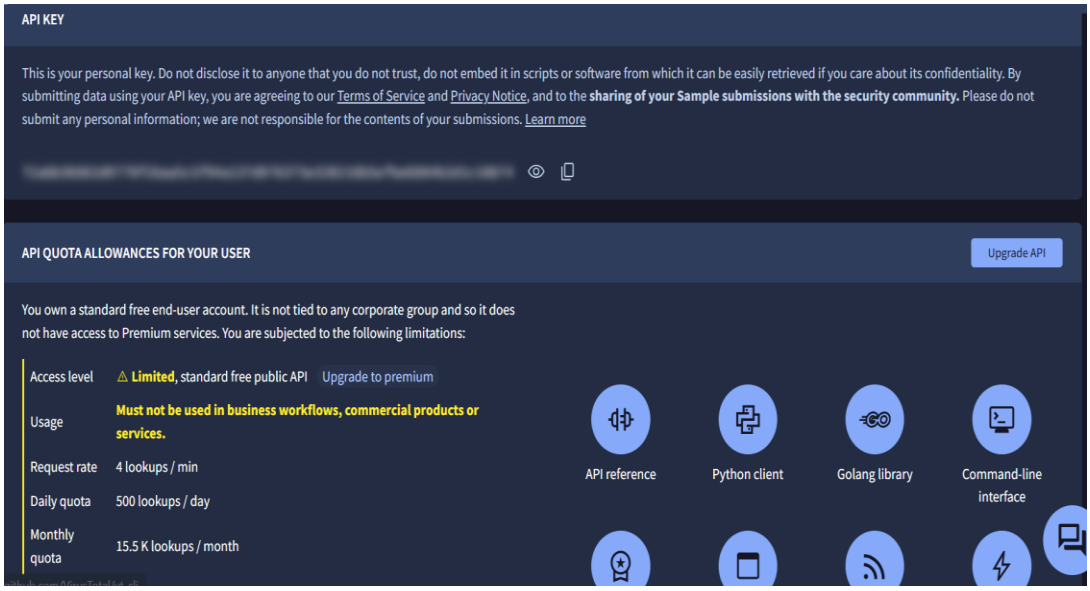
Step 5:

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



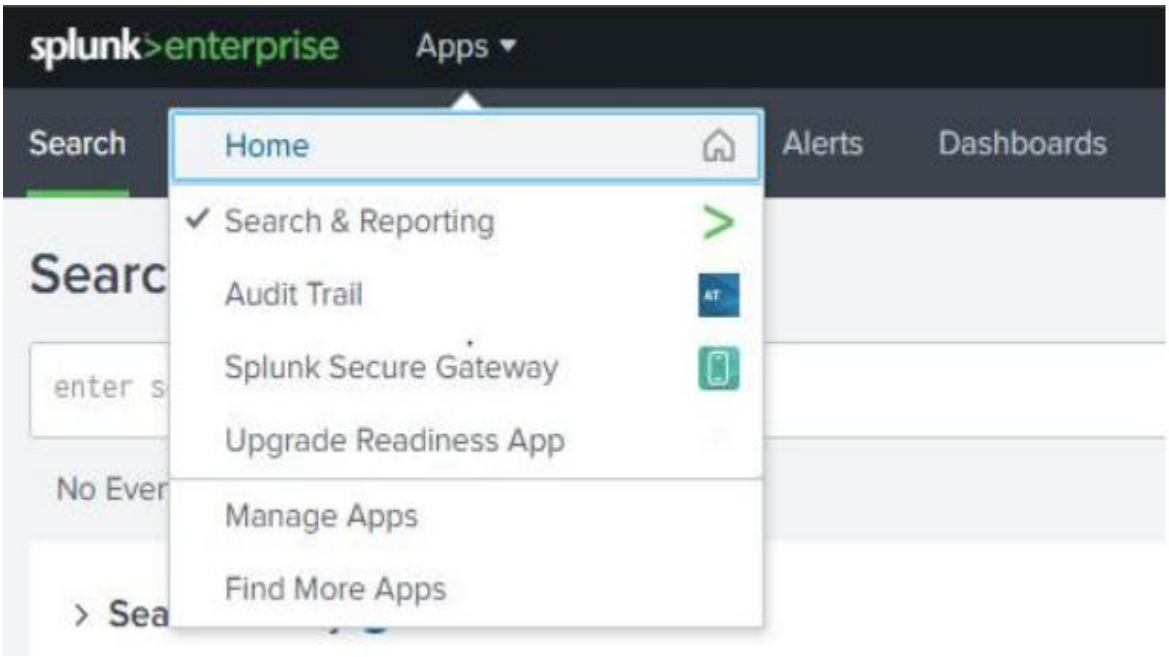
Step 6:

Open VirusTotal in your browser and sign into your account.Then, click on your profile icon and then select **API key**. Copy the API Key.



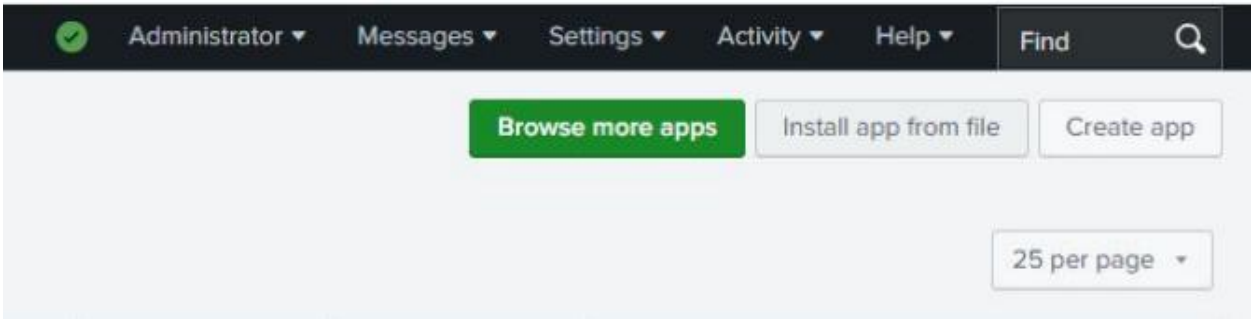
Step 7:

After saving the API key in the VirusTotal app setup, navigate 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.



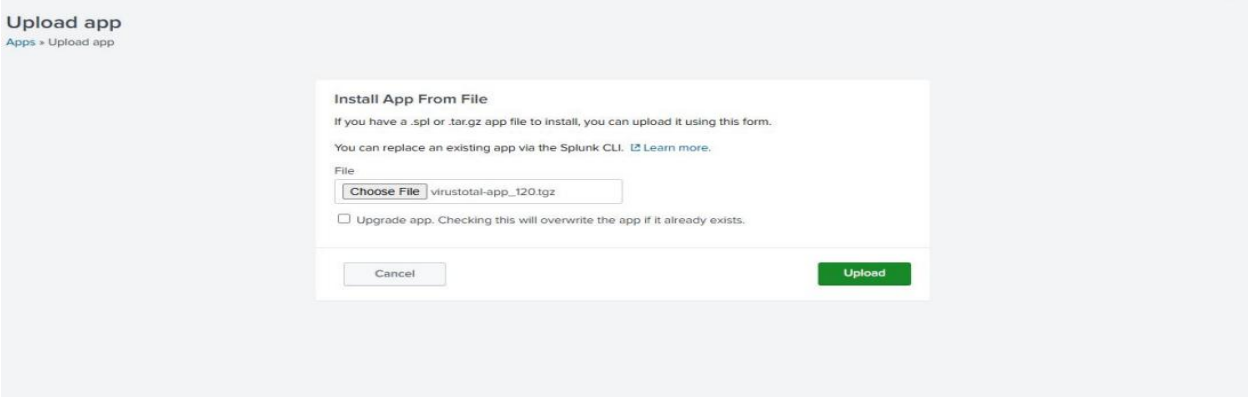
Step 8:

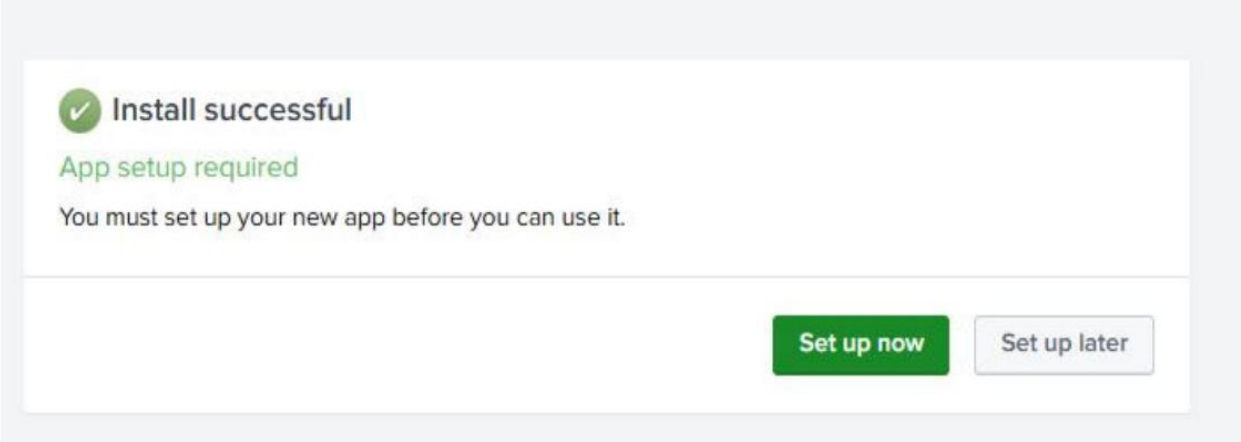
Download the **Virus total app** from Splunk base. Then Go to **Apps > Manage Apps > Install app from file**, upload the downloadedVirusTotal app file from Splunk-base, and complete the setup by saving your API key



Step 9:

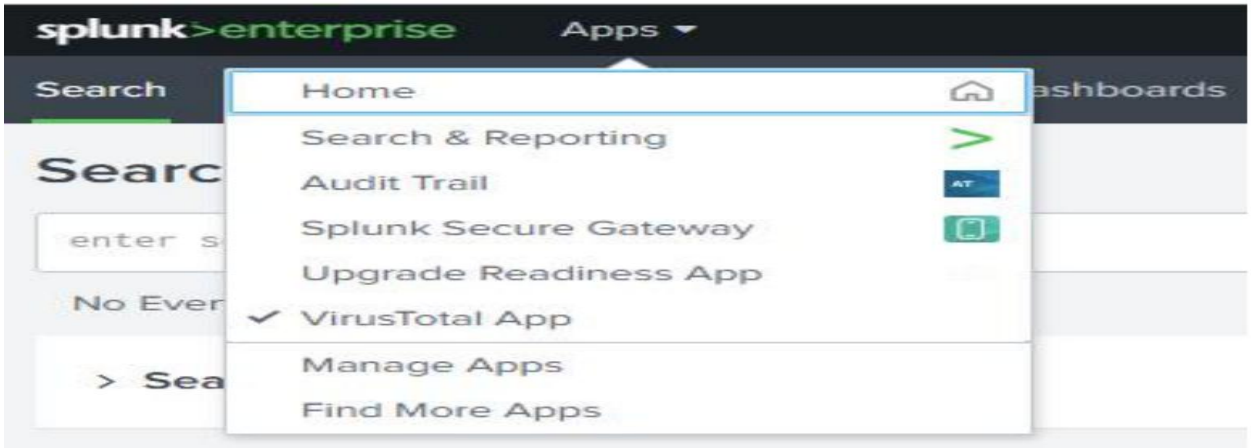
Select the downloaded Virus Total app file. Click Upload.After the install completes If it says “App setup required”, click Set up now. Enter yourVirusTotal API key there and save It .After this Click Set up now.





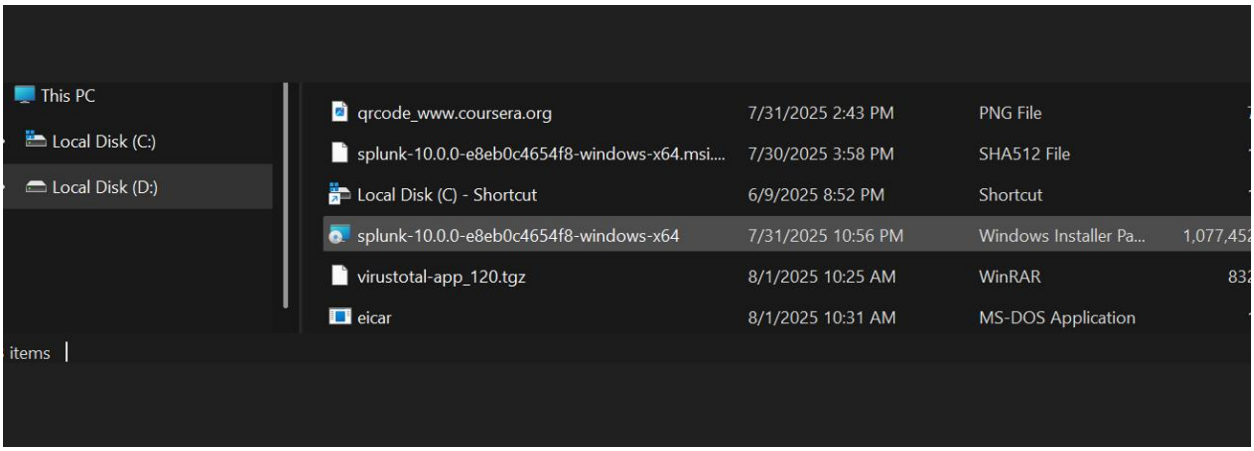
Step 10:

Now Virus total is Integrated successfully with Splunk. You can see it in the home Section.



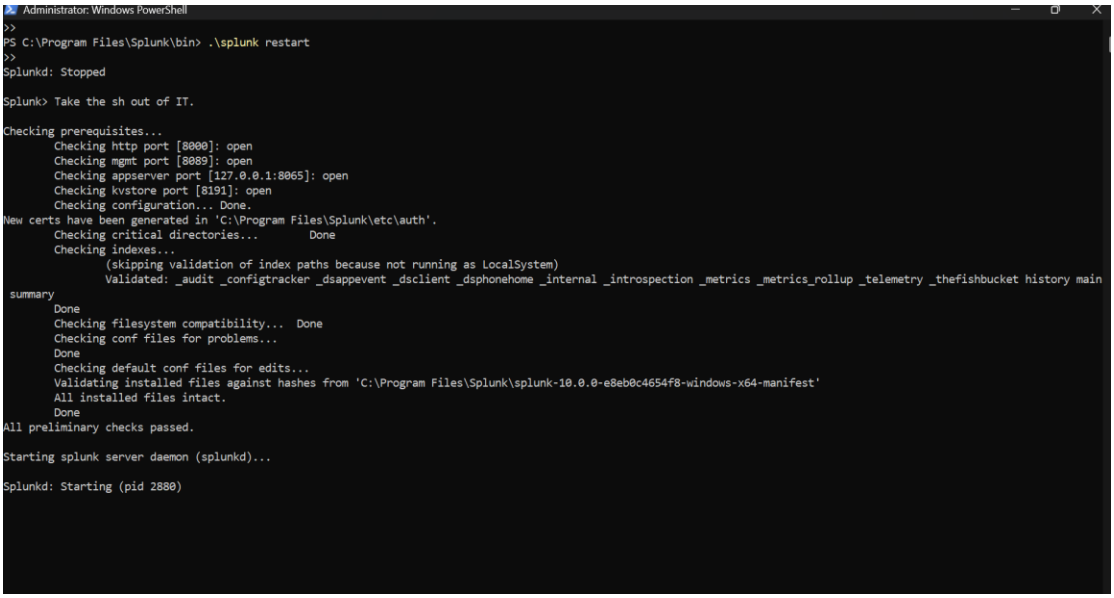
Step 11:

Test the Sample Malware file **Eicar(easily downloadable from internet)** to check our Integration.



Step 12:

Restart Splunk using **powershell** and then interpret Virus total results in Splunk.



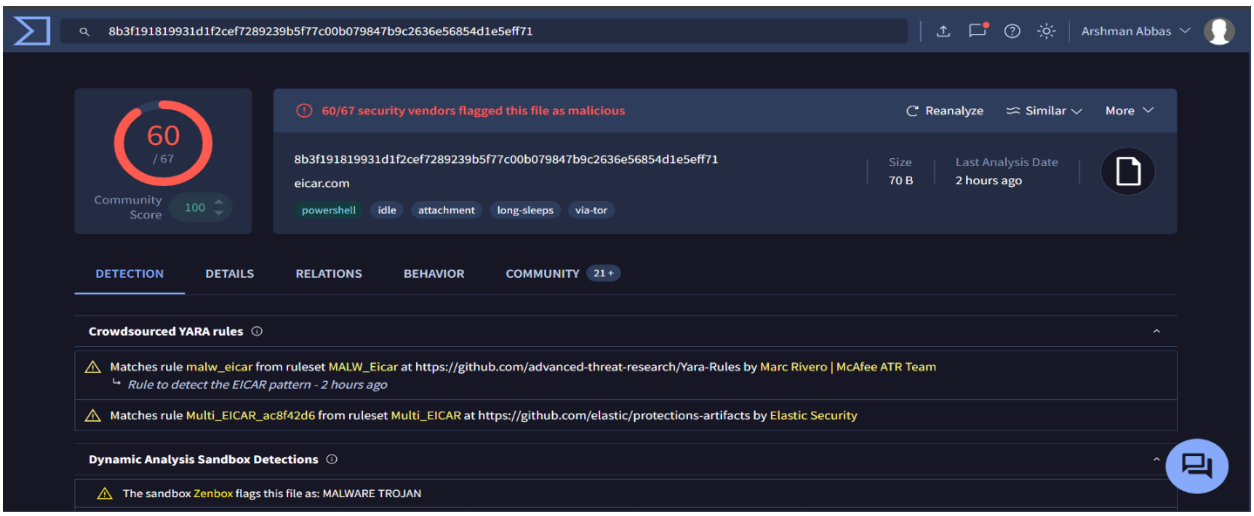
Here the results are visible in Splunk:


```
"source": "virustotal",
"file_name": "eicar.com",
"file_hash": "44D88612FEA8A8F36DE82E1278ABB02F",
"malicious_engines": 55,
"total_engines": 60,
"detection_ratio": "55/60",
"severity": "high",
"scan_date": "2025-07-06",
"status": "malicious",
"host": "WIN10-HBK"
}
Collapse
```


host = DESKTOP-MAIANMK | source = virustotal_detection.log | sourcetype = VT4splunk

Step 13:

We also queried hash on Virus total for Additional Verificaton.



THE END