



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

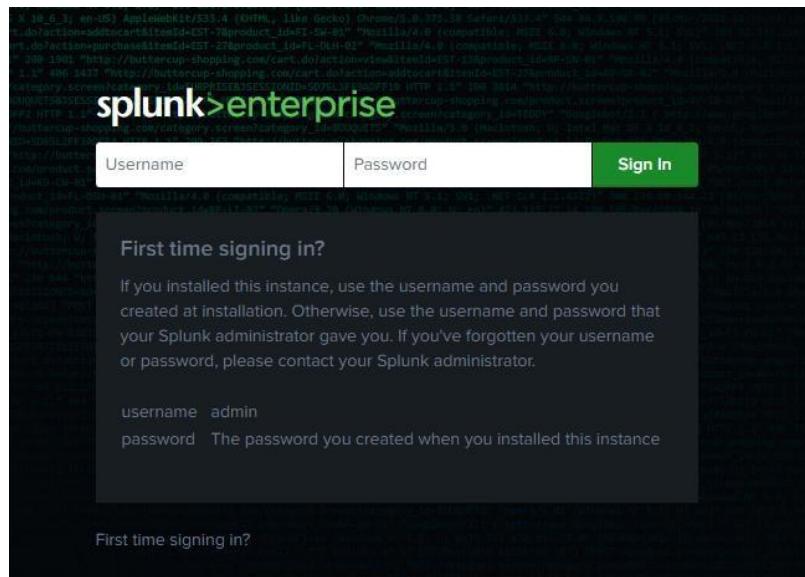
The purpose of integrating Virus Total with Splunk is to enhance threat detection by identifying malicious hashes in log data. Splunk collects and indexes system logs, while Virus Total provides verdicts (malicious, clean, suspicious) for file hashes. This integration helps security analysts quickly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



Setup Guide:

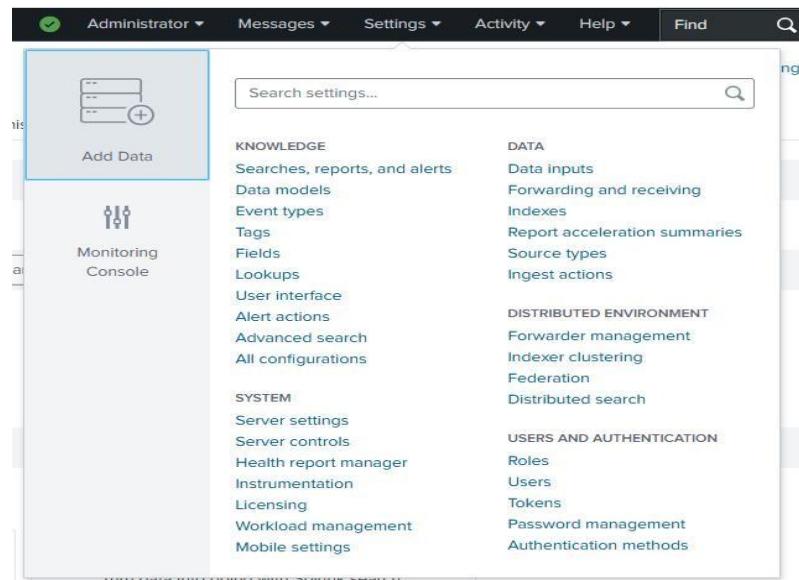
Step No. 1:

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.

The screenshot shows the 'Add Data' wizard in the Splunk interface, currently at the 'Select Source' step. The steps are indicated by a progress bar: Select Source (green dot), Input Settings (white circle), Review (white circle), Done (white circle). Buttons for < Back and Next > are visible.

The left sidebar lists several data collection options:

- Local Event Logs**: Collect event logs from this machine.
- Remote Event Logs**: Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.
- Files & Directories**: Upload a file, index a local file, or monitor an entire directory.
- HTTP Event Collector**: Configure tokens that clients can use to send data over HTTP or HTTPS.
- TCP / UDP**: Configure the Splunk platform to listen on a network port.
- Local Performance Monitoring**: Collect performance data from this machine.
- Remote Performance Monitoring**: Collect performance and event information from remote hosts. Requires domain credentials.

A dropdown menu on the right says "Select an option".

Available item(s) [add all >](#)

- Application
- Security
- Setup
- System
- ForwardedEvents
- DirectShowPluginControl
- Els_Hyphenation/Analytic
- EndpointMapper
- FirstUXPerf-Analytic

Select the Windows Event Logs you want to index from the list.

Selected item(s)

- Application
- System

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.

Add Data [Select Source](#) [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](#)

Host field value

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](#)

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.

This screenshot shows the VirusTotal API key management interface. At the top, it displays a warning about the API key's personal nature and legal agreements. Below this, the "API QUOTA ALLOWANCES FOR YOUR USER" section indicates a standard free account with limited access. It lists the following quotas:

- Access level: Limited, standard free public API
- Usage: Must not be used in business workflows, commercial products or services.
- Request rate: 4 lookups / min
- Daily quota: 500 lookups / day
- Monthly quota: 15.5 K lookups / month

On the right side, there are icons for various API clients: API reference, Python client, Golang library, Command-line interface, and others like Java, .NET, and Ruby.

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.

This screenshot shows the Splunk Enterprise search interface. The "Search" tab is active. The "Apps" menu is open, showing the following options:

- Home
- ✓ Search & Reporting
- Audit Trail
- Splunk Secure Gateway
- Upgrade Readiness App
- Manage Apps
- Find More Apps

The "Search & Reporting" option is highlighted with a checkmark and a green arrow icon.

The screenshot shows the Splunk search interface with the following details:

- Search Bar:** index=* [source="WinEventLog:Application" OR source="WinEventLog:System"]
- Results Summary:** 5,044 events (7/5/25 1:00:00.000 PM to 7/6/25 1:45:46.000 PM) No Event Sampling
- Time Range:** Last 24 hours
- Event List:** The results table shows two event entries:

 - Event 1:** Time: 7/6/25 1:43:28 PM, LogName=System, EventCode=158, EventType=4, ComputerName=DESKTOP-2B7TA25. It also shows interesting fields like host, source, and sourcetype.
 - Event 2:** Time: 7/6/25 1:27:15 PM, LogName=Application, EventCode=3, EventType=4, ComputerName=DESKTOP-2B7TA25.

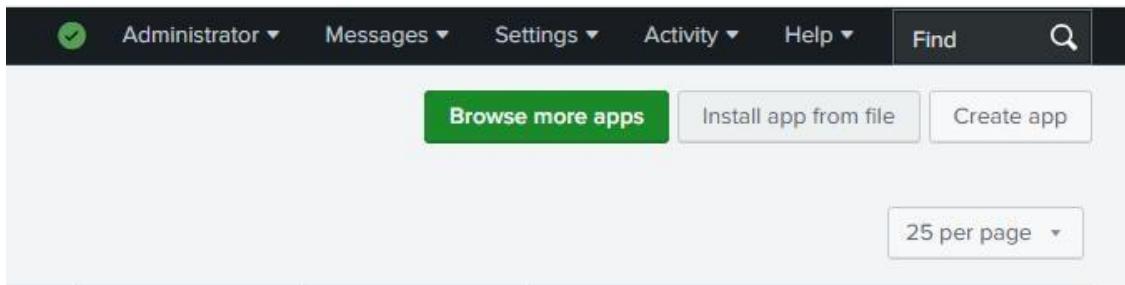
- Navigation:** Includes buttons for Timeline format, Zoom Out, Zoom to Selection, Deselect, and a page navigation bar from 1 to 8.

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.

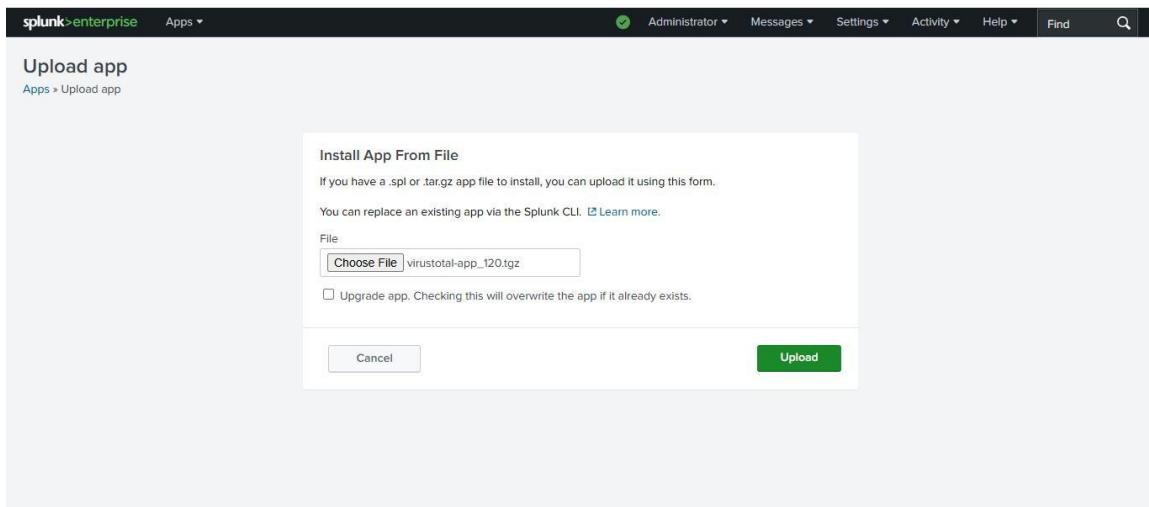
The screenshot shows the Splunk enterprise dashboard with the following details:

- Search Bar:** index=*
- Results Summary:** 5,044 events
- Event List:** Shows a single event entry: 7/6/25 1:45:46.000 PM, LogName=System, EventCode=158, EventType=4, ComputerName=DESKTOP-2B7TA25.
- Apps Menu:** The "Apps" dropdown menu is open, showing options like Home, Alerts, Search & Reporting, Audit Trail, Splunk Secure Gateway, Upgrade Readiness App, Manage Apps, and Find More Apps.



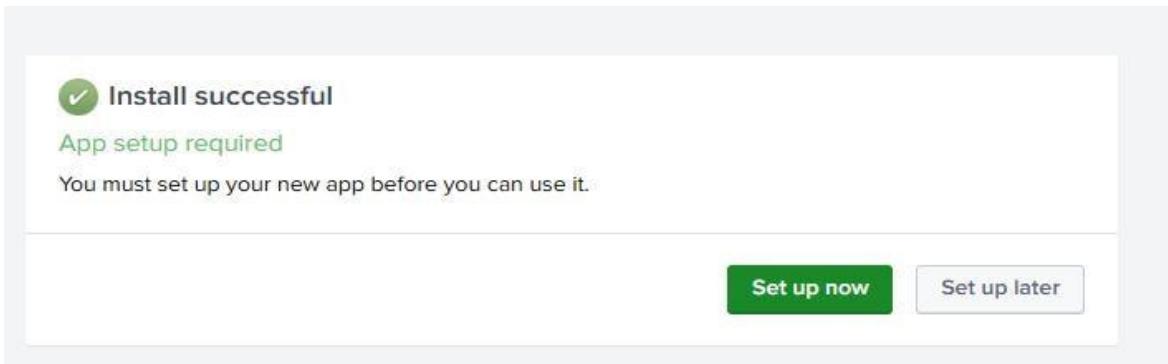
Step No. 9:

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.



VirusTotal API Key Configuration

API Key

Proxy

API Key

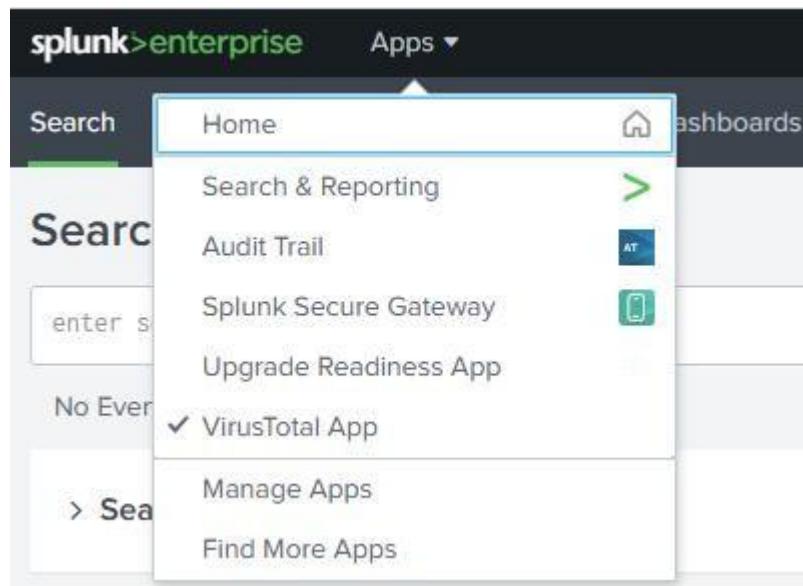
.....| 

Save API Key

Help
Please enter your VirusTotal API key above. You can find your API key in your VirusTotal account settings.
[View VirusTotal API documentation](#)

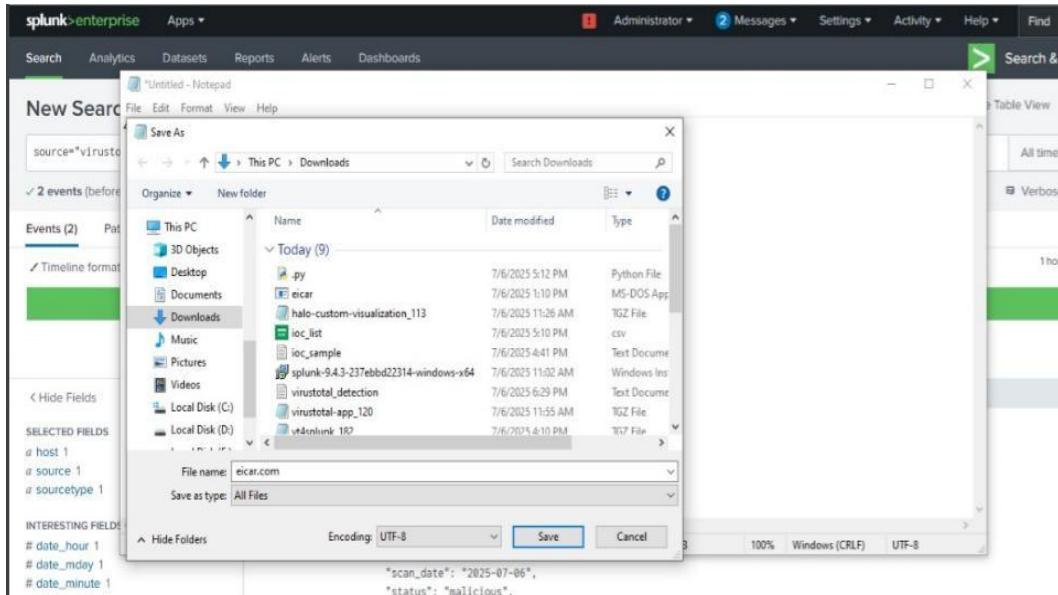
Step No. 11:

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.

A screenshot of a Windows PowerShell window titled "Administrator: Windows PowerShell". The command entered is "& \"C:\Program Files\Splunk\bin\splunk.exe\" restart". The output shows the "Splunkd" service stopping, followed by a message "Splunk> Like an F-18, bro.". It then performs several checks: "Checking prerequisites...", "Checking http port [8000]: open", "Checking mgmt port [8089]: open", "Checking audit port [8080,8.0.1:8085]: open", "Checking restore port [8911]: open", "Checking configuration... Done", "Checking critical directories... Done", "Checking index paths... Done", "Validated: _audit _configtracker _dsappevent _dsphonehome _internal _introspection _metrics _metrics_rollup _telemetry _thefishbucket history main summary", "Done", "Checking filesystem compatibility... Done", "Checking conf files for problems... Bad regex value: '(?:){0}**', of param: props.conf / [(?:){0}**]; why: this regex is likely to apply to all data and may break summary indexing, among other Splunk features.", "One or more regexes in your configuration are not valid. For details, please see btool.log or directly above.", "Done", "Checking default conf files for edits...", "Validation of default conf files against hashes from 'C:\Program Files\Splunk\splunk-9.4.3-237ebbd22314-windows-x64-manifest' All installed files intact.", "Done", "All preliminary checks passed.", "Starting splunk server daemon (splunkd)...", "Splunkd: Starting (pid 14752)". The PowerShell window is running in the background of a Windows desktop. The taskbar at the bottom shows various icons for apps like File Explorer, Edge, and File History. The system tray indicates a temperature of 34°C, a battery level of 63%, and the date and time as 7/6/2025 3:35 PM.

Screenshot of a Splunk search results page showing two events related to a file named 'eicar.com'.

Events (2)

i	Time	Event
>	06/07/2025 23:45:00.000	<pre>{ "timestamp": "2025-07-06T18:49:00Z", "source": "virustotal", "file_name": "eicar.com", "file_hash": "44088612FEBAB8F36DE82E1278ABB82F", "malicious_engines": 55, "total_engines": 68, "detection_ratio": "55/68", "severity": "high", "scan_date": "2025-07-06", "status": "malicious", "host": "WIN10-HBK" }</pre> <p>host = DESKTOP-MAIANMK source = virustotal_detection.log sourcetype = VT4splunk</p>
>	06/07/2025 18:31:18.000	<pre>{ host = DESKTOP-MAIANMK source = virustotal_detection.log sourcetype = VT4splunk }</pre>

SELECTED FIELDS

- a host 1
- a source 1
- a sourcetype 1

INTERESTING FIELDS

- # date_hour 1
- # date_mday 1
- # date_minute 1
- # date_month 1
- # date_second 1
- # date_wday 1
- # date_year 1
- # date_zon 1
- a index 1
- # linecount 2
- a punct 2
- a splunk_server 1
- # timeendpos 1
- a timestamp 1

Step No. 14:

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

Screenshot of the VirusTotal analysis interface for the file 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f.

Community Score: 66 / 69

File distributed by Offensive Security

File Details:

- File Hash: 275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f
- File Name: eicar.com.txt
- Size: 68 B
- Last Analysis Date: 12 minutes ago
- Tags: powershell, idle, direct-cpu-clock-access, long-sleeps, via-tor, legit, attachment, known-distributor

Detection (3677)

Code insights

EICAR is a test string used to detect and test antivirus software. It's like a "dummy virus" that triggers an antivirus engine to react, demonstrating its ability to identify and neutralize threats.

Here's the key:
It's NOT a real virus: EICAR is harmless and cannot infect your computer.

[Show more](#)

Crowdsourced YARA rules

⚠️ Matches rule malw_eicar from ruleset MALW_Eicar at <https://github.com/advanced-threat-research/Yara-Rules> by Marc Rivero | McAfee ATR Team

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