**Integrating VirusTotal with Wazuh**

This guide provides step-by-step instructions to integrate **VirusTotal** with **Wazuh** for enhanced threat detection and malware analysis.

**Prerequisites**

* Wazuh Manager installed and configured
* Active VirusTotal API key (Get it from [VirusTotal API](https://www.virustotal.com/gui/my-apikey))

**Step 1: Get API key from VirusTotal**

1. Scroll down on home page and click on API Key.

A screenshot of a computer

AI-generated content may be incorrect.

1. Copy your API key from here.

**Step 2: Enable VirusTotal Integration in Wazuh**

1. **Log in to the Wazuh Manager**
2. Navigate to the configuration file:
3. sudo nano /var/ossec/etc/ossec.conf
4. Add the VirusTotal integration section:

<integration>

<name>virustotal</name>

<api\_key>Your\_VirusTotal\_API\_Key</api\_key>

<timeout>60</timeout>

<alert\_format>json</alert\_format>

</integration>

1. Save and exit the file.
2. Restart the Wazuh Manager to apply changes:
3. sudo systemctl restart wazuh-manager

**Step 3: Verify Integration**

1. Generate a test alert with a malicious file or hash.
2. Check the Wazuh alerts using the following command:
3. sudo cat /var/ossec/logs/alerts/alerts.json | grep virustotal

**Troubleshooting**

* **API Key Issues:** Ensure the VirusTotal API key is valid and has sufficient quota.
* **No Alerts:** Confirm the rule configuration is correct and check /var/ossec/logs/ossec.log for any errors.
* **Firewall Issues:** Ensure the Wazuh Manager can access the VirusTotal API (api.virustotal.com).

**Conclusion**

By integrating VirusTotal with Wazuh, you can automate the detection of malicious files and receive actionable threat intelligence, strengthening your organization's security posture.