|  |  |
| --- | --- |
|  | **Virus Total** |

**Description**

VirusTotal aggregates many antivirus products and online scan engines to check for viruses that the user's own antivirus may have missed, or to verify against any false positives.[5] Files up to 128 MB can be uploaded to the website or sent via email.[6] Anti-virus software vendors can receive copies of files that were flagged by other scans but passed by their own engine, to help improve their software and, by extension, VirusTotal's own capability. Users can also scan suspect URLs and search through the VirusTotal dataset

**Supported Versions**

V2.1, V2.2, V2.3, V2.4, V3.0, V3.3, V4.0, V4.2

**Integration Credentials**

* Api Key
* Verify SSL

**Additional Information**

None

**Actions**

|  |  |
| --- | --- |
| **Scan IP** | **Description**  VirusTotal scan external IP address.  **Action outcome**  **Result**  is\_success (True/False depends if success)  **Enrichment**   * Entity Csv table: with detections scores and related information after calculation. * Entity enrichment: with detections scores and related information after calculation. * Web link to original entity report page. * Json Result - full report |
| **Scan Hash** | **Description**  Scan Hash via VirusTotal.  \*Mark entity as suspicious and show insights if risk score exceed threshold  Action will fetch the latest result using cache mechanism:  Check if hash need to be rescanned or should fetch an existing report. Determine by ‘Rescan after days’ parameter. If the current date minus the existing scan date in VirusTotal is bigger/equals to the mentioned ‘Rescan after days’ parameter (in days) - Rescan the hash in VirusTotal. Otherwise, fetch the existing report from VirusTotal.  **Parameters**   * Threshold (Virus total detection risk score) * Rescan after days (number that determine how many days after to rescan )   **Action outcome**  **Result**  is\_risky (True/False depends if pass the given threshold)  **Enrichment**   * Entity Csv table: with detections scores and related information after calculation. * Entity enrichment: with detections scores and related information after calculation. * Web link to original entity report page. * Entity mark as suspicious if it pass the given threshold. * Json Result - full report   **Insights**  Entity insight with engines detection summary information (if it pass the given threshold). |
| **Get Domain Report** | **Description**  Get domain report from VirusTotal.  \*Mark entity as suspicious and show insights if risk score exceed thresholdץ  **Action outcome**  **Result**  is\_success (True/False depends if success)  **Enrichment**   * Entity Csv table: with detections scores and related information after calculation. * Entity enrichment: with detections scores and related information after calculation. * Web link to original entity report page. * Json Result - Full report |

|  |  |
| --- | --- |
| **Scan URL** | **Description**  scan URL via VIrusTotal.  Report include URL scanning engines results is returned. VirusTotal related metadata (first seen date, last seen date, files downloaded from the given URL, etc.) and the output of other tools and datasets when fed with the URL.  Action will fetch the latest result using cache mechanism:  Check if hash need to be rescanned or should fetch an existing report. Determine by ‘Rescan after days’ parameter. If the current date minus the existing scan date in VirusTotal is bigger/equals to the mentioned ‘Rescan after days’ parameter (in days) - Rescan the hash in VirusTotal. Otherwise, fetch the existing report from VirusTotal.  **Parameters**   * Threshold (Virus total detection risk score) * Rescan after days (number that determine how many days after to rescan )   **Action outcome**  **Result**  is\_risky (True/False depends if pass the given threshold)  **Enrichment**   * Entity Csv table: with detections scores and related information after calculation. * Entity enrichment: with detections scores and related information after calculation. * Web link to original entity report page. * Entity mark as suspicious if it pass the given threshold. * Json result - full report   **Insights**  Entity insight with engines detection summary information (if pass the given threshold). |
| **Upload And Scan File** | **Description**  Upload file and scan it on VirusTotal.  \*Files can be uploaded from remote path (Windows share OR Linux remote server)  **Parameters**   * Threshold (Virus total detection risk score) * File Paths (Target file paths) * Linux Server Address (if exists. e.g. x.x.x.x) * Linux User (if exists) * Linux Password (if exists)   **Action outcome**  **Result**  is\_risky (True/False depends if pass the given threshold)  **Enrichment**   * Entity Csv table: with detections scores and related information after calculation. * Web link to original entity report page. * Json result - full report   **Insights**  Insight with engines detection summary information for the uploaded file (if pass the given threshold). |