Datasheet

Introducing the new ECS Security VirusTotal Malware Lookup Add-on for Splunk

Splunk makes machine data accessible, usable and valuable to everyone.

Splunk Enterprise is the industry-leading platform for machine data. Machine data is one of the fastest growing, most complex areas of big data. It's also one of the most valuable, containing a categorical record of user transactions, customer activity, sensor readings, machine behavior, security threats, fraudulent activity and more.

ECS Security is an Elite partner of Splunk, providing a portfolio of Splunk Professional Services and Managed Services to leading financial services and retail clients to maximise the value Splunk brings to their business.

ECS Security is an award-winning provider of Security Operations Centre (SOC) and Security Information and Event Management (SIEM) services. Our expert team designs, builds, runs and assesses SOC and SIEM solutions. Using our unique methodology, we work with clients to ensure they have an effective security monitoring capability that is tailored to their specific requirements.

At ECS Security, we provide flexible offerings and excellent customer service whilst ensuring context-aware support. We provide the right balance between reactive monitoring and proactive threat hunting.

How to speed up security investigations?

An ECS Security customer found security investigations were taking an increasing amount of time and running ad-hoc scripts outside of Splunk to gather contextual information from VirusTotal (VT) on suspicious files detected within their environment.

This step in the process was delaying security investigations and causing additional operational overhead. They asked us to help speed up the process and make it more efficient.

The speed of detection & investigation is critical with potential malware infections. We therefore developed a new Splunk command enabling a correlation search for them which would help to address these challenges. Following the success of this additional functionality and extremely positive feedback from the client, ECS Security expanded on this concept and created this as a Splunk Add-on so that others may benefit.

The **VirusTotal Malware Lookup for Splunk Add-on** is in the form of a search command which can be included in a correlation search to lookup suspicious file hash values from VirusTotal and store them efficiently in Splunk.

VirusTotal inspects items with over 70 antivirus scanners, in addition to a myriad of tools to extract signals from the studied content. The customer specific submissions are internally hashed and then compared using the HTTPs-based public API.

The Add-on is designed for bulk lookups and stores the enrichment content as a KV Store Lookup file in Splunk so is efficient in terms of usage of the VirusTotal API and Splunk license. There is also user configurable result caching to avoid stale results.

How does it work?

You can download this Technology Add-on (TA) from Splunk via their Splunkbase site: *https://splunkbase.splunk.com/app/4283/*

ECS Security also makes the source code available on GitLab for tracking changes and submitting issues: *https://gitlab.com/ecs_public_projects/splunk/TA-VirusTotal*

The Add-on can be run on a Splunk Search Head and requires minimal configuration.

The "VirusTotal" command in Splunk takes your file hash values and does a bulk lookup in VirusTotal and stores the enriched data about these file hashes in an efficient KV Store lookup file in Splunk.

The data returned by the Add-on includes;

- The VT resource, normally the hash value
- The number of vendors who scanned the file
- The number of vendors confirming it is malicious
- A URL for more detailed analysis of the threat
- A classification of the threat type of the content
- When VT last scanned this file hash

The results are stored as a table for analysis, to include in correlation searches or create dashboards showing the results. As an example, dashboard that could be created is shown below with a summary of results for a single Hash value.

What are the benefits?

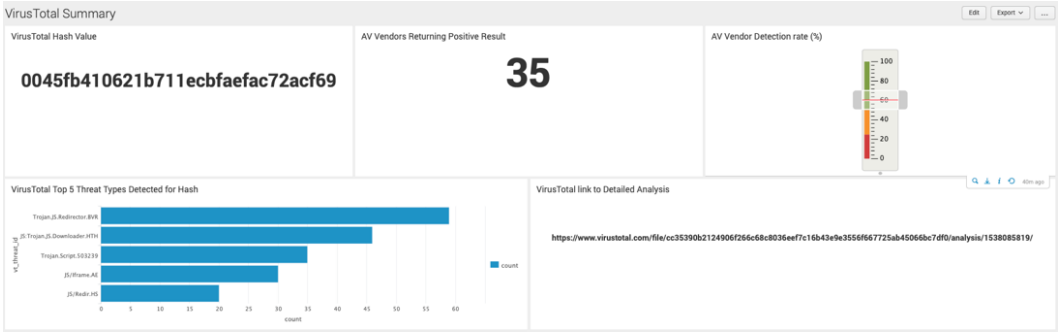
The VirusTotal Malware Lookup for Splunk enables near real-time alerting of potential malicious files on any of your internal endpoints.

Our customer is gathering endpoint logs (including potentially malicious file hashes) and storing them in Splunk. They then use the VirusTotal Malware Lookup for Splunk TA to do a bulk lookup of those hashes to see which are malicious as indicated by any of the vendors who participate in VirusTotal.

This provides a "single source of truth" within Splunk and allows Security Analysts to investigate Malware from a single interface which has now automated this previously time-consuming manual process.

Another great benefit is that this TA provides an efficacy check on your existing antivirus provider. Combining multiple vendors on the detection of malicious content provides a far greater level of certainty – i.e. if a high percentage of the vendors agree the file is malicious and return the same classification for the threat. This process will at the same time, flag inaccurate, ineffective providers.

Clients could also scan email logs for attachments that contain malicious file content and produce an alert or automated response to mitigate the threat.



To find out more about the VirusTotal Malware Lookup for Splunk or any of our Splunk Services please contact enquiries@ecssecurity.co.uk