Trend Micro™ Attack Scanner 1.1 for Splunk Frequently Asked Questions

Splunk and Squid Information

1. Does Attack Scanner work with Splunk Free?

   Attack Scanner has been certified to work with both Splunk Free and Splunk Enterprise 6.0 and 6.1 running on both Windows and Linux systems.

2. Does Trend Micro have a plan to provide similar tools for IBM QRadar, HP ArcSight, and other SIEM solutions?

   Trend Micro is currently only announcing Attack Scanner availability for the Splunk platform. Support for other SIEM solutions is under consideration and will be announced at an appropriate time.

3. Aside from Squid logs, what other log formats does Attack Scanner support?

   Attack Scanner supports the Web and Proxy data model of Common Information Model (CIM) add-on. If you have created a technology add-on that supports the Web and Proxy data model, you can set this source type through the app's **Settings** screen.

   Alternatively, take advantage of Splunk's field alias to create an alias for specific fields.

   Note

   Attack Scanner uses `src` (traffic source) and `dest` (traffic destination) by default. To enable support, create another alias for your own source and destination fields.

Licensing and Activation Code

1. How do I purchase a license for Attack Scanner?

   License for Attack Scanner will be available for purchase at a date to be announced later. Please contact the Trend Micro sales office nearest you by visiting www.trendmicro.com.

2. Why do I need a license to use Attack Scanner? How do I obtain a license?

   A valid license is required to receive the latest C&C intelligence updates from Trend Micro™ Smart Protection Network™. The list of C&C servers monitored by Trend Micro changes dynamically on a regular basis and updates are necessary to ensure that detection results are as accurate as possible.

   Use the following trial Activation Code to install and run the app for 90 days: `DM-4MQP-JU5F8-J9ME3-VNMK4-25A9N-HPMGC`

   Note

   This Activation Code is due to expire by March 31, 2015.

   Subsequent trial requests can be sent to spapp_ac_request@trendmicro.com.

Scanning

1. Does Attack Scanner scan all my network access events?

   Attack Scanner only scans indexed events stored in the index repository specified in the Attack Scanner **Set Up** screen. Moreover, only the events falling within the time range specified by **Start time for C&C Callback Scan** and **End time for C&C Callback Scan**, also configurable from the **Set Up** screen, will be scanned with the latest, downloaded C&C intelligence.

2. What is the default scan range? How do I change it?

   By default, Attack Scanner only scans events with timestamps within the past seven days. This can be changed by modifying the values associated with the parameters

Start time for C&C Callback Scan and **End time for C&C Callback Scan** on the app **Set Up** screen. For example, to extend the scan period to cover the past 10 days, specify `-10d@d` for **Start time for C&C Callback Scan**.

3. How come I do not see any detection?

   Detections are not displayed for a number of reasons:

   - During the period covered by the event logs, you do not have any host attempting to communicate with C&C servers monitored by Trend Micro Smart Protection Network. Consider increasing the amount of logs indexed by Splunk and to be scanned by Attack Scanner.

   - The time range for event correlation by Attack Scanner is too short. By default, time range is only limited within the past seven days, so earlier attempts to communicate with C&C servers are not detected. Consider changing the settings in the **Time Range for Event Correlation** section of the app **Set Up** screen to cover a longer period.

   - Your app installation might not have a valid license, or the Activation Code might have expired.

4. Attack Scanner is displaying that some hosts on my network have been communicating with C&C servers. How do I obtain more information about the C&C servers in question?

   Starting with version 1.1, Attack Scanner is integrated with Trend Micro Threat Connect portal, which provides a wealth of information related to each C&C server, including profile of the associated attack family. Additional information from Threat Connect can be obtained for a specific C&C server from the screen under the **C&C Server Timeline** menu.

5. How can I run an on-demand scan?

   By default, Attack Scanner generates and refreshes results every 24 hours. (However, this can be changed by modifying the configuration settings.) Running an on-demand scan is not yet supported in this release but is planned in a future update.