WEBROOT
BrightCloud IP Reputation Service for Splunk

Webroot BrightCloud Threat Intelligence App V1.0
User Guide
# Table of Contents

Introduction ................................................................................................................................. 2  
Prerequisite .................................................................................................................................. 3  
Installation and Configuration ...................................................................................................... 3  
How To Use .................................................................................................................................. 13  
  Overview ...................................................................................................................................... 13  
  IP Reputation Statistics .................................................................................................................. 14  
  IP Threat Analysis .......................................................................................................................... 17  
  One-Click Lookup of Malicious IPs From IP Threat Analysis ...................................................... 22  
  IP Reputation Lookup .................................................................................................................... 25  
  Alerts ............................................................................................................................................. 27  
Using BrightCloud Data in Splunk Queries .................................................................................... 29  
  brightcloud_getcategories ............................................................................................................... 29  
  brightcloud_bcss_info .................................................................................................................... 30  
Legal Notice .................................................................................................................................... 31
Introduction

The BrightCloud IP Reputation Service is a predictive threat intelligence service that continuously monitors 4.3 billion IPs and identifies malicious IPs that enterprises should detect in their IP traffic and respond to quickly before those malicious IP activities lead to more costly security breaches.

The BrightCloud IP Reputation Service for Splunk provides a Webroot BrightCloud Threat Intelligence app for Splunk, hereafter known as the Splunk app, which detects and alerts users of malicious IP activities in their infrastructure by doing the following:

- Regularly downloading the most up-to-date malicious IP database from BrightCloud.
- Comparing IP traffic logs stored inside Splunk against the malicious IP database downloaded from BrightCloud.
- Detecting and alerting users of malicious IP activities found in their IP traffic logs.

Note: This document reflects information and images for Splunk Version 6.2.
Prerequisite

The Webroot BrightCloud Threat Intelligence app V1.0 supports Splunk Enterprise V6.0 and higher. The rest of the documentation assumes the user already has a Splunk Enterprise V6.0 or higher deployed and that the user has a valid userid to download apps from apps.splunk.com.

Installation and Configuration

This document assumes that the user has already downloaded the Splunk app from apps.splunk.com. If not, please navigate your browser to apps.splunk.com, search for Webroot BrightCloud Threat Intelligence and download it to your local directory.

This section contains instructions on how to:

- Install and configure the Webroot BrightCloud Threat Intelligence app
- Uninstall the Webroot BrightCloud Threat Intelligence app

To install and configure the Webroot BrightCloud Threat Intelligence app:

1. Log in to Splunk Web as administrator.
2. On the Home page, click the blue **Apps** icon.

![Home page with Apps icon highlighted](image)

3. Click the **Install app from file** button.

![Install app from file button highlighted](image)

The system displays the Upload app page.

![Upload app page](image)
4. In the *File* field, click the **Choose File** button and browse to the file to select it.

5. Select the **Upgrade app** checkbox.
6. Click the **Upload** button.

7. To complete the installation, click the **Restart Splunk** button.
The Install successful message displays.

8. Click the **Set up now** button.

The system displays the Configuration window.
9. In the field, enter your **UID**. This personal license key will be used during the update process.

10. Click the **Save** button.

The system displays the Manage Apps window. The message in the upper left of the window indicates whether the app was successfully installed.
11. Click the **Splunk** link.

The system displays the Home page, with the icon for the Webroot BrightCloud app in the left column.

12. Click the **Webroot BrightCloud** icon.
The first time you click the Webroot BrightCloud icon, the system displays the EULA Acceptance page.

13. Optionally, you can click the BrightCloud Security Services for Enterprise Agreement link and review the EULA Acceptance document.

The system displays the Welcome to Webroot! Page, where you can review the EULA agreement.

Note: If you do click the link, click the Splunk tab in your browser to return to the EULA Acceptance page.
14. Select the checkbox, then click the **Start using Webroot BrightCloud Threat Intelligence app** button.

15. When you are ready, return to the Splunk page, and click the Webroot BrightCloud icon.
The system displays the Overview page, where you can access additional functionality.

To uninstall the Webroot BrightCloud Threat Intelligence app:

1. Remove the app or add-on's indexed data.

   Typically, Splunk does not access indexed data from a deleted app or add-on. However, you can use Splunk's CLI clean command to remove indexed data from an app before deleting the app. For more information, see Remove data from indexes with the CLI command.

   **Note:** This is an optional step.

2. Delete the app and its directory. This should be located here:

   `$SPLUNK_HOME/etc/apps/<appname>`

   You can run the following command in the CLI:

   `/splunk remove app [appname] -auth <username>:<password>`

3. You may need to remove user-specific directories created for your app or add-on by deleting the files, if any, found here:

   `$SPLUNK_HOME/splunk/etc/users/*/<appname>`

4. Restart Splunk.
How To Use

The app consists of several dashboards, which are described in this section.

Overview

The Overview tab displays the following information:

- The email address where you can contact Webroot to upgrade your license.
- A description of the Splunk app.

Contact info:
Contact splunk@webroot.com if you have any questions about licensing for this Splunk app for BrightCloud.
The Splunk app needs to first download the list of millions of malicious IPs from the BrightCloud IP Reputation Service to a local IP reputation database. It will then regularly update the local IP reputation database with updates from BrightCloud. The local IP reputation database is used to correlate against log files indexed by Splunk and detect malicious IP activities.

The IP Reputation Statistics tab displays information about the local IP reputation database:

- The number of IP addresses contained in the database that have been downloaded from BrightCloud IP Reputation Service.
- The version number and the build date.

To download the first version of the IP reputation database:

1. Do either of the following:
   - From the Automatic download frequency drop-down menu, select a frequency and then click the **Apply** button. This will trigger the initial download and creation of the local IP reputation database as well as subsequent regular updates to it.
To manually trigger the download of the latest data from BrightCloud IP Reputation Service to the local IP reputation database, click the **Download now** button. Please note that this is a one-time operation. To set up regular update of the local IP reputation database, configure the Automatic download frequency.

The system displays the following information:

- The number of IP addresses contained in the database that have been downloaded from BrightCloud IP Reputation Service.
- The version number and the build date.
Keep in mind the following:

- It takes a couple of minutes for the update to take place as it downloads the changes since the last update and merges those into the local database file.
- Additionally, you can set the frequency of the update to either 15 minutes, 12 hours, or 24 hours. If you change the frequency, you must reboot the Splunk server for the change to take effect.
IP Threat Analysis

The IP Threat Analysis tab lets you examine threats using time ranges, source types, and other data points. You can look for malicious IP activities in specific log files indexed by Splunk and alert the info security team so that they can quickly respond and investigate these activities. Use the IP Threat Analysis tab to accomplish this by:

- Selecting specific time frame when user wants to search for malicious IP activities
- Selecting specific log files for searching
- Selecting specific IP fields in those log files

To run a threat analysis:

1. From the Select a time range drop-down menu, select a time range.

2. From the Select a sourcetype drop-down menu, select a sourcetype.
   
   A sourcetype is a log file that will be analyzed against the IP reputation database.
3. From the Select a field drop-down menu, select a data field in the log file specified in the sourcetype selection.

A data field is the specific IP field inside of the log files that will be compared against the IP reputation database.

4. Click the Submit button.

**Note:** To correlate IP rep against multiple sourcetypes or fields, please create merged sourcetypes and fields by combining multiple sourcetypes or fields into singles in Splunk, and then come back to this Splunk app to use those merged sourcetypes or fields.

The dashboard displays a table with the following information:

- The proportion between good and bad IP addresses
- Malicious IPs grouped by category and country.
- Potentially malicious IP addresses.
- A map with the threats’ geo-distribution.
5. To create an alert, click the **Create Alert** button at the top of the page.

When you create an alert, you will be notified of malicious IP activities detected with BrightCloud Reputation.
6. From here you can create a personalized alert.

For more information on how to create a personalized alert, see the Splunk Alerting Manual.
One-Click Lookup of Malicious IPs From IP Threat Analysis

In addition to creating an alert from the IP Threat Analysis tab, you can also click on any malicious IP detected and lookup additional info on that IP for investigation and analysis.

To look up malicious IPs:

1. From the Select a time range drop-down menu, select a time range.

![Select a time range](image1)

2. From the Select a sourcetype drop-down menu, select a sourcetype.

A sourcetype is a log file that will be analyzed against our IP reputation database.

![Select a sourcetype](image2)

3. From the Select a field drop-down menu, select a data field in the log file specified in the sourcetype selection.

A data field is the specific IP field inside of the log files that will be compared against our malicious IP list.

![Select a field](image3)
4. Click the **Submit** button.

![IP Threat Analysis](image)

**Note:** To correlate IP rep against multiple sourcetypes or fields, please create merged sourcetypes and fields first, for example, combine multiple sourcetypes or fields into singles, in Splunk and then come back to this Splunk app.

The dashboard displays a table with the following information:

- The relationship between good and bad IP addresses
- Malicious IPs grouped by category and country.
- Potentially malicious IP addresses.
- A map with the threats’ geo-distribution.
5. To view information on the IP Lookup page, click on a specific IP in the dashboard. The dashboard displays additional information about malicious IPs, which you can use for investigation or incident response.

**IP Reputation Lookup**

Use the IP Reputation Lookup tab to check whether an IP is malicious or not. You can enter an IP address, and get information about the IP address. If it’s malicious, you will see additional information about the IP, for example, where the IP is located, what kind of threat the IP presents, etc.

**To look up an IP’s reputation:**

1. Within Splunk, click the **IP Reputation Lookup** tab.
2. In the *Insert an IP address* field, enter a site’s IP number.

3. Click the **Submit** button.

The system displays information about the IP’s reputation, including their status and geographical information.
Alerts

From the Alerts tab, you can manage all the alerts you created.

To manage an alert:

1. Click on an alert to view the trigger history.

The system displays information about the alert.

2. From here you can do either of the following:
   - Click **Disable** to disable the alert.
   - Click **Edit** next to any setting for the alert.

   The system displays a window where you can edit the settings.
3. In the Actions column, click the **View results** button.

The system displays the Statistics tab.

Additionally, you can click any of the following tabs:

- Events
- Patterns
- Visualization
Using BrightCloud Data in Splunk Queries

BrightCloud IP Reputation data can be used both inside and outside of the Splunk app in Splunk queries. Go to the Search tab either inside or outside the Splunk app to access the Search panel.

Use the following commands in Splunk queries to correlate BrightCloud IP reputation data with other data in Splunk. For more information, see Splunk Documentation.

- `brightcloud_getcategories`
- `brightcloud_bcss_info`

**brightcloud_getcategories**

This command takes as input one field, named `ip`, and returns the category that the IP address matches or a list of categories if the IP address matches more than one category.
**Threat Categories**

BrightCloud tracks IP threats across these categories:

- SpamSources
- WindowsExploits
- WebAttacks
- BotNets
- Scanners
- DenialOfService
- Reputation
- Phishing
- Proxy
- Network
- CloudProviders
- MobileThreats

You can use these categories directly inside a Splunk search query:

```
Search Categories = "Proxy"
```

**brightcloud_bcss_info**

This command is used to get more contextual information about the IP, for example, where it came from, what type of IP threat it is, etc. Query results are large because the system renames and reformats to make the information more readable.

**Note:** Because this lookup performs a cloud lookup it should not executed against large lists of IP addresses, due to latency of online lookup.
Legal Notice

© 2014 Webroot Inc. All rights reserved. Reproduction or distribution of this documentation is prohibited unless you are either duly licensed to reproduce or distribute this documentation within the applicable license terms or you have otherwise obtained the prior written permission of the copyright owner to do so. Webroot and BrightCloud are trademarks or registered trademarks of Webroot Inc. in the United States and other countries. All other trademarks are properties of their respective owners.

netaddr

COPYRIGHT AND LICENSE

Copyright (c) 2008-2014, David P. D. Moss. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of David P. D. Moss nor the names of contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.