Network Integration Fireeye

CB v4.2.5.150311.1434

March 11, 2015

Contents

Overview

Carbon Black provides integration with an on-premise FireEye device for correlating FireEye alerts with Carbon Black collected data. More information about FireEye can be found at: http://www.fireeye.com/

To support this integration, Carbon Black provides an out-of-band bridge that receives alerts from the FireEye device and communicates with the Carbon Black enterprise server.

Prerequisites

```
1. A Carbon Black enterprise server installation >= 4.0

2. FireEye
```

Installation

1. Configure a yum repo that points to the Carbon Black yum repository that contains the FireEye bridge.
   Create a new file '/etc/yum.repos.d/FireEye.repo' with the following content:

   ```
   [FireEye]

   name=FireEye
   baseurl=https://yum.carbonblack.com/enterprise/integrations/fireeye/x86_64

   gpgcheck=0
   enabled=1

   metadata_expire=60
   sslverify=1

   sslclientcert=/etc/cb/certs/carbonblack-alliance-client.crt
   sslclientkey=/etc/cb/certs/carbonblack-alliance-client.key
   ```

2. Verify the yum configuration and install the FireEye bridge

   ```
   yum info python-cb-fireeye-bridge
   yum install python-cb-fireeye-bridge
   ```

3. Edit the FireEye bridge configuration file
   The FireEye bridge configuration is located here:

```
/etc/cb/integrations/carbonblack_fireeye_bridge/carbonblack_fireeye_bridge.conf
```

Update the *carbonblack_server_url* option to set the URL of the Carbon Black enterprise server.

Update the *carbonblack_server_token* options to set a Carbon Black enterprise server user api token that has administrative rights on the server.

The remainder of the options are documented and can be customized if needed to match specific requirements.

Save the configuration

4. Start the FireEye bridge

```
/etc/init.d/cb-fireeye-bridge start
```

5. Examine the FireEye bridge log to verify the service is running normally

```
/var/log/cb/integrations/carbonblack_fireeye_bridge/carbonblack_fireeye_bridge.log
```

FireEye Feed

Once the service is running, the FireEye feed can be added to the Alliance feeds on the enterprise server. Add a new feed and specify the following URL:

```
http://[bridge host]:[listener_port from bridge config]/fireeye/json

Example: http://127.0.0.1:3000/fireeye/json
```