Network Integration Fidelis

CB v4.2.5.150311.1434

March 11, 2015

Contents

Overview

Carbon Black provides bi-directional integration with an on-premise Fidelis device for correlating Fidelis alerts in the Carbon Black enterprise server and returning Carbon Black metadata to Fidelis. More information about Fidelis can be found at: http://www.fidelissecurity.com/

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

Prerequisites

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

2. Fidelis XPS
```

Installation

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

   ```
   [Fidelis]

   name=Fidelis
   baseurl=https://yum.carbonblack.com/enterprise/integrations/fidelis/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 Fidelis bridge

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

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

```
/etc/cb/integrations/carbonblack_fidelis_bridge/carbonblack_fidelis_bridge.conf
```

Update the *listener_api_token* option to set the shared secret token to allow for Fidelis-to-Bridge communications.

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 Fidelis bridge

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

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

```
/var/log/cb/integrations/carbonblack_fidelis_bridge/carbonblack_fidelis_bridge.log
```

Fidelis Feed

Once the service is running, the Fidelis 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]/fidelis/json
```

```
Example: http://127.0.0.1:8000/fidelis/json
```