**Arcsight FlexConnector JSON Folder Follower**

**Connector Installation Guide**

1. Required: Arcsight Connector 7.7.0.8044.0 or newer.
2. Log into Arcsight console, create directory for Connector, e.g. /opt/arcsight/connectors/gib\_ti  
   **mkdir /opt/arcsight/connectors/gib\_ti**  
   (arcsight user must have permissions to create, delete and edit files in this directory).
3. Go to directory where ArcSight-XXXXX-Connector-Linux64.bin is and execute it in console mode  
   **./ArcSight-XXXXX-Connector-Linux64.bin –i console**  
   (XXXXX stand for Connector version)
4. Follow the instructions and complete the installation. After installation do not execute script runagentsetup.sh immediately. Before that add all **\*.jsonparser.properties** files from “configs” folder to directory **<connector installation path>/current/user/agent/flexagent**.
5. Take api.py script and configure it:
   1. Choose a directory for **api.py** script which downloads files for parser(“data” in example).
   2. Enter **API\_USER** and **API\_KEY in the api.py**.
   3. Don’t forget to configure cron task to start script hourly.
6. Log into **ArcSight Web Interface**. Go to **Configuration -> Receivers**. Press **Add** button to create a new Receiver. Choose a name (e.g. gib\_ti\_receiver), select **SmartMessage Receiver** as a type, press **Next**. Select **UTF-8** Encoding and **CEF**  Source Type, check **Enable** and click on **Save**.
7. After that go to **<connector installation path>/current/bin** and execute script runagentsetup.sh in console mode  
   **./runagentsetup.sh –i console**
8. Choose **“Add a connector”** option.
9. Choose **“ArcSight FlexConnector JSON Folder Follower”** option.
10. JSON Log Folder Location is **<path to API.PY script>/data**.
11. JSON Configuration File Name Prefix is **gib\_root\_parser**.
12. Ignore “Folder does not exist” warning.
13. Choose **“ArcSight Logger SmartMessage (encrypted)”** option as a type of destination.
14. Host Name/IP is a hostname or IP of Arcsight console.
15. Choose port (e.g. default – 443).
16. Enter name of the **Receiver** that was created on 6th step of this guide.
17. Select **Disabled** Compression Mode and **0.1** CEF Version.
18. Enter **Name, Location, DeviceLocation and Comment** for FlexConnector (**these fields aren’t recommended to be left empty or to consist of numbers only!**).
19. Choose **Install as a service** option, remember **Service Internal Name**. Choose **Exit** option.
20. After the configuration start the service with the following command:  
    **service arc\_<Service Internal Name> start**

**Connector User Guide**

* Connector automatically takes \*.json files from chosen folder, parses them and adds into ArcSight.
* To view parsed data log into **ArcSight Web Interface**, go to **Analyze -> Search**, type   
  **receiver = “<Receiver Name>”** in a search query field. To view special collection data use the following search query:  
  **receiver = “<Receiver Name>” AND name CONTAINS “<Collection Name>”**where **<Collection Name>** is one of following:
  + DDOS Attacks
  + Brand abuse advert
  + Brand abuse domains
  + Brand abuse mobile application
  + Brand abuse phishing
  + Brand abuse phishing kit
  + Brand abuse SSL certificates
  + Compromised Account
  + Compromised Bank Card
  + Android devices
  + Money Mules
  + Hacktivism
  + Leaks
  + Sample
  + Open proxy
  + Socks proxy
  + Tor nodes
  + Threats