Forcepoint DLP API and ServiceNow Integration Configuration Guide

Forcepoint

forcepoint.com

Forcepoint DLP API and ServiceNow Integration Tool Configuration Steps

Description

This code is designed to interact with the Data Loss Prevention (DLP) API and the ServiceNow incidents API. It performs the following tasks:

1. Authenticates with the DLP API by sending a POST request to obtain a refresh token and an access token.
2. Uses the access token to send a POST request to the DLP API to retrieve a list of incidents within a specified date range.
3. Parses the JSON response from the DLP API into a list of incident dictionaries.
4. Writes the JSON response to a file named **EL-DLP_incidents_DIM.json**.
5. Creates ServiceNow incidents for each incident retrieved from the DLP API by sending a POST request to the ServiceNow incidents API.

Code Explanation

1. The code starts by importing the necessary modules: **requests** for making HTTP requests, **json** for working with JSON data and **csv** for working with CSV files.
2. The DLP API endpoints are defined using the base URL **https://james.tingley.lab.go4labs.net:9443/dlp/rest/v1/auth**. The specific endpoints used are **/refresh-token** and **/access-token**.
3. The authentication credentials **username and password** are set in the **headers** dictionary along with the content type.
4. A POST request is sent to the DLP API refresh token endpoint to obtain a refresh token. The request is made using the **requests.post()** method, passing the **refresh_url** and **headers** as parameters. The **verify=False** parameter is used to disable SSL verification.
5. The refresh token is extracted from the response by parsing the JSON content using **json.loads(refresh_response.text)["refresh_token"]**.
6. Another POST request is sent to the DLP API access token endpoint to obtain an access token. The request is made using the **requests.post()** method, passing the **access_url**, **headers** and the refresh token in the request payload **access_payload.** The request data is serialized to JSON format using **json.dumps(access_payload)**.
7. The access token is extracted from the response by parsing the JSON content using **json.loads(access_response.text)["access_token"]**.
8. The **headers** dictionary is updated with the access token, which will be used in future requests to authenticate with the DLP API.
9. The DLP API incidents endpoint URL is defined.
10. A JSON payload is created, specifying the type of incidents to retrieve **INCIDENTS** and the date range **from_date** and **to_date**.
11. A POST request is sent to the DLP API incidents endpoint using the **requests.post()** method, passing the URL, headers and payload as parameters. The response is stored in the **response** variable.

12. The JSON response is parsed using **json.loads(response.text)[incidents]** to extract the list of incident dictionaries.
13. The **fieldnames** list is defined, specifying the field names for the CSV file.
14. The response is written to a JSON file named **EL-DLP_incidents_DIM.json** using the **open()** function with the **w** mode and the **write()** method.
15. ServiceNow details, including the instance URL, username and password, are provided.
16. The **create_service_now_incident()** function is defined, which takes an incident dictionary as input.
17. Inside the function, the incident data is defined as a JSON string, including the short description and description fields.
18. A POST request is sent to the ServiceNow incidents API using the **requests.post()** method, passing the incident data, authentication credentials, headers and the ServiceNow incidents API URL.
19. If the response status code indicates an error (>= 300), an error message is printed.

Usage

To use this code, follow these steps:

1. Make sure the **requests**, **json** and **csv** modules are installed.
2. Set the appropriate values for the **username** and **password** variables in the **headers** dictionary.
3. Set the appropriate values for the **service_now_instance**, **service_now_user** and **service_now_pass** variables.
4. Run the code.
5. The code will authenticate with the DLP API, retrieve the incidents within the specified date range, parse the response and write it to a JSON file.
6. For each incident, a ServiceNow incident will be created using the provided details.
7. If there are any errors during the process, they will be displayed in the console.

Note: This code assumes the availability of the DLP API and ServiceNow incidents API endpoints, as well as the necessary permission and access credentials.

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

© 2023 Forcepoint. Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
[FP DLP API and SerivceNow Configuration Guide] 06Nov2023