aims-ui-access.py

Created by: Michael Gupton
mgupton@alertlogic.com

Summary

aims-ui-access.py is a proof-of-concept that shows how to programmatically login to the Cloud Defender UI and access data from it. Accessing data in this way is generally motivated by the desire to consume data from Cloud Defender with some other tooling or solutions the customer is using. Ideally this kind of integration would be accomplished using an API.

The solution demonstrated in this script supplements the Cloud Defender functionality that is currently lacking a formal API. One example of this is accessing vulnerability assessment scan results.

An alternative way to get scan result data is to programmatically access the Cloud Defender UI and to manipulate the interface and fetch the data of interest. To fetch scan results from the UI two things are needed, a scan policy id and scan policy log id. The scan policy id identifies the scan configuration and the scan policy log id identifies a specific execution of the scan.

A webhook handler/receiver could be used to get a notification when a scan job completes, which could be used to trigger a solution to lookup the scan results. Currently, the webhook notification for a scan job includes the scan policy id, but not the scan policy log id. And the notification does not include a URL to the scan results. Using logic, like that demonstated in this POC, requests to the UI can be made using the scan policy id to acquire the scan policy log id. With the scan policy log id another request can be made to fetch the scan results CSV data.

This script shows how to authenticate with the Cloud Defender web console and then read the scans page for the latest scan results for a specified scan policy.

Dependencies

- Requests module
- BeautifulSoup module

Use the requirements file to install the modules.

```
pip install -r requirements.txt
```

Usage

```
python aims-ui-access.py -u %username% -p %password% [-o <policy_id>] [-f <output_file>]
```

-u/--username is a valid user name for accessing the Cloud Defender UI.
-p/--password is the password for the user account.
-o/--policy_id is an optional scan policy id. If provided the latest scan results for that policy will be downloaded. -f/--output_file is an option file that the scan results will be written to.

Fetching Scan Results CSV files/data

For each scan that is configured there is a policy id, which is a unique number that identifies the scan configuration. Each time a scan runs there is a unique number that identifies that execution. That value is called the policy log id. Using the policy id and policy log id the scan results can be accessed.

1. First, request the page that list all the scan results for a specified scan policy.

- Example URL, https://console.alertlogic.net/ajax_handler.php?cat=get_scan_results&policy_id=4223

2. Then loop over the list of results and get the policy_log_id for each one and sort the list in descending order. In descending order the most recent scan result will be first.1

3. Then select the first value, which represents the most recent scan result. Request the URL for the CSV file and specify the scan policy id and policy log id.

- Example URL, https://console.alertlogic.net/reports/csv/vuln_by_scan.php?policy_id=4223&policy_log_id=13956

Using Webhooks for scan completion notifications

A scan configuration/policy has an option to send a notification email or webhook request when a scan completes. By using a webhook notification an automated system can be implemented to fetch the results. The details of this are outlined below.

1. Implement a webhook receiver to receive the webhook requests from Cloud Defender.
2. Configure a webhook in Cloud Defender and give it the URL for the receiver endpoint.
3. Configure the scan policy to send a notification to the webhook.
4. When a scan runs and completes a webhook notification will be sent to the configured endpoint. The policy id for the scan policy that completed will be in the data provided in the webhook request.
5. The webhook endpoint can take the policy id and lookup the policy log id.
6. With the policy id and policy log id a request can be made to to the UI to fetch the scan results CSV data.