



IDENTITY FLOWS INTEGRATION

(Changing Authentication Policy based on SentinelOne Risky Person)

IDENTITY FLOWS - TECHNICAL DOCUMENTATION TEMPLATE

Name of Company: SentinelOne

Website: <https://www.sentinelone.com>

Name of Product: Singularity

Version: Any SaaS Version

Date: 05.15.23

PARTNER SOLUTION OVERVIEW

SentinelOne Singularity XDR unifies and extends detection and response capability across multiple security layers including endpoint, cloud, identity, network, and mobile providing security teams with centralized end-to-end enterprise visibility, powerful analytics, and automated response across a large cross-section of the technology stack.

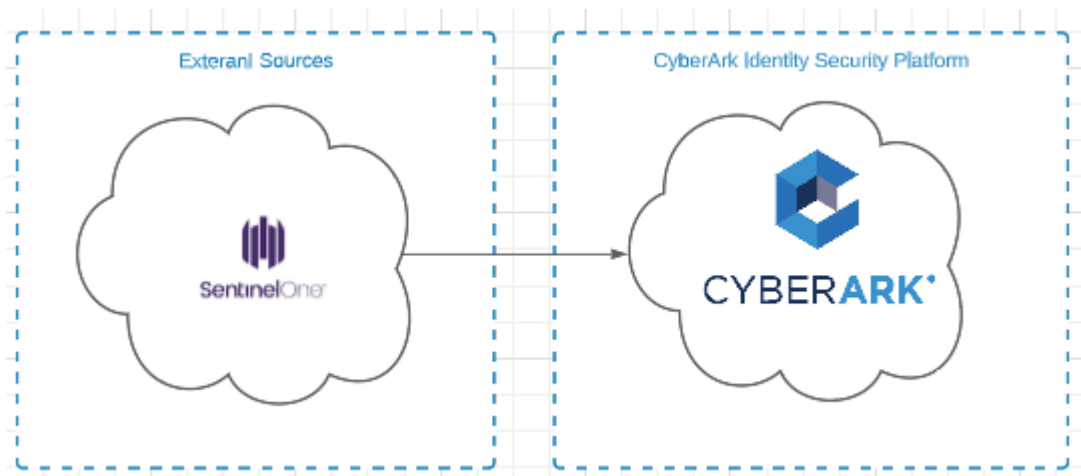
Sentinel Agents are managed via our globally-available multi-tenant SaaS console designed for ease of use and flexible management that meets your requirements. Our Vigilance Managed Detection & Response (MDR) services subscription is available to back your security organization 24x7.

KEY BENEFITS

Enable real-time risk-based access policy enforcement of authentication levels for user's access to systems, devices, and applications. Determine access control permissions and restrictions based on a user's risk score versus hardcoded rules. A real-time risk score is calculated based on user outlier behavior percentage, resident user risk and reputation, and data or transaction risk classification. This score is then used to make real-time authentication and access decisions, while simplifying the user experience and enhancing security.

- Significantly enhance user experience based on the user behavior patterns
- Identify changes in user behavior before any security incident happens or data is exfiltrated

PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



REQUIREMENTS

List software, network, and hardware requirements. Provide context of requirements and team expertise for user planning needs.

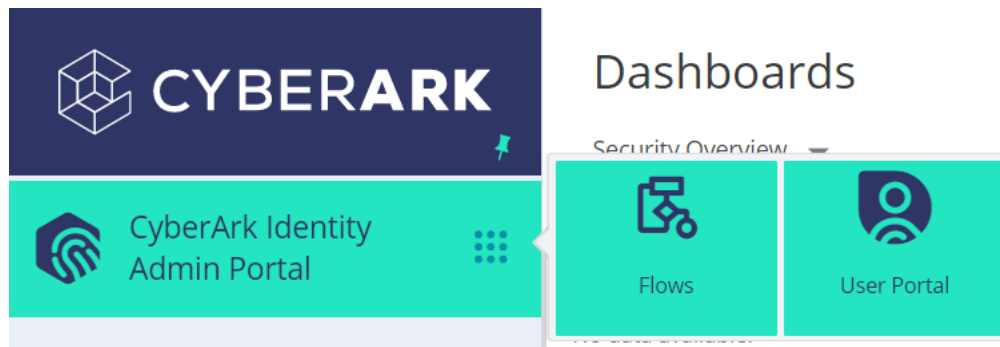
- CyberArk Identity tenant
- CyberArk Flows tenant
- SentinelOne Singularity with Identity Surface tenant

FLOWS TEMPLATE INSTALLATION

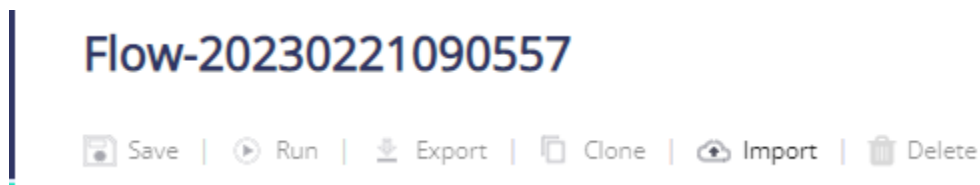
The [CyberArk Marketplace](#) contains two files. This integration guide and a CyberArk Identity Flows JSON file that contains the template for this integration.

Once you have the JSON file, you can import it into your Identity Flows tenant.

Login to your CyberArk Identity tenant and Launch Flows from the waffle menu.



The CyberArk Identity Flows builder will launch in a new tab.



Once the Flows Builder loads, On the Action Menu at the top of the screen **Click** on the **Import** button.

Upload From Computer ×



Drop or upload

The Upload dialog box will launch after Clicking the Import button. Either drag the **SentinelOne – Risky Persons. Json** onto the Upload dialog or **Click the Cloud with the Up Arrow** to select the file.

SENTINELONE API KEY

To define a SentinelOne API client, **you must be designated as Singularity Administrator** to view, create, or modify API clients or keys. **Secrets** are only shown when a new API Client is created or when it is reset.

When logged into the Singularity UI, navigate to **Support > API Clients** and Keys. From there you can view existing clients, add new API clients, or view the audit log. When you click “Add new API Client” you will be prompted to give a descriptive name and select the appropriate API scopes. After you click save, you will be presented with the Client ID and Client Secret. The secret will only be shown once and should be stored in a secure place. If the Client Secret is lost, a reset must be performed and any applications relying on the Client Secret will need to be updated with the new credentials.

API clients				+ Add new API client	See action log
Client name	Created	Last modified	Client ID	Actions	
QRadar Integration	Apr. 5 12:24:02	Apr. 5 12:24:02	e00000000000000000000000...	Edit	Reset
Compliance/Audit Team Too...	Mar. 28 10:54:06	Mar. 28 10:54:06	f00000000000000000000000...	Edit	Reset
ServiceNow Integration	Jan. 4 12:38:11	Jan. 4 12:38:11	g000000000000000000000000...	Edit	Reset
Devices Manager	Jan. 4 12:37:51	Jan. 4 12:37:51	h000000000000000000000000...	Edit	Reset

Add new API client
×

CLIENT NAME

Systems Administrator Access

DESCRIPTION

API SCOPES

	Read	Write
Detections	☐	☐
Hosts	☒	☒
Host groups	☐	☐
Prevention policies	☐	☐
Sensor update policies	☒	☒
User management	☐	☐

CANCEL

ADD

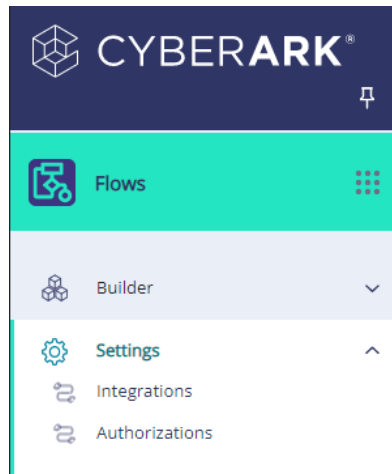
FLOWS CONFIGURATION

To configure the flow for your tenants the following Items must be changed:

- Configure Authorizations for SentinelOne.
- Configure CyberArk Identity OAuth2 Client.
- Configure Authorizations for CyberArk Identity.
- Configure the Hostname on all connectors
- Set the Risky Persons GUID

CONFIGURING SENTINELONE AUTHORIZATION

To define configure the authorization for SentinelOne go into the **Settings** section in the Flows Builder menu on the **Left-hand** side of the builder.



Click on the **Authorizations**. This will launch the **Manage Authorizations** dialog box where you can configure all the Authorizations needed for the **SentinelOne – Risky Persons** Flow.

Manage Authorizations

New Authorizations X

Q Search Authorizations

Auth Name	Auth Type	Actions
Identity - AAS4010	oauth2	
S1- SRF	apiKey	
Identity - AAH4087	oauth2	
Google E3	oauth2	
Jira E3	oauth2	

Settings

Name*

S1- SRF

Type*

API Key

Api Key Location*

query

Api key Name*

apiToken

Api key Value*

Reset

Update

To configure an Authorization for **SentinelOne**. For the **Name** enter **SentinelOne**. On the **Type**, Select **API Key**. For the **API Key Location** select **query**. In the **API Key Name** input “**apiToken**”. In the **API Key Value** enter the **API Key** generated in the previous step. In the **Client Secret** enter the **Client Secret** generated in the previous step.

CYBERARK IDENTITY OAUTH2 CLIENT

There are several steps in creating an OAuth2 Client inside of CyberArk Identity:

- Create a User to use as the ClientID and Client Secret.
- Create a OAuth2 Client Web App

CREATE A USER

Login to the CyberArk Identity Admin Portal, go to **Core Services->Users** and click **Add User**. Set up an API Service User like this, using your own domain instead of greentech.com.

apiuser@greentech.com

Type: CyberArk Cloud Directory User

Last Login: 12/09/2021 3:31:48 PM

Status: **Active**

Account

Activity

Application Settings

Assigned Applications

Endpoints

Roles

Provisioned Applications

Additional Attributes

Policy Summary

Identity Verification Details

Account
[Learn more](#)

Login Name *

apiuser

Suffix

@ greentech.com

Email Address

apiuser@greentech.com

Display Name *

API User

Status

☐ Locked

☒ Password never expires

☐ Require password change at next login

☒ Is Service User

☒ Is OAuth confidential client

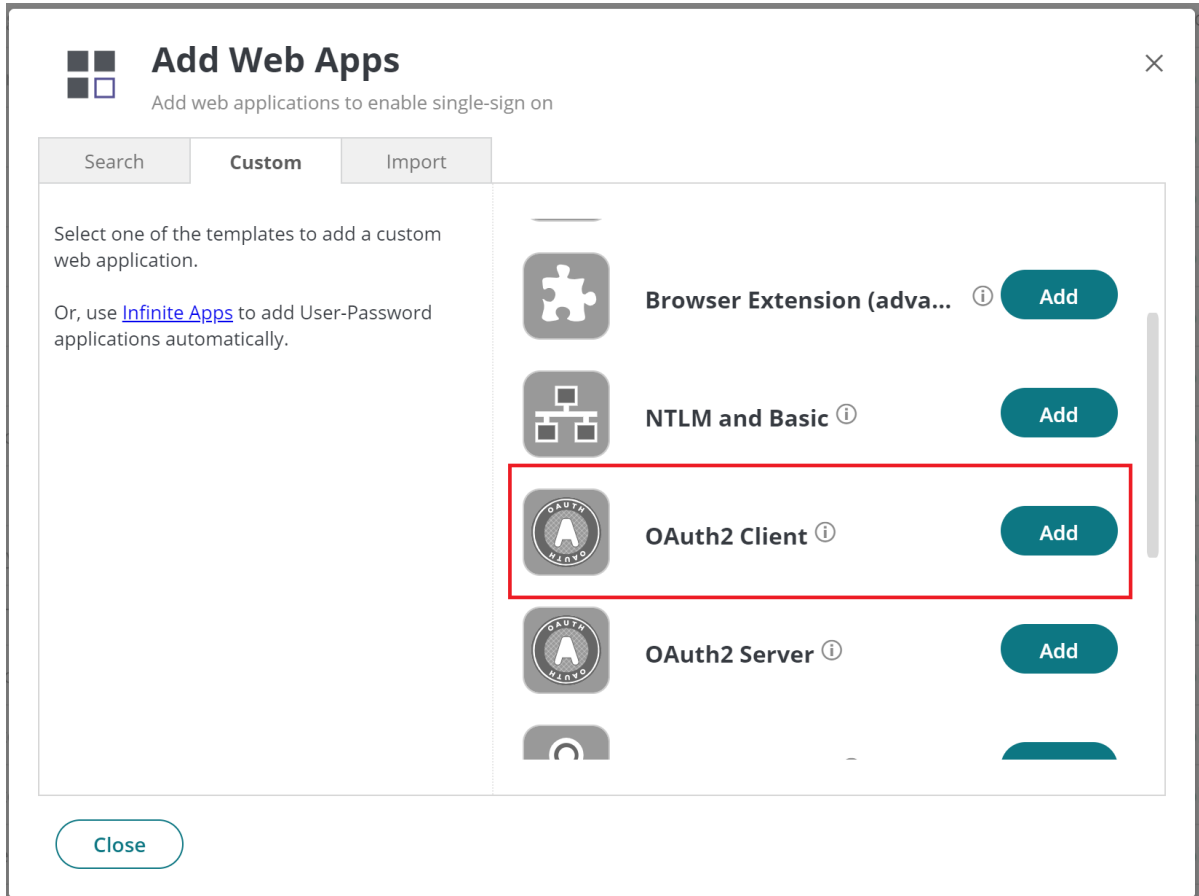
☐ Send email invite for user portal setup

☐ Send SMS invite for device enrollment

Next go to **Roles**, click **System Administrator**, and add the **apiuser** to that Role.

CREATE AN OAUTH2 CLIENT WEB APP

To create a new OAuth2 Client go to **Apps->Web Apps** and click **Add App**. This will launch the Web App selection page.



Click the **Custom Tab** up top and select the **OAuth2 Client**.

Add Web App



OAuth2 Client

Description

Use this template to set up an application that is making OAuth secured REST calls to the Idaptive Platform

Do you want to add this application?

Yes

No

Click **Yes** to add a new OAuth2 Client.

Add Web Apps

Add web applications to enable single-sign on

Search

Custom

Import

Select one of the templates to add a custom web application.

Or, use [Infinite Apps](#) to add User-Password applications automatically.

Bookmark ⓘ

Add

Browser Extension ⓘ

Add

Browser Extension (advanced) ⓘ

Add

NTLM and Basic ⓘ

Add

OAuth2 Client ⓘ

Add

Close

Then select **Close** down at the bottom. This will launch the Configuration Wizard.



CyberArk Identity API

Type: **Web - Other Type**

Status: **Deployed**

Settings

General Usage

Tokens

Scope

Permissions

Changelog

Secure Web
Sessions

Settings

[Learn more](#)

Application ID  

IdentityAPI

Description

☐ Customize Name and Description for each language 

Name 

CyberArk Identity API

Description

OAuth2 Client for Identity API

Category 

Other

Logo



[Browse](#)

Recommended image size is 180 x 180

On the **Settings** Tab, Enter the Following information. Enter the **Application ID** and **Name** of the WebApp. If you do not name your **Application ID** as **IdentityAPI** please note it down including the Case used. Since this ID is case sensitive. You will need this ID in later configuration of Flows Authorization.



CyberArk Identity API

Type: Web - Other Type

Status: **Deployed**

Settings

General Usage

Tokens

Scope

Permissions

Changelog

Secure Web
Sessions

General Usage

Client ID Type

☐ Anything

☐ List

☒ Confidential

☒ Must be OAuth Client

Confidential client is an CyberArk Cloud Directory user. [Click here to create one.](#)

Issuer

https://aae4199.my.idaptive.app

Allowed Redirects

Add

Redirect destinations

https://oauth.pstmn.io/v1/callback



Select on the **General Usage** Tab. In this screen you will need to add a call back URL in the **Redirect destinations**: **Select** the **Add** button. You will need to add the following URL replacing the TENANT section in the URL with your Tenant ID:

https:// TENANT.flows.cyberark.cloud/gateway/callback



CyberArk Identity API

Type: Web - Other Type

Status: Deployed

Settings

General Usage

Tokens

Scope

Permissions

Changelog

Secure Web
Sessions

Tokens

Token Type *

JwtRS256

Auth methods *

☐ Auth Code

☐ Implicit

☒ Client Creds

☐ Resource Owner

Token Lifetime *

5 hours

☒ Issue refresh tokens

Refresh token lifetime *

365 days

Select the **Tokens** Tab. Confirm that the **Token Type** is **JwtRS256** next select the Auth Methods of **Auth Code** and **Client Creds**. Check the **Issue refresh tokens** and leave the default of 365 Days.



CyberArk Identity API

Type: Web - Other Type

Status: Deployed

Settings

General Usage

Tokens

Scope

Permissions

Changelog

Secure Web
Sessions

Scope

☐ User must confirm authorization request

☐ Allow scope selection

Scope definitions

Add

Name	Description	Filters	
all		.*	

Select the **Scope** Tab, then **Click Add** and give it a Name of **all** and a filter of **.*** as you see above.
Note the name of the scope is case sensitive.

Under Permissions, add your **apiuser** and give that user all rights.

CyberArk

CyberArk Identity API

Type: Web - Other Type Status: Deployed

Settings

General Usage

Tokens

Scope

Permissions

Changelog

Secure Web Sessions

Permissions

[Learn more](#)

Add

	Name	Grant	View	Manage	Delete	Run	Automatically D...
☐	alero-integration-user\$@...	☒	☒	☒	☒	☐	☐
☐	Read Only Admin	☐	☒	☐	☐	☐	☐
☐	sws-integration-user\$@cy...	☒	☒	☒	☒	☐	☐
☐	sysadmin	☒	☒	☒	☒	☐	☐
☐	Technical Support Access	☐	☒	☐	☐	☐	☐
☐	apiuser@greentech.com	☒	☒	☒	☒	☒	☒

Select the **Permissions** tab, add your **apiuser** that you created in the first steps and give that user **View** and **Run** rights.

CYBERARK IDENTITY FLOWS AUTHORIZATION

In Flows on the Builder Menu **Select** on **Settings** then **Authorizations**. This will launch the **Manage Authorizations** page.

Manage Authorizations New Authentication

Auth Name	Auth Type	Actions
Slack E3	oauth2	
Duo	hmac	
Cyberark Identity AAH4087	oauth2	
Bamboo HR	basic	
Slack Bot E3	apiKey	
Cyberark Identity - AAS4010	oauth2	

Settings

Name*

Type* OAuth2

Flow Authorization Code

Content Type application/json

Client ID

Client Secret

Auth Token

Reset Authorize Save

Once the Manage Authorization screen loads. Select **OAuth2** as the **Type** and give it a descriptive name such as **Product – Tenant ID**. Next, select the OAuth **Flow** that you will be using.

Setup of the OAuth2 Client will support both the **Auth Code** and **Client Creds** flows. If you use the **Client Creds** flow you will need to change the Content-Type to be **application/x-www-form-urlencoded**.

Next, fill in the **Client ID** with the **Username** that you created in the first step. Set the **Client Secret** to be the **Password** you set on that user.

Next, scroll down on the Authorization configuration screen to get to the remaining configuration settings. So the **Authorization URL**, **Token URL** have some Tenant specific settings. For the **Authorization URL** specify it in this format:

<https://TENANT.id.cyberark.cloud/oauth2/authorize/APPLICATION ID>

The **Application ID** can be obtained from the OAuth2 Client configuration we completed before. It should be set to **IdentityAPI** if you followed these instructions.

For the Token URL specify in this format:

<https://TENANT.id.cyberark.cloud/oauth2/token/APPLICATION ID>

Note: If you had Flows enabled on an older tenant you will need to use the host name format of **TENANT.my.idaptive.app** instead of **TENANT.id.cyberark.cloud**.

Manage Authorizations

Search Authorizations

Auth Name	Auth Type	Actions
Cyberark Identity - AAS4010	oauth2	 
Microsoft Dev	oauth2	 
Proofpoint VAP	basic	 
Gurukul	apiKey	 
CorePAS	basic	 
Gurukul Dummy	apiKey	 

Refresh Token

.....

Authorization URL *

https://aas4010.id.cyberark.cloud/oauth2/authorize/identityapi

Token URL *

https://aas4010.id.cyberark.cloud/oauth2/token/identityapi

Redirect URL[Set this as the Redirect URL in your app settings page]

https://aal7307.cybrflows.com/gateway/callback

Scopes

☒ Scopes

☒ Scope

all

Description

all



+Add

Reset

Reauthorize

Update

Finally, we need to do is set the **Scopes**. Click on the **Add** button and set the **Scopes** to **All** and the **description** to **All**. At this point the configuration is done. Click **Save** or **Update**. Now you are ready to test the Authorization. Click the Authorize/Reauthorize button. This will kick off the OAuth2 flow and try to obtain an **Access Token** and a **Refresh Token**.

If there are any errors here are the following things to check:

- Is your Application ID and Tenant ID correct in your Token and Authorize URLs? Case Sensitive!
- Is your Scope set correctly? Case Sensitive!

- Are your Client ID and Client Secret Correct?
- Does the user we created in the first step in Identity have View and Run permissions to the OAuth2 Client?
- Is the user created in the first step in a Role that gives them admin permissions in Identity?

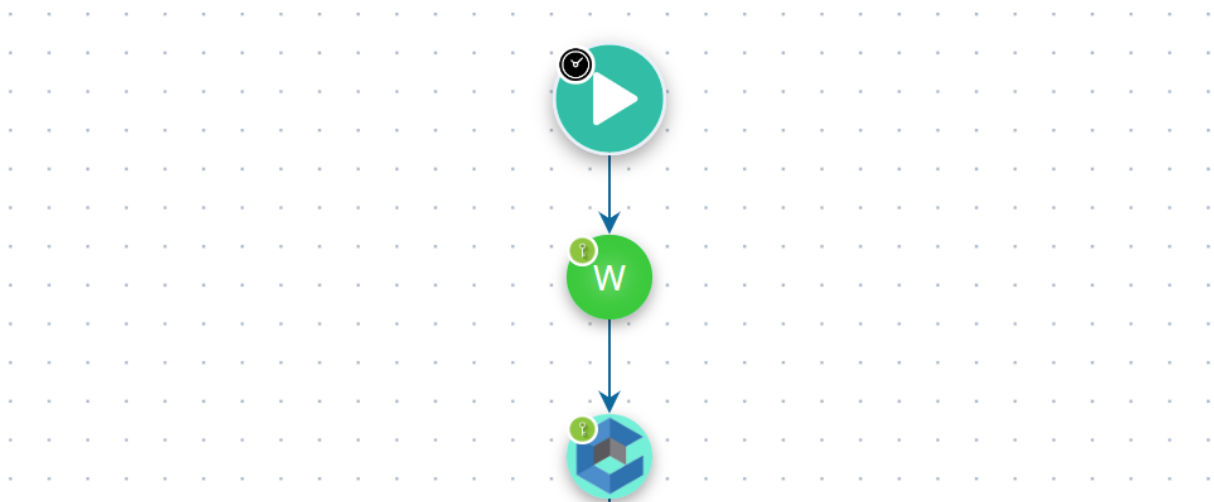
Once you have your Authorization configured and returning Tokens you can proceed to the next section.

CONFIGURING FLOW CONNECTORS

Now that we have all of the needed Authorizations configured for the Flow, we need to configure each connector to use the proper Authorization.

S1 - Risky Persons

Save | Run | Export | Clone | + Import | Delete



Select the **SentinelOne** connector in the Flow. This will open the **Connector Menu** on the right-hand side of the Builder. Click the **Down Arrow** on the **Authorizations** and Select the **SentinelOne** Authorization you setup in the previous step. We do not need to change the SentinelOne hostname because SentinelOne uses a common API endpoint for all Tenants.

Save | Run | Export | Clone | + Import | Delete

+ 100% | New flow | Refresh

Web Api V2.1 Threats

Settings | Map

Authorizations Clear Manage

S1- SRF
apiKey authentication

☐ Force User Authorizations

Connector Settings

Hostname
usea1-partners.sentinelone.net

Next, **Select** the **Cyberark** connector in the Flow. This will open the **Connector Menu** on the right-hand side of the Builder. **Click** the **Down Arrow** on the **Authorizations** and **Select** the **CyberArk Identity** Authorization you setup in the previous step.

We need to change the hostname to your CyberArk Identity Tenant. If you have an older CyberArk Identity tenant your hostname format will be: **tenant.my.idaptive.app**. Newer CyberArk Identity or ISPSS tenants will have the following format: **tenant.id.cyberark.cloud**. Where “tenant” is replaced with your **Tenant ID**.

Repeat this step for every CyberArk connector in the Flow.

At this point you should be able to Run flow. Once you are happy you can configure the Flow to run on a schedule. CrowdStrike VAP scores are only calculated 1 time per day. So best to schedule this Flow to run once a day.

PARTNER CONTACT INFO

Business Contact	Name	Megan Eiszler
	Email	Megan.eiszler@sentinelone.com
	Tel	
Technical Contact	Name	
	Email	
	Tel	
Support Contact	Name	
	Email	
	Tel	