



# CYBERARK SECRETS MANAGER

**(Agentless Central Credential Provider CCP)**

## SECRETS MANAGER INTEGRATION - TECHNICAL DOCUMENTATION

Name of Company: DFLabs

Website: [www.dflabs.com](http://www.dflabs.com)

Name of Product: DFLabs IncMan SOAR

Version: 5

Date: 10 March 2021

## DFLABS INCMAN SOAR OVERVIEW

DFLabs is a pioneer, and a globally recognized industry leader in security orchestration, automation, and response (SOAR) technology. The company's management team has helped shape the cyber security industry, which includes co-editing several industry standards such as ISO 27043 and ISO 30121. Its award-winning product, IncMan SOAR, is a multi-patented technology and has been adopted by Fortune 500 and Global 2000 organizations worldwide. DFLabs has operations in EMEA Americas and APAC. For more information, visit [www.dflabs.com](http://www.dflabs.com).

Version: 5

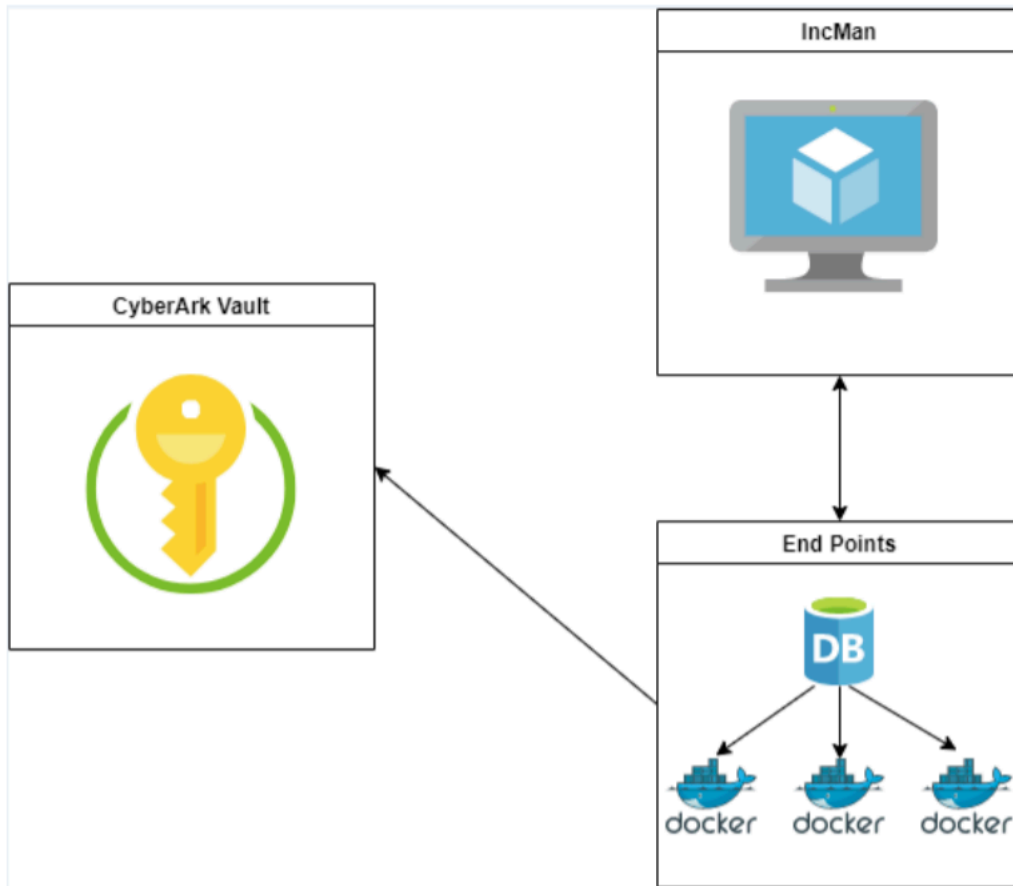
## KEY BENEFITS

Benefits of IncMan SOAR:

- All-in-one platform to empower SecOps
  - Easily orchestrate your tools leveraging Open Integration Framework
  - Playbooks improve SecOps processes and allow analysts to follow Standard Operating Procedures (SOP)
  - Better resource allocation based on task priorities
  - Advanced forensics and case management features
- Save time and focus on real threats
  - “Progressive” automation of time-consuming activities and mundane tasks
  - Significant reduction of false positives with an accurate enrichment and validation of alarms
  - Analysis of alarms before incidents are created
  - Deduplication feature (incidents with similar characteristics are merged)
- Measure success and improve communication
  - Manage the escalation process and allows multiple analysts to work simultaneously on incidents
  - Notify stakeholders when its important
  - Immediate and detailed incident reports with related IOCs, timeline and corrective actions executed
  - Customized role focused KPIs dashboard to monitor incidents and S.L.A.
- Native multi-tenancy platform
  - Centralized management with aggregated reporting and high visibility on tenants
  - Propagate standards from master to tenant (e.g. playbooks, custom fields, etc.))
  - Physical data segregation

DFLabs' IncMan SOAR is a Technology Platform for MSSPs, SOC's and security teams to enable collaborative and automated real-time incident management, threat and data breach response.

## PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION



## SECRETS MANAGER INTEGRATION

DFLabs's IncMan integrates CyberArk Secrets Manager API (CCP) using a specific abstraction level called IncMan OIF (Open Integration Framework). In a very simple way the end user can define the integration connector and the actions that can be executed using CyberArk Secrets Manager. In this case a couple of action are defined: get account details and upload certificate. First action represents the core of the integration; the second action is needed to setup the integration.

Location of integration: Each endpoint is designed as an integration/connector and actions and the code of the integration is stored in a DB on Linux based VM. Each endpoint is executed inside a docker container for security reasons and to isolate execution respect the IncMan system space. Every time the action "Get account details" is executed, the results are stored in the IncMan database. The IncMan application can be setup as located virtual machine or can be hosted remotely respect CyberArk Secrets Manager or in cloud. The only requirement is that the HTTPS (if a specific port is needed can be customized at IncMan configuration level as described below) path from IncMan to CyberArk Secrets Manager system is open.

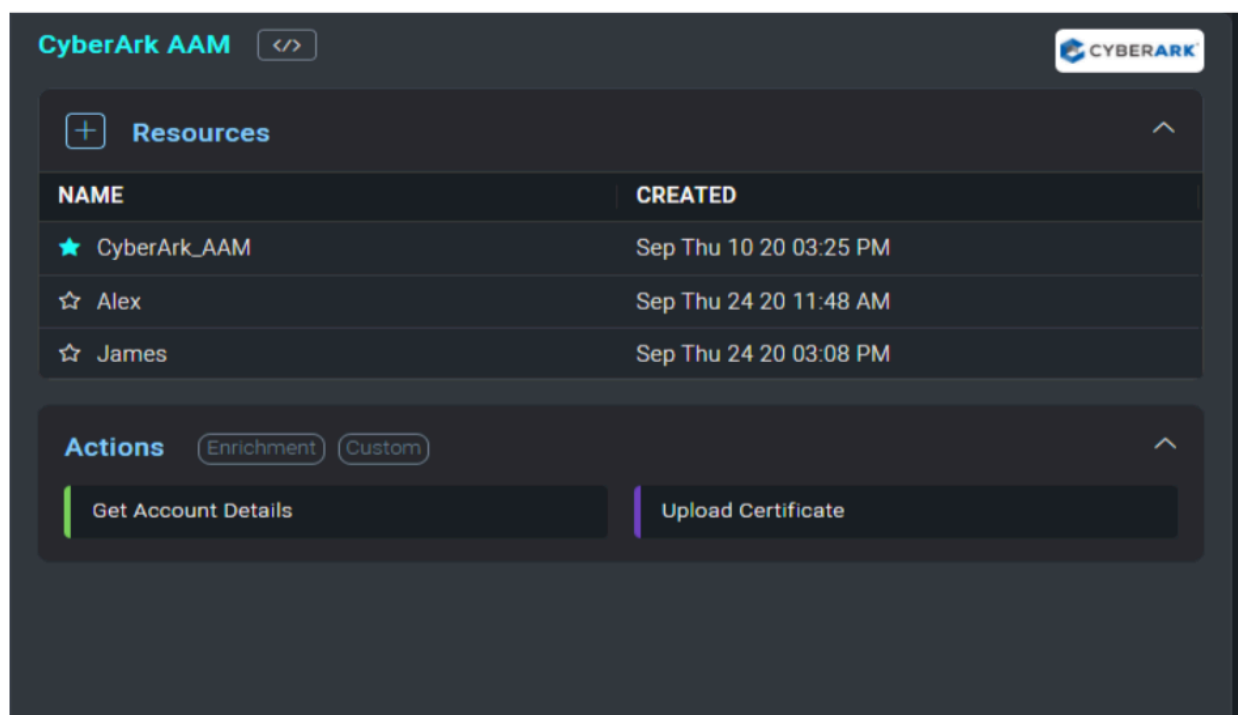
## CREDENTIAL RETRIEVAL

The credential retrieval (Get Account Details) is an enrichment action for our SOAR platform. Enrichment means that no modification is made into CyberArk Secrets Manager but only get operations are accomplished.

Once credentials are retrieved in IncMan, they can be used inside a playbook whenever needed, for other actions and various integrations. The trigger for the action/endpoint is when an incident is created inside IncMan and the playbook containing the action is executed.

**Below is the guide for retrieving credentials from CyberArk, through IncMan:**

1. Create resource in the integration CyberArk Secrets Manager with only Label and Server populated for now.



+ Resource

×

Label

James

Server \*

https://services-uscentral.skytap.com:<port>/

Certificate

client.crt Use action Upload Certificate to get this value

Key

client.pem Use action Upload Certificate to get this value

Root

RootCA.crt Use action Upload Certificate to get this value

Proxy Options

Use no proxy

▼

SAVE

2. Upload the certificates (located on CyberArk environment) in incident attachments section (certificate=client.crt, Key=client.pem, Root=RootCA.crt)

Add attachment

Browse your computer or Drop files here

Files:

RootCA.crt
client.crt
client.pem

Change Folder

/

Description

B I U S I\_x

SAVE

INC MAN
INCIDENTS
ENTITIES
in: global

CyberArk\_AAM
Opening time: 21/09/2020 11:20...
Type: Incident Response
Status: Open

OVERVIEW
OPERATIONS
ENTITIES
DOCUMENTATION

ACTIVITY LOG
ATTACHMENTS
REPORT
CONTACTS

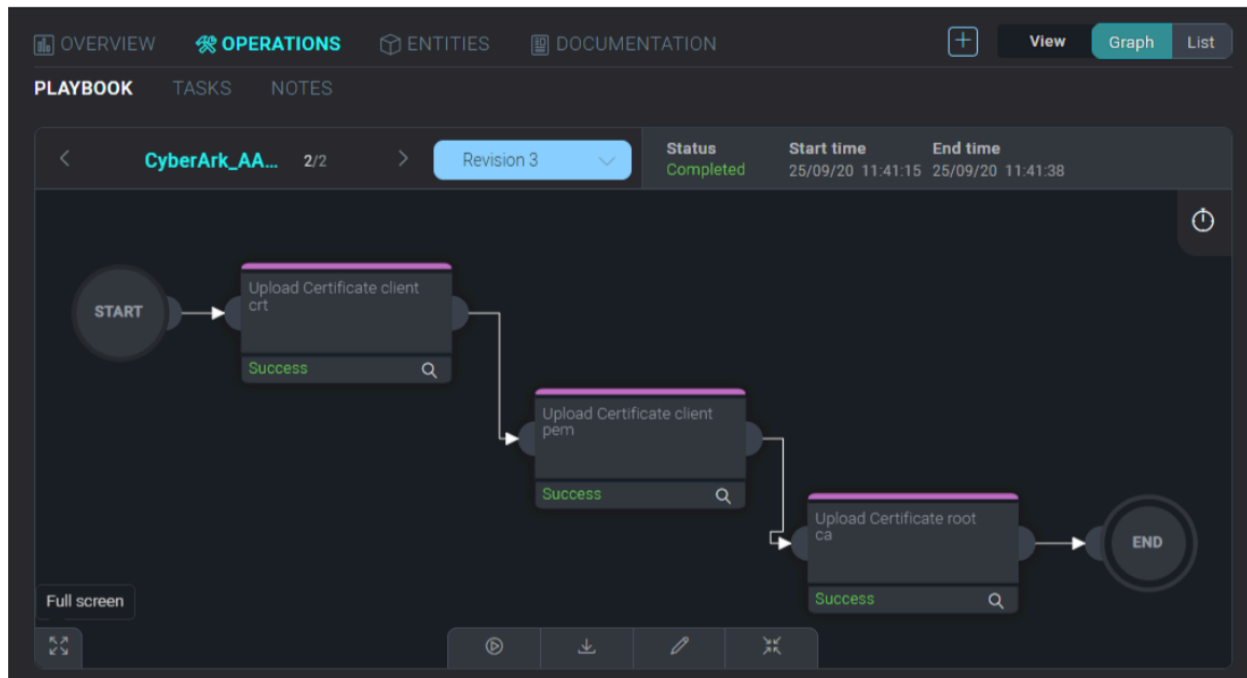
+
Search

NEW FOLDER
DOWNLOAD ALL
EXPORT

RootCA.crt
client.crt
client.pem

ADD INVESTIGATORS
CLOSE INCIDENT

- Create and run a playbook that has the action Upload Certificate three times, with the selected certificates (client.crt, client.pem and RootCA.crt)



4. Copy the results (string) and paste them correspondingly in the resource configurations

The screenshot shows the CyberArk console interface with the "INCIDENTS" tab selected. On the left, there is a sidebar for "CyberArk\_AAM" with details: "Opening time: 21/09/2020 11:20...", "Type: Incident Response", and "Status: Open". Below this are buttons for "ADD INVESTIGATORS" and "CLOSE INCIDENT". The main area displays the results of the playbook execution, showing three steps: "Upload Certificate Client Cr...", "Upload Certificate Client P...", and "Upload Certificate Root Ca...", all marked as "SUCCESS". Each step shows a JSON response with a "file" field containing a long string of characters. The interface also includes tabs for OVERVIEW, OPERATIONS, ENTITIES, and DOCUMENTATION, and a search bar at the top.

**Resource**✕

**Label**

James

**Server \***

https://services-uscentral.skytap.com:11111/

**Certificate**

\*LS0tLS1CRUdJTlBDRVJUSUZJQ0FURStLS0tCk1JSUV2ekNDQTZlZ0f

**Key**

\*LS0tLS1CRUdJTlBSU0EgUFJJVWkFURSBkRVktLS0tLQpNSUlfFb3dJQkFt

**Root**

|LS0tLS1CRUdJTlBDRVJUSUZJQ0FURStLS0tCk1JSUVGRENDQXZ5ZI

**Proxy Options**

Use no proxy▼

**SAVE SETTINGS**

5. Run the action Get Account Details with provided values for App ID, Safe name, Folder and Object name (this can be done either with Test Action, or in playbook)

### Test Action

Run Get Account Details over CyberArk AAM

Resource \*

James

APP ID \*

TestAPPID

Safe \*

Test

Safe name

Folder \*

Root

Folder name

Object \*

TestObject

Object name

TEST ACTION

6. The result would be the retrieved credentials from CyberArk

Show Details

SUCCESS ⓘ

Search in table

| USERNAME | CONTENT | POLICY ID | PASSWORD CHANGE IN P... |
|----------|---------|-----------|-------------------------|
|          |         |           |                         |

CLOSE

The upload of the certificates is done only once per user, after that you can use the Get Credentials action as many times as needed.

If credentials are needed in some other action (depending on your use case) we suggest that you use Get Credentials action in playbook, and use the output as input in the next action.

## SECRETS MANAGER INSTALLATION

Refer to the “[Credential Provider Implementation Guide](#)” for CyberArk Agentless installation and configuration.

## SECRETS MANAGER CONFIGURATION

The following sections provide details on DFLabs IncMan SOAR configuration with CyberArk Secrets Manager.

### DEFINING THE APPLICATION ID (APPID) AND AUTHENTICATION DETAILS

To define the application, define it manually through the CyberArk Password Vault Web Access (PVWA) interface:

- ☐ Log in as user allowed to manage applications (it requires Manage Users authorization)
- ☐ In the Applications tab, click **Add Application**. The Add Application page appears.

**Add Application** Type: Certificate Serial Number (1 item)

Name: DFLabs-IncManAppID

Description:

**Business owner**

First Name:

Last Name:

Email:

Phone:

Location: \

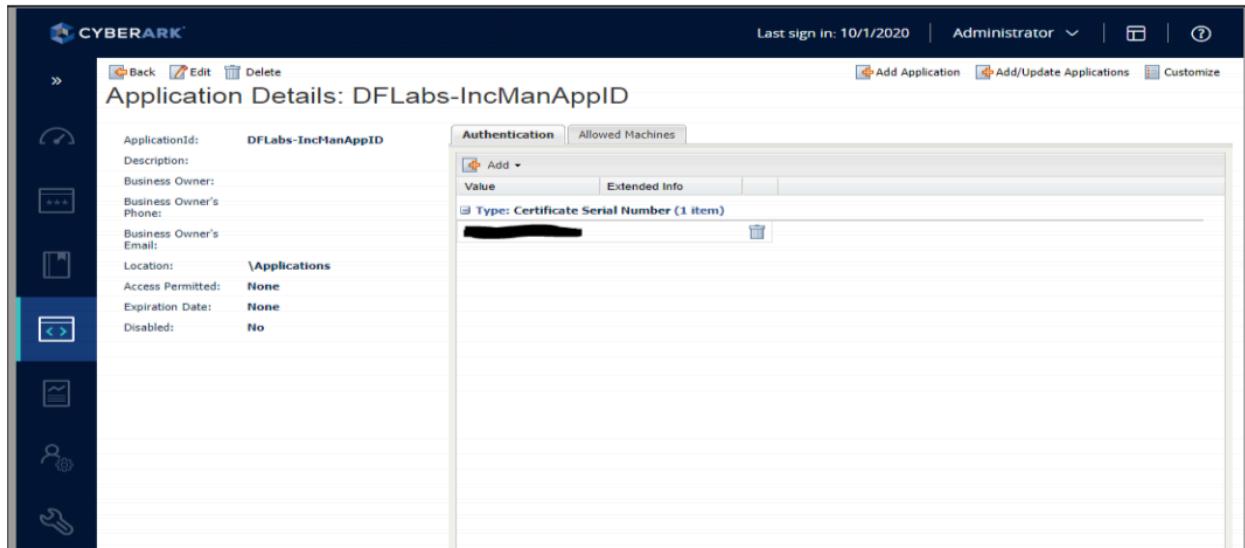
☐ Access Permitted: From: To:

☐ Expiration Date:

☐ Disabled

Add Cancel

- ☐ Specify the following information:
  - In the **Name** box, specify the unique name (ID) of the application. The recommended Application ID for this integration is: DFLabs-IncManAppID
  - In the **Description** box, specify a short description of the application that will help you identify it.
  - In the **Business owner** section, specify contact information about the application's business owner.
  - In the **Location** box, specify the location of the application in the Vault hierarchy. If a location is not selected, the application will be added in the same location as the user who is creating this application.
- ☐ Click **Add**. The application is added and is displayed in the Application Details page.



- ☐ Check the **Allowing extended authentication restrictions** box. This enables you to specify an unlimited number of machines and Windows domain OS users for a single application.
- ☐ Specify the application's **Authentication** details. This information enables the Credential Provider to check certain application characteristics before retrieving the application password.
- ☐ In the Authentication tab, click **Add**. A drop-down list of authentication characteristics is displayed.
- ☐ Select the authentication characteristic to specify.
- ☐ Select **OS user**. The Add Operating System User Authentication window appears.

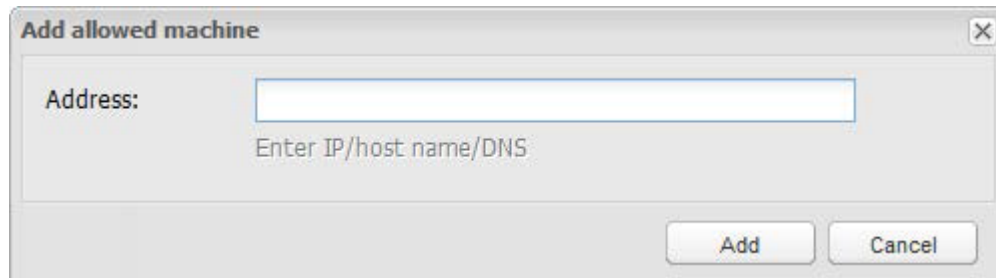
The screenshot shows a dialog box titled 'Add Operating System User Authentication'. It has a text field labeled 'OS User:' and two buttons: 'Add' and 'Cancel'.

- ☐ Specify the name of the OS user who will run the application, then click **Add**. The OS user is listed in the Authentication tab.
- ☐ Specify the Certificate Serial Number.

The screenshot shows a dialog box titled 'Add Certificate Serial Number Authentication'. It has a text field labeled 'SN:' and two buttons: 'Add' and 'Cancel'.

- ☐ Specify the application's Allowed Machines. This information enables Secrets Manager to make sure that only applications that run from specified machines can access their passwords.

- In the Allowed Machines tab, click **Add**. The Add allowed machine window is displayed.

A screenshot of a dialog box titled "Add allowed machine" with a close button (X) in the top right corner. Inside the dialog, there is a label "Address:" followed by a text input field. Below the input field, there is a placeholder text "Enter IP/host name/DNS". At the bottom right of the dialog, there are two buttons: "Add" and "Cancel".

- In the **Address** box, specify the IP/hostname/DNS of the machine where the application will run and will request passwords, then click **Add**. The IP address is listed in the Allowed Machines tab.

## PROVISIONING ACCOUNTS AND SETTING PERMISSIONS FOR APPLICATION ACCESS

For the application to perform its functionality or tasks, the application must have access to particular existing accounts, or new accounts to be provisioned in CyberArk Vault.

In the Password Safe, provision the privileged accounts that will be required by the application. You can do this in either of the following ways:

- **Manually** – Add accounts manually one at a time, and specify all the account details.
- **Automatically** – Add multiple accounts automatically using the Password Upload feature.

For this step, you require the **Add accounts** authorization in the Password Safe.

For more information about adding and managing privileged accounts, refer to **the Privileged Access Security Implementation Guide**.

Once the accounts are managed by CyberArk, make sure to setup the access to both the application and CyberArk Application Password Providers serving the Application.

Add the provider user (where the Central Credential Provider is installed) and application users as members of the Password Safes where the application passwords are stored. This can either be done manually in the Safes tab, or by specifying the Safe names in the CSV file for adding multiple applications.

☐ Add the Provider user as a Safe Member with the following authorizations:

- List accounts
- Retrieve accounts
- View Safe Members

**Note:** When installing multiple Providers for this integration, it is recommended to create a group for them, and add the group to the Safe once with the above authorization.

### Add Safe Member

Search: 
Search In:

Selected Search: Vault
Display 1 result(s)

|                                                                                   | Name               | Business Email | Full Name |
|-----------------------------------------------------------------------------------|--------------------|----------------|-----------|
|  | DFLabs-IncManAppID |                |           |

☐ Access

☒ Use accounts
☒ Retrieve accounts
☒ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☒ View Audit log
☒ View Safe Members

☐ Workflow

- ☐ Add the application (the APPID) as a Safe Member with the following authorizations:
- Retrieve accounts

**Add Safe Member**

Search:  Search In:

Selected Search: Vault Display 1 result(s)

| Name               | Business Email | Full Name |
|--------------------|----------------|-----------|
| DFLabs-IncManAppID |                |           |

☐ Access

☐ Use accounts

☒ Retrieve accounts

☐ List accounts

☐ Account Management

☐ Safe Management

☐ Monitor

☐ View Audit log

☐ View Safe Members

☐ Workflow

- ☐ If your environment is configured for dual control:
  - In Privileged Account Security solutions, when working with dual control, the Provider user can always access without confirmation, thus, it is not necessary to set this permission.
- ☐ If the Safe is configured for object level access, make sure that both the provider user and the application have access to the password(s) to retrieve.

For more information about configuring Safe Members, refer to the **Privileged Access Security Implementation Guide**.

## DFLABS INCMAN SOAR INSTALLATION & INTEGRATION CONFIGURATION

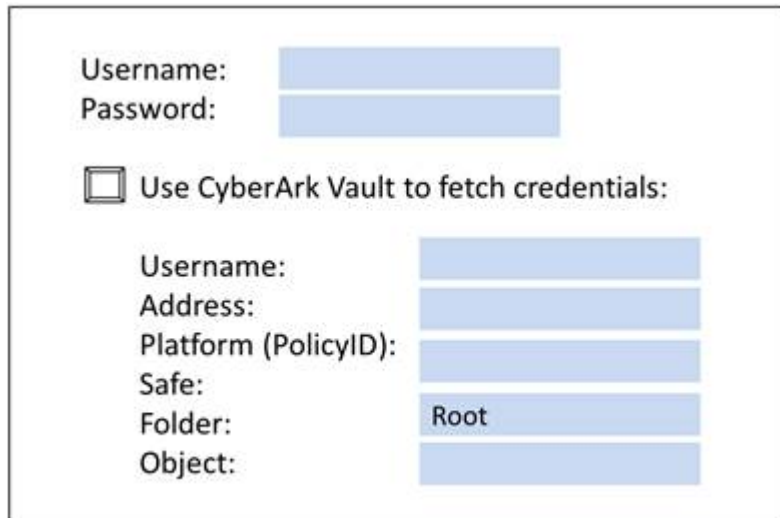
Refer to DFLabs for DFLabs IncMan SOAR installation.

List specific steps to configuring Partner Product to work with Secrets Manager, including:

1. Any special configurations within or outside the product
2. How to specify credentials for scanning, that are stored in the Vault (instead of providing usernames and passwords) – include screenshots and description of steps

>>Replace this screenshot with your actual integration configuration screenshots:

**Partner Application UI:**



The screenshot shows a configuration form for a Partner Application UI. It contains the following fields and options:

- Username:** [Text input field]
- Password:** [Text input field]
- ☐ **Use CyberArk Vault to fetch credentials:**
- Username:** [Text input field]
- Address:** [Text input field]
- Platform (PolicyID):** [Text input field]
- Safe:** [Text input field]
- Folder:** [Text input field with the value "Root" pre-filled]
- Object:** [Text input field]

## PARTNER CONTACT INFO

|                   |       |                   |
|-------------------|-------|-------------------|
| Business Contact  | Name  | Enrico Benzoni    |
|                   | Email | sales@dfllabs.com |
|                   | Tel   | +39 0373 82416    |
| Technical Contact | Name  |                   |
|                   | Email |                   |
|                   | Tel   |                   |
| Support Contact   | Name  |                   |
|                   | Email |                   |
|                   | Tel   |                   |