ServiceNow

Purpose: Integrate ServiceNow with CrowdStrike to generate tickets from IOM/IOA alerts.

Benefits: Streamline incident management by automating ticket creation and tracking for security events

Requirements:

1. Service Account with required permissions (ServiceNow Admin involvement)

2. ServiceNow domain

- Use this format: `crowdstrike.service-now.com`

3. Create a SOAR workflow within CrowdStrike that automates ticket creation based off IOM/IOA triggers
4. Work with ServiceNow admin to set up integration

Documentation utilized:

1. https://falcon.crowdstrike.com/documentation/page/dfe838e5/crowdstrike-store-app-integrations#fa465454
2. https://marketplace.crowdstrike.com/listings/ServiceNow-ITSM-SOAR-Actions

ServiceNow account must have required permissions below:

A ServiceNow user configured with necessary configuration and permissions:

- The User Level option **web-service access only** must be enabled for this user.
- The **personalize_choices** role must be assigned to this user, as this role provides access to the required ServiceNow tables.

ServiceNow Table	Required access	Table description
incident	Write	Used to create ITSM incidents
sys_user_group	Read	Used to populate User Groups to the Workflow UI (name and sys_id fields)
sys_choice	Read	Used to populate the category choices from an incident form (name and sys_id fields)
cmdb_ci	Read	Used to search for matching CI names for a given CrowdStrike Detection (name and sys_id fields)

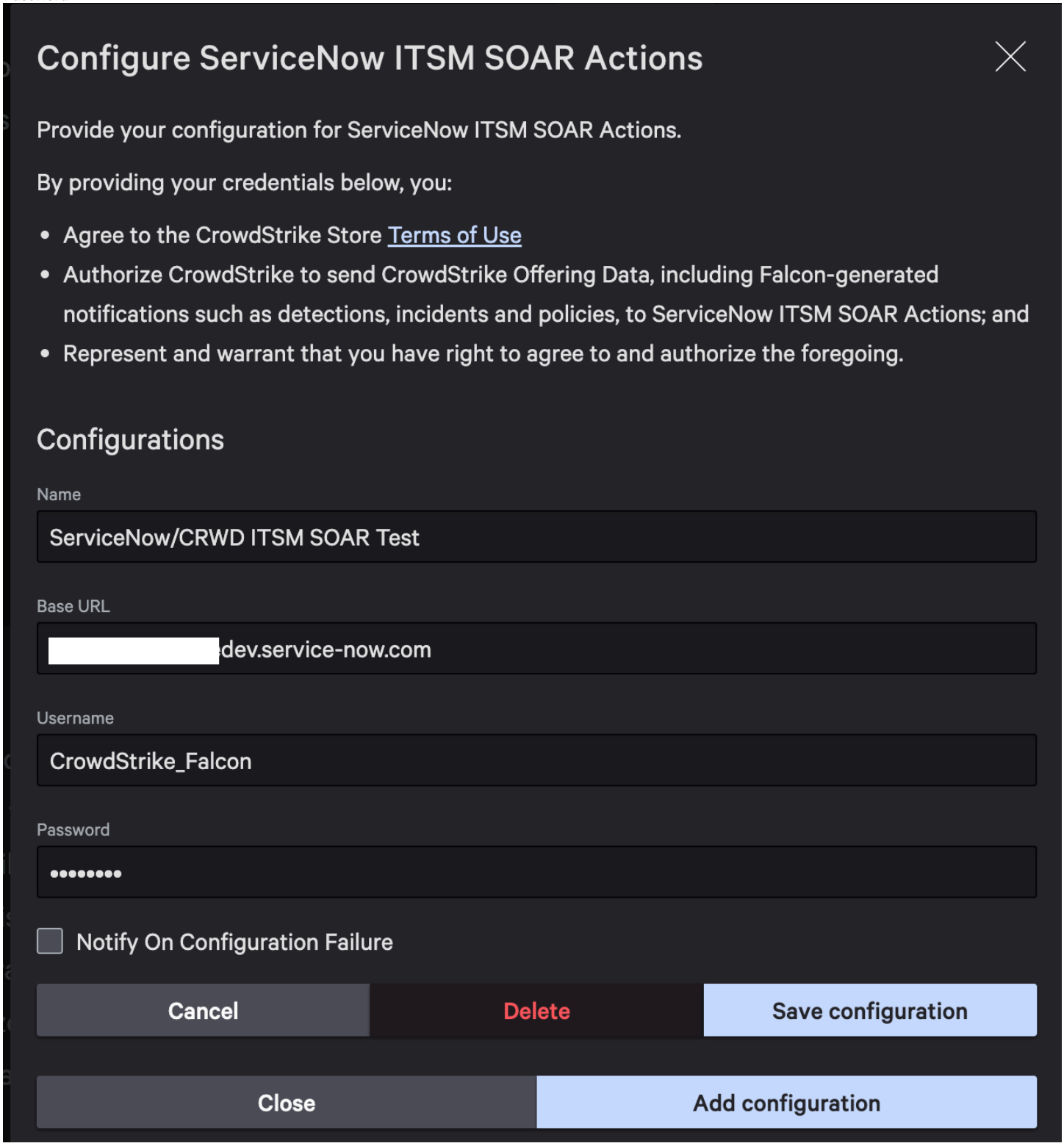
Creating the ServiceNow integration in the Falcon console

- Without this configuration, you will not be able to see "Create a ServiceNow Ticket" in Fusion SOAR workflows action.

1. Go to CrowdStrike store here -> https://falcon.crowdstrike.com/store-v2/5ec093b6cc1d4c29984e79689498f0df
2. Enter required info:

- Base URL: edev.service-now.com
- Username

- Password

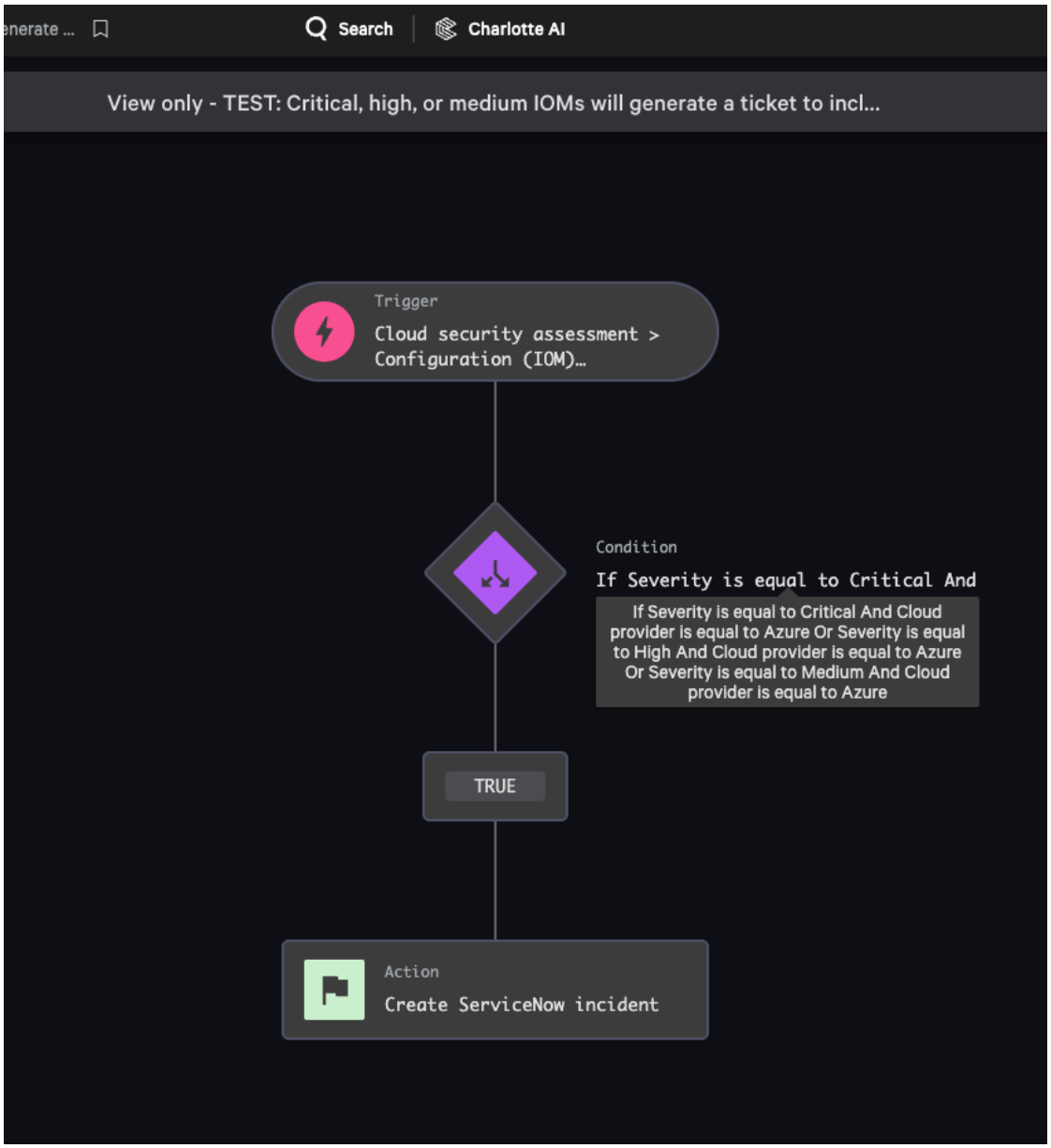


3. Click **Save configuration**.
   Note: This info was provided by Dave Miles

ServiceNow is now an action option when you create a workflow. When you define the action, you can customize it using values generated from your ServiceNow instance.

Azure Only SOAR Workflow (#3):

- If you do not create this workflow, no tickets will be generated. This workflow sets up the triggers and if there is a IOM/IOA alert, it will run this SOAR workflow to create a ServiceNow ticket.



1. Trigger: Cloud Security Assessment > IOMs
- This means that in order for this workflow to run, an IOM alert must be detected from Falcon
2. Severity and cloud provider must meet these conditions
3. Create ServiceNow ticket
- Ticket will be created based on those trigger and conditions

Note: AWS will require its own SOAR workflow or we can make changes to the "Condition"