AWS Test Environment and CRWD integration process

Purpose: Document the steps taken to integrate AWS and CRWD and note down that specific configurations we selected

Prerequisites:

1. AWS account with permission (ask Paul for specifics)
2. Organizational Account ID (o-
3. Delegated admin account ID ( )
4. Organizational unit

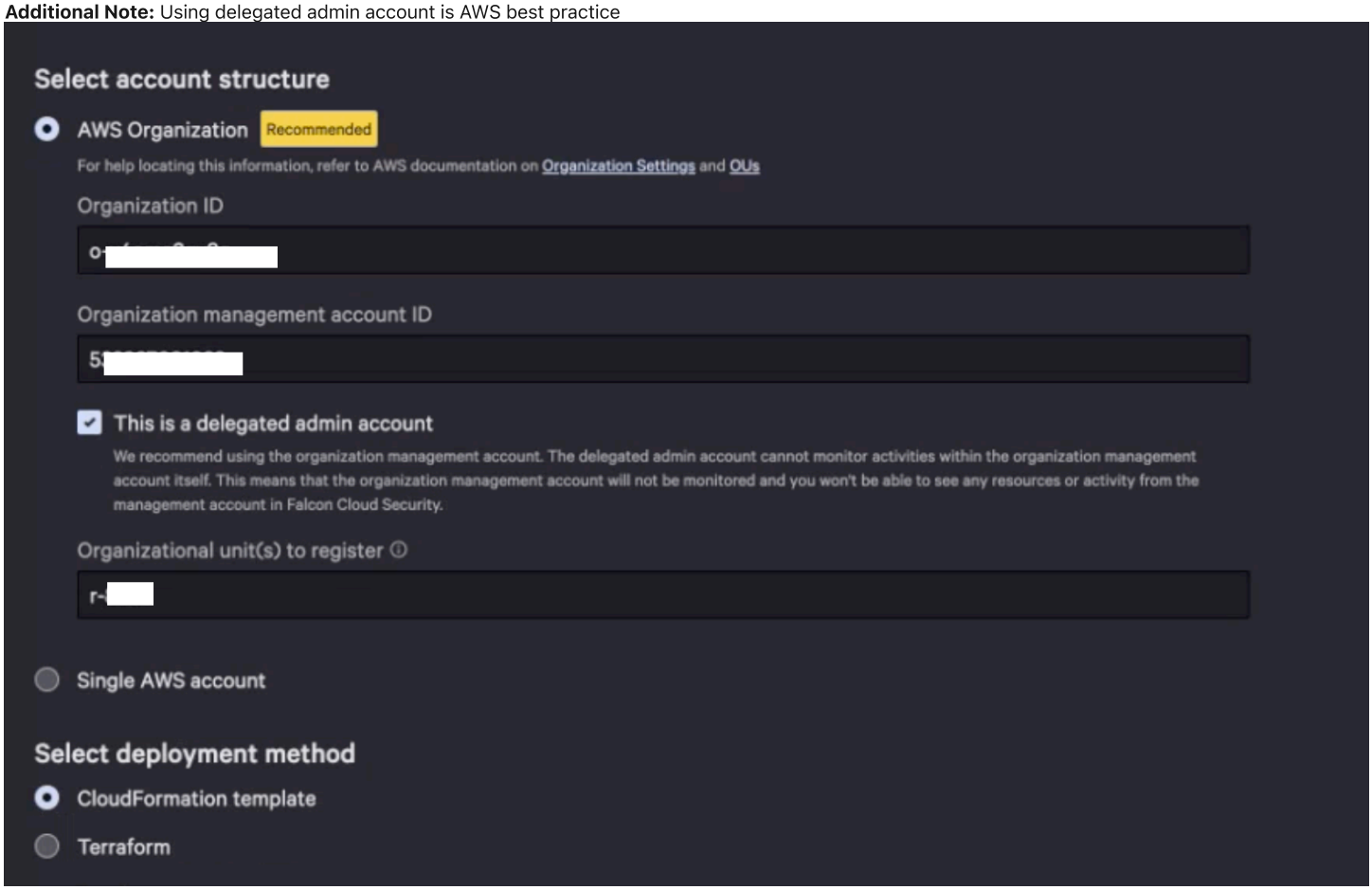
Step 1:

- Entered Organizational Account
- Delegated Admin Account used instead of Organizational Management account

1. **Note:** Delegated Admin Account cannot monitor activities within the organization management account itself. This means that the organizational management account will not be monitored and you won't be able to see any resources or activity from the management account in Falcon Cloud Security.

- **AWS organizational account will show as inactive.**

2. **Additional Note:** Using delegated admin account is AWS best practice

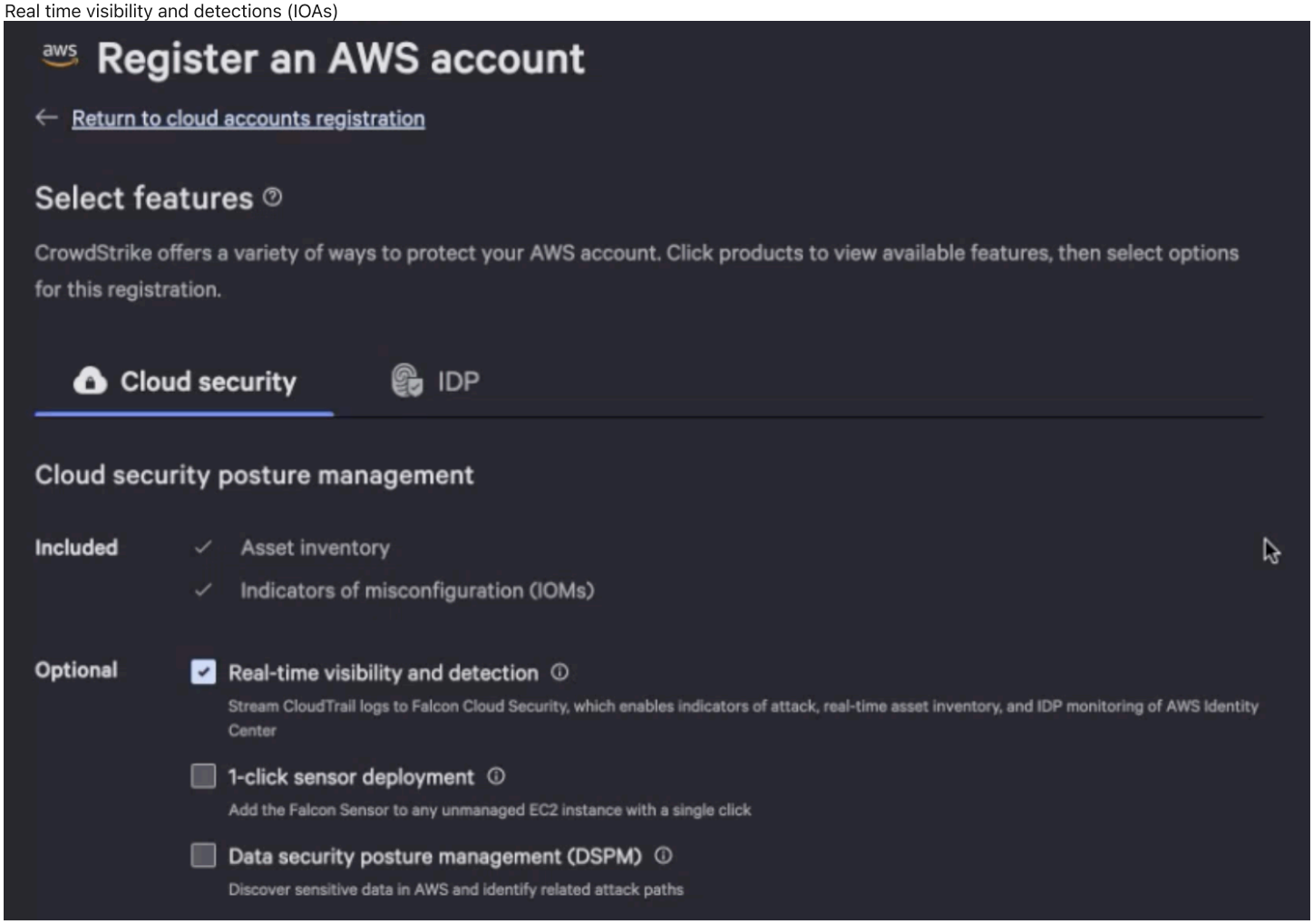


Step 2:
Select deployment method:

1. CloudFormation template

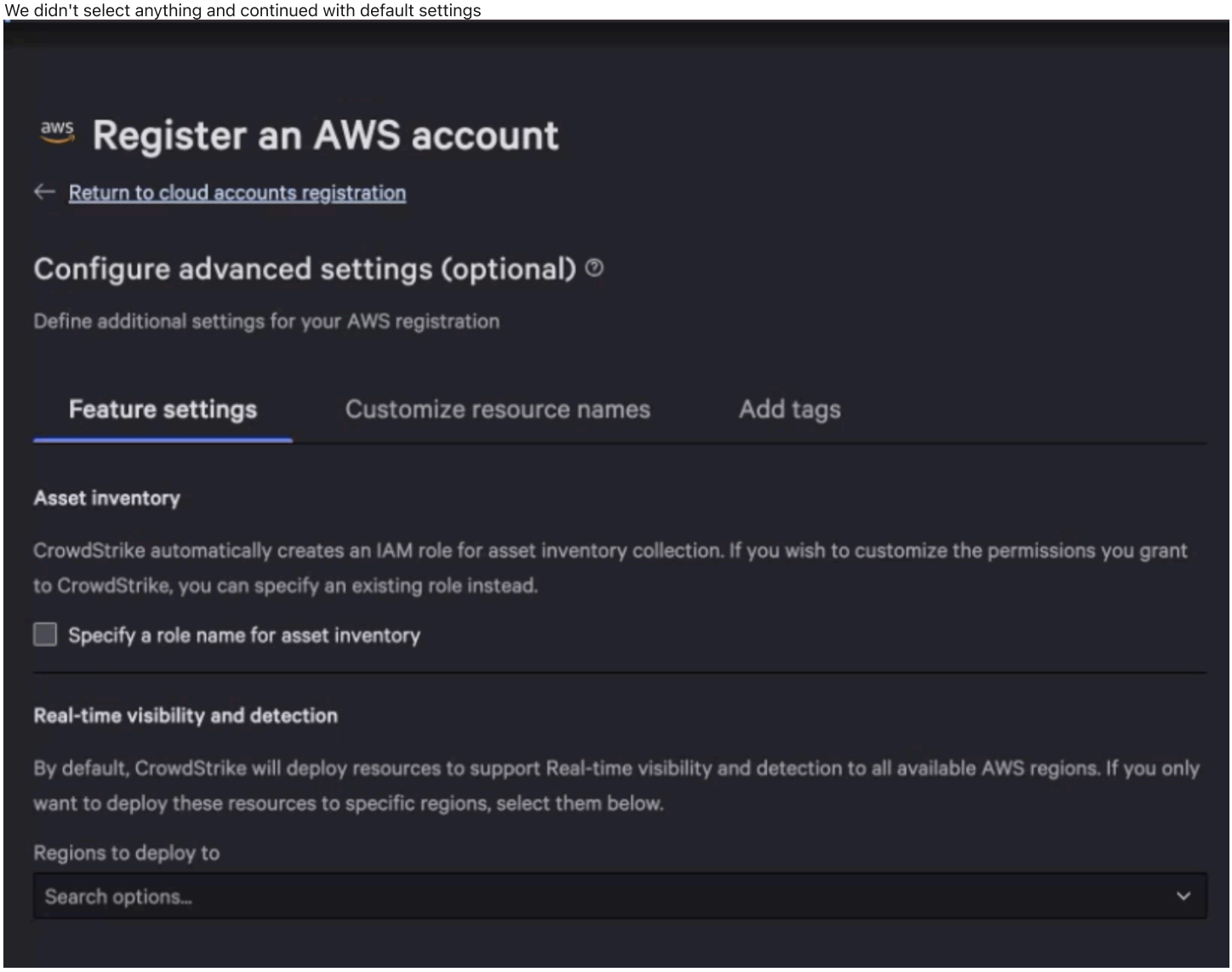
Step 3:

1. Real time visibility and detections (IOAs)



Step 4:

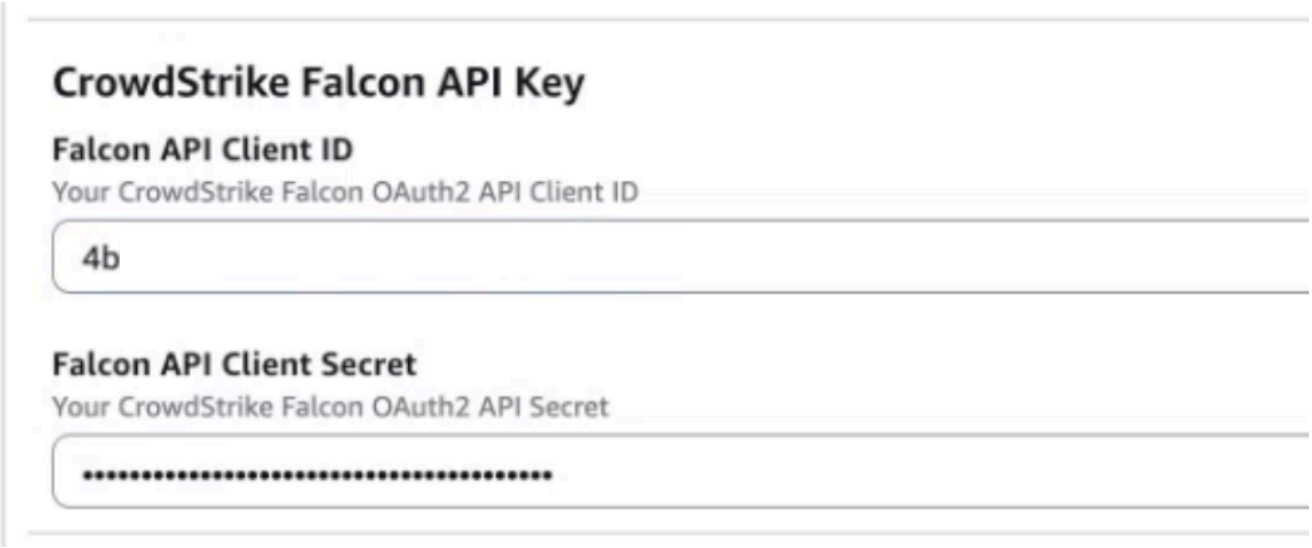
1. We didn't select anything and continued with default settings



Step 5:

1. Selected "Open CloudFormation Template"
2. Entered CrowdStrike API key's client Secret ID and client Secret value
   Note: API key is stored in key vault name "zhe2-cloudsec-kv-prod-01"

- https://zhe2-cloudsec-kv-prod-01.vault.azure.net/



Step 6:

1. Select "Create Stack"

Note: You will notice multiple Stacks created. Registering AWS Organizations using CloudFormation, the registration process creates both stacks and StackSets that contain the resources required for the features that we're enabling:

- StackSets contain the resources for the Organization's member accounts and/or resources that need to be deployed to more than one region in an account
- Stacks contain the resources for the Organization's management account

- CrowdStrike-Integration stack - CrowdStrike Registration Template
- StackSet-crowdstrike-RealtimeVisibility-StackSet
- StackSet-crowdstrike-AssetInventory
- StackSet-AWS-QuickSetup-SSM-TA