# Cb Defense + Slack Integration Set-up:

**GETTING STARTED**

* Configure CbAPI
  + Instructions here: <https://cbapi.readthedocs.io/en/latest/installation.html>
* Download associated CB+Slack python script.

**IN CB PSC CONSOLE**

Create CBC API Key

Navigate in CBC Console to [Settings > API Keys > Add API Key]

Create API Key with ‘Access Level’ **SIEM**

Copy Keys Created for Configuration:

API ID (Connector ID)

API Secret Key (API Key)

Create CBC Notification

Navigate in CBC Console to [Settings > Notifications > Add Notification]

Set-up desired notification

Under “How do you want to be notified?” Select SIEM connector made in step 1, under API Keys

Configure API Credentials File

Open Terminal or Command and cd to CbAPI directory

cbapi-defense configure

ENTER Hostname: Copy CbPSC URL i.e. <https://defense-prod05.conferdeploy.net/>

ENTER Connector ID: <Now called API ID>

ENTER API Key: <Now called API Secret Key>

Once configured change extension from credentials.defense to credentials.psc

VI into credentials.psc to identify the ‘profile’ name (in brackets above the api keys) – you might not have to do this with the updated Cbapi, please check.

Adjust line 12 of CB+Slack py script with the correct ‘profile’ name

**IN SLACK**

1. Create a new workspace (unless you already have one – then skip this step)
   1. Create Channel titled ‘cb\_alerts’
      1. If Channel name is different than ‘cb\_alerts’ adjust line 24 of CB+Slack py script
2. Install slack python client:
   1. <https://python-slackclient.readthedocs.io/en/latest/>
   2. Generate API Token:
      1. <https://api.slack.com/custom-integrations/legacy-tokens>
   3. Save this API Token as an environmental variable (tutorial link below):
      1. Windows: <https://www.youtube.com/watch?v=IolxqkL7cD8>
      2. Mac & Linux: <https://www.youtube.com/watch?v=5iWhQWVXosU>
      3. Enter Slack API environmental variable to line 15 of CB+Slack py script
3. Creating SLACK App for PSC Integration
   1. Select Workspace (far left of Slack Desktop)
   2. Select ‘Customize Slack’
   3. In Left Nav. Panel select ‘API’
   4. Select ‘Start Building’
   5. Create an App
      1. ENTER App Name: <example PSC Alerts>
      2. ENTER Dev. Slack Workspace
      3. Select ‘Create App’
4. Customize SLACK App
   1. Select the App you just created
   2. Select “Basic Information”
   3. “Add Features and Functionality”
      1. Turn ON ‘Incoming Webhooks’
      2. Select ‘Add New Webhook to Workspace’
         1. Select Channel of ‘cb\_alerts’
      3. Copy Webhook URL to line 27 of CB+Slack py script
5. Repeat 7b and 7cc Select ‘Bots’
   1. Add Bot User
6. Add newly created all to your workspace (if not already)

**Now run the script!**

The Cb notification listener will check every 30 seconds to see if a new alert has been generated – if so it will post it right within slack, and the bot will carry out the suggested actions!