ChatBot 3

한주성

Agenda

1. Bot 1 – bot!?, ci/cd with docker, filesystem, operation, dockerfile
2. Bot 2 – docker compose, sqlalchemy(database)
3. **Bot 3 – IoC Response, Create app**
4. Bot 4 – Response advance

IoC Hunting

VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE URL SEARCH

Choose file

IoC Response - 실습

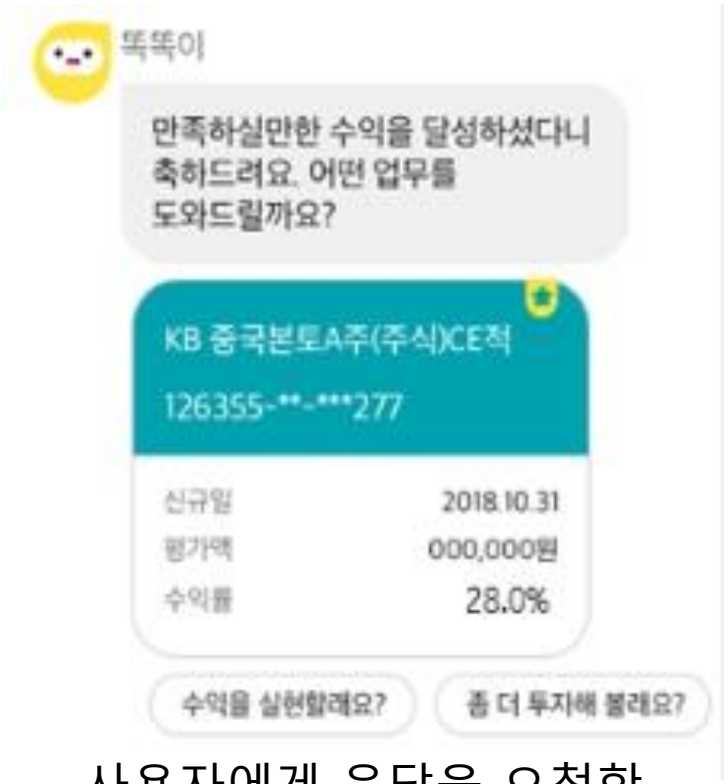
Virustotal IoC Hunting - vt.py

```
from splunklib.searchcommands import dispatch, GeneratingCommand, Option, Configuration
import virustotal3.core
import json

from config import virus_total_api_key as api_key

def virustotal(query_item, query_type):
    """ virustotal api """
    result = {}
    if query_type == 'ip':
        virus_total = virustotal3.core.IP(api_key)
        result = virus_total.info_ip(query_item)
...
```

Reactive and Proactive Chatbot

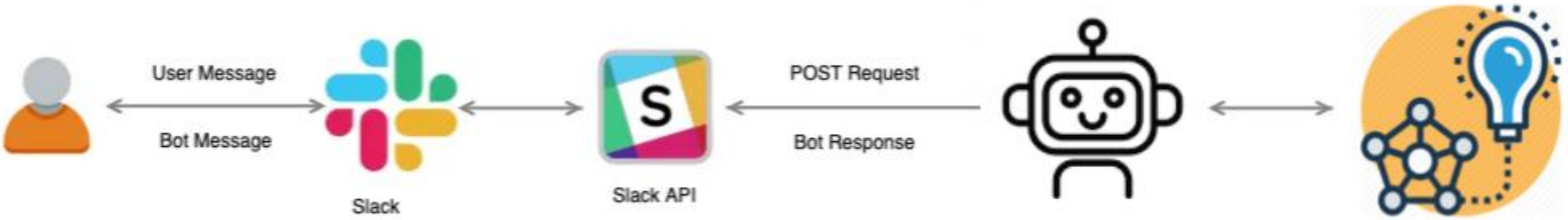
자동화 시스템으로, 답변을 제공하거나, 거래를 수행하고, 대기 시간을 줄이고, 고객 만족도를 높이는 데 사용된다.

사용자의 요청시 진행



사용자에게 응답을 요청함

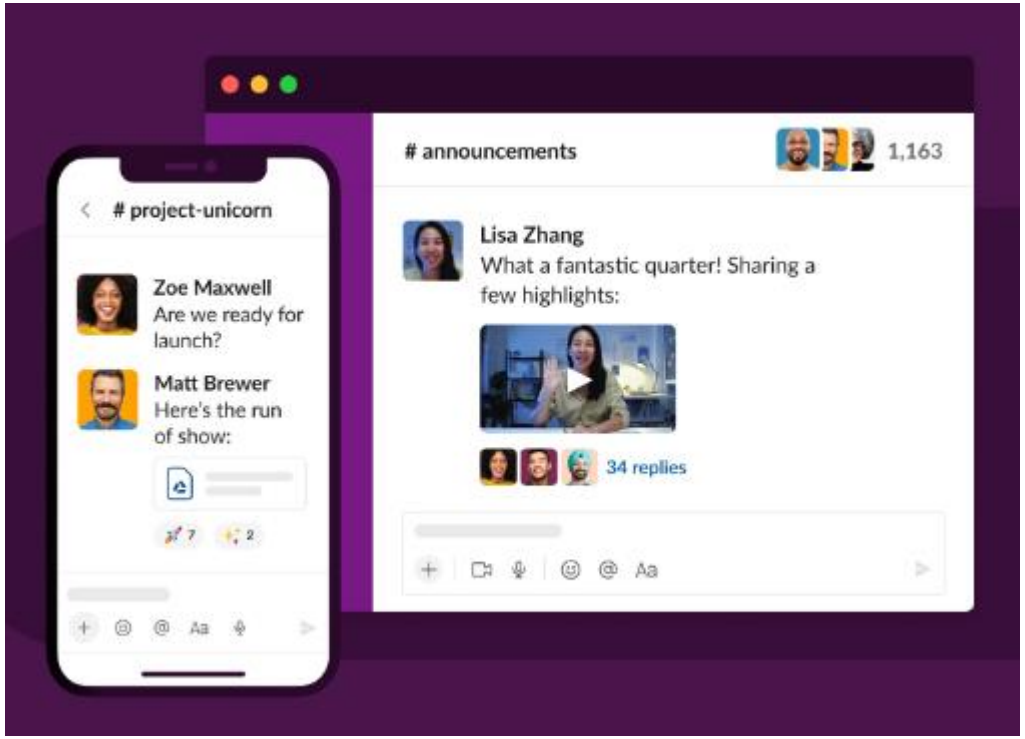
Bot Framework



Slack?!

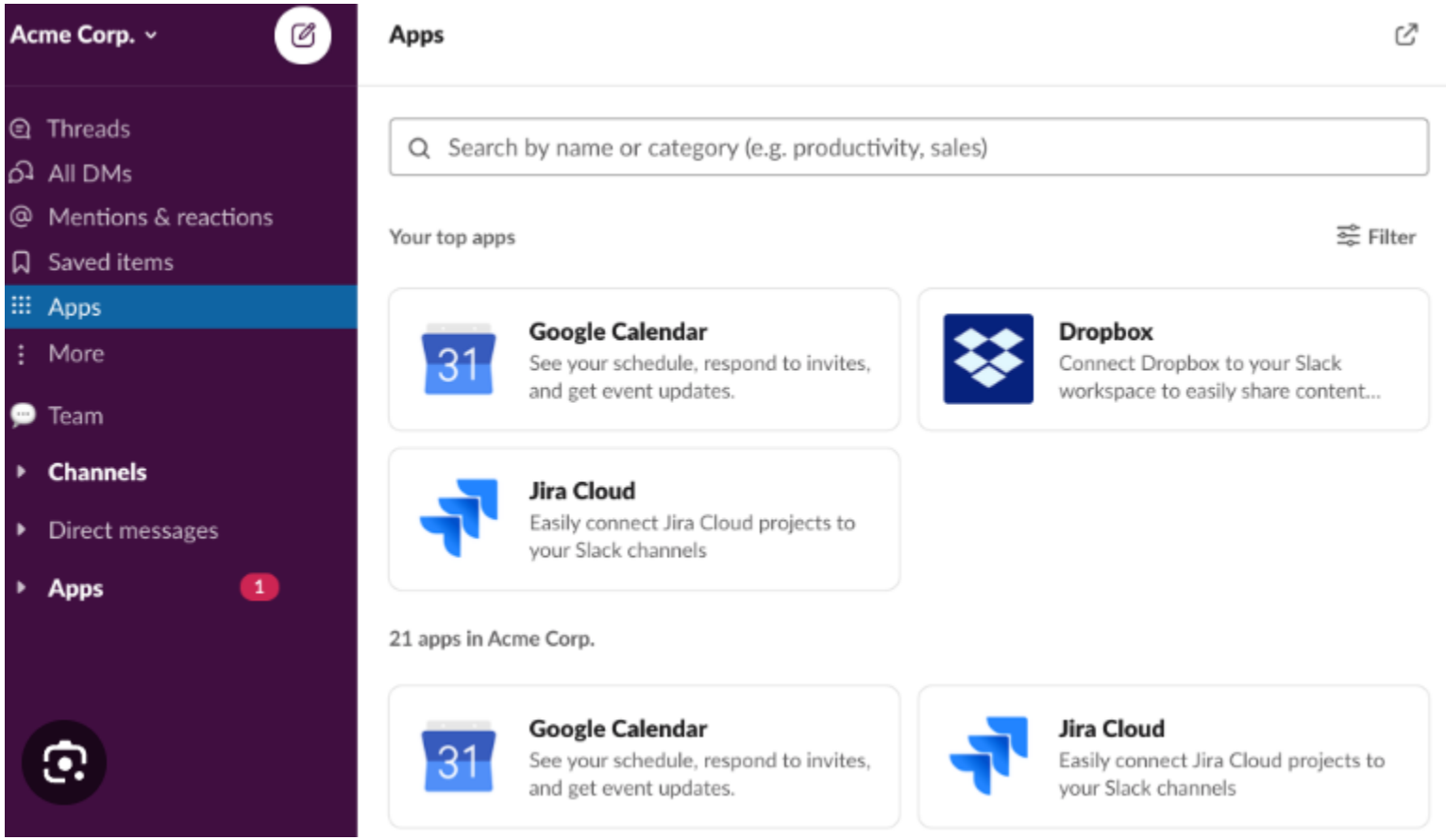
"모든 대화와 지식을 위한 검색 가능한 로그"(Searchable Log of All Conversation and Knowledge)의 준말
대다수의 빅테크 기업에서 사용하고 있다.

- 하위 스레드 대화하기
- 비공개/공개 채널
- 검색



Slack APP

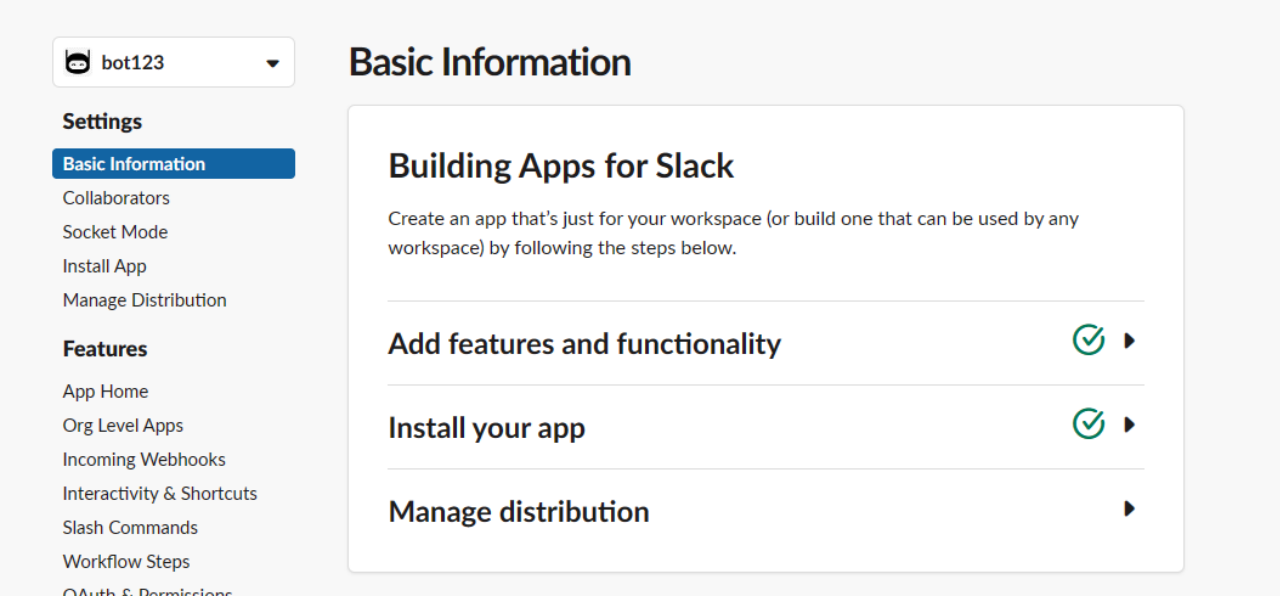
Slack에서 Webhook 혹은 API등으로 연결하여 Slack과 상호 동작하도록 구성한 Application



Slack App - 실습

App 생성 진행하기

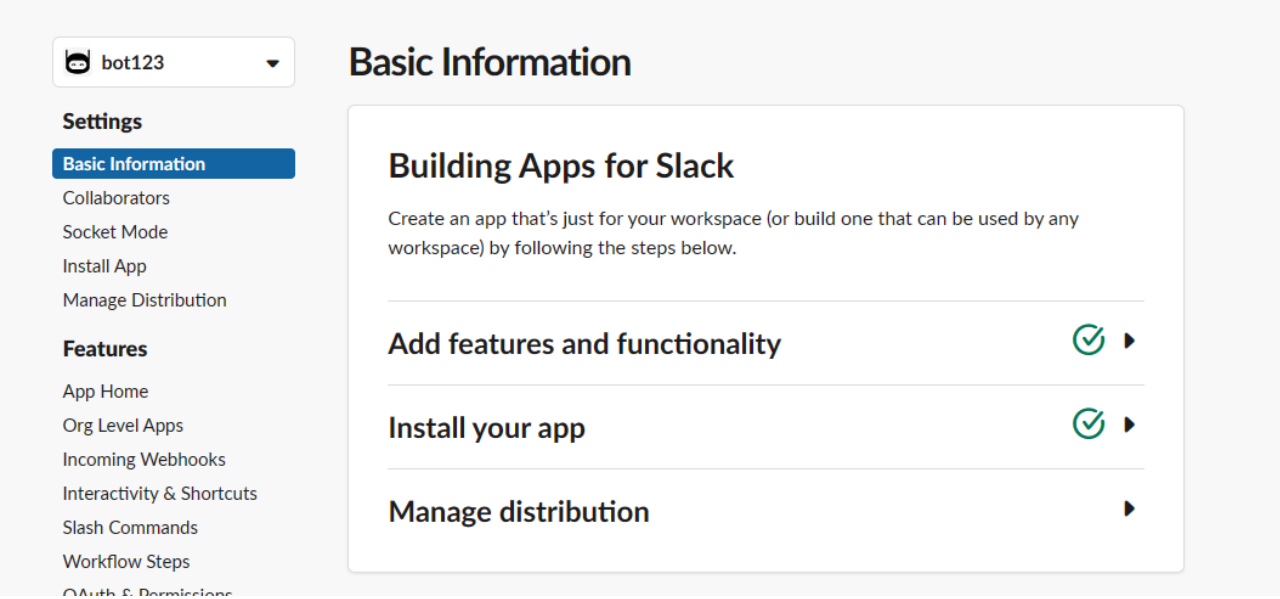
https://api.slack.com/



Slack App - 실습

App 생성 진행하기

https://api.slack.com/



Slack API 이해

https://api.slack.com/methods

Web API methods

</> Search methods

Popular method groups apps auth × chat conversations files reactions reminders teams users usergroups views

chat.delete	Deletes a message.
chat.deleteScheduledMessage	Deletes a pending scheduled message from the queue.
chat.getPermalink	Retrieve a permalink URL for a specific extant message
chat.meMessage	Share a me message into a channel.
chat.postEphemeral	Sends an ephemeral message to a user in a channel.
chat.postMessage	Sends a message to a channel.
chat.scheduleMessage	Schedules a message to be sent to a channel.
chat.unfurl	Provide custom unfurl behavior for user-posted URLs
chat.update	Updates a message.
chat.scheduledMessages.list	Returns a list of scheduled messages.

Slack API 이해

https://api.slack.com/methods

Web API methods

</> Search methods

Popular method groups apps auth × chat conversations files reactions reminders teams users usergroups views

chat.delete	Deletes a message.
chat.deleteScheduledMessage	Deletes a pending scheduled message from the queue.
chat.getPermalink	Retrieve a permalink URL for a specific extant message
chat.meMessage	Share a me message into a channel.
chat.postEphemeral	Sends an ephemeral message to a user in a channel.
chat.postMessage	Sends a message to a channel.
chat.scheduleMessage	Schedules a message to be sent to a channel.
chat.unfurl	Provide custom unfurl behavior for user-posted URLs
chat.update	Updates a message.
chat.scheduledMessages.list	Returns a list of scheduled messages.

Slack API 이해

https://api.slack.com/methods

Web API methods

</> Search methods

Popular method groups apps auth × chat conversations files reactions reminders teams users usergroups views

chat.delete	Deletes a message.
chat.deleteScheduledMessage	Deletes a pending scheduled message from the queue.
chat.getPermalink	Retrieve a permalink URL for a specific extant message
chat.meMessage	Share a me message into a channel.
chat.postEphemeral	Sends an ephemeral message to a user in a channel.
chat.postMessage	Sends a message to a channel.
chat.scheduleMessage	Schedules a message to be sent to a channel.
chat.unfurl	Provide custom unfurl behavior for user-posted URLs
chat.update	Updates a message.
chat.scheduledMessages.list	Returns a list of scheduled messages.

Bot 개발 - 실습

bot.py

- Bot 요청기록하기 (access 활용)
- 자신 계정으로 사용할 때만 응답 하도록 하기 (homework 활용)
- 응답 내용은 IoC(VT) 질의 내용으로 회신 (virustotal 활용)

HomeWork

Slack Bot IoC 을 질의후 응답 생성

- (2+1) Slack Bot IoC 을 질의
  - Bot에 IoC를 질의하면 결과를 회신해줌
  - Threat Intelligence platform 2 이상 질의
  - 코드 및 동작 흐름 설명
  - 결과 표시 방식에 따라서 점수 차등(가산 1점)
- (2+1) Bob 친구들 정보 알리미
  - BoBWiki 기준 개발보안 친구들 특성 입력하여 정보 출력
  - 코드 및 동작 흐름 설명
  - 결과 표시 방식에 따라서 점수 차등(가산 1점)

(3)+1 제출, 가산점

(2)금요일(8/16) 저녁 24:00까지 1차 인정
(1)일요일(8/18) 저녁 24:00까지 2차 인정