

# Security Workflow Automation

Automate some tasks for security stuff



HADESS

[WWW.HADESS.IO](http://WWW.HADESS.IO)

# FOREWARD

Automation has become a buzzword in the world of cybersecurity, and for good reason. With the increasing sophistication of cyber threats, traditional manual methods of cyber threat hunting and bug bounty programs are no longer enough to keep up with the pace of the attackers. This has led to the adoption of automated solutions that leverage machine learning algorithms and other advanced technologies to enhance threat detection and response capabilities.

In this article, we will explore the benefits and challenges of automation in cyber threat hunting, bug bounty programs, and open-source intelligence (OSINT) gathering. We will also examine some of the best practices for implementing automation in these areas and explore how it can help organizations stay ahead of the ever-evolving threat landscape. Whether you are a security analyst, a bug bounty hunter, or a cybersecurity enthusiast, this article will provide valuable insights into how automation can transform the way we approach cyber defense.

Cover By [Álvaro Pinto](#)

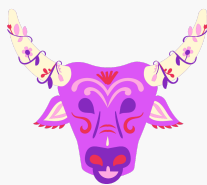


# Introduction



## Make.com

From tasks and workflows to apps and systems, Make is where you create and automate at the speed of your ideas.



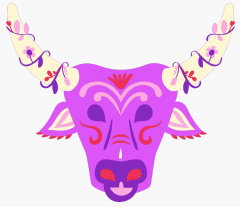
**Cyber Threat Intelligence**



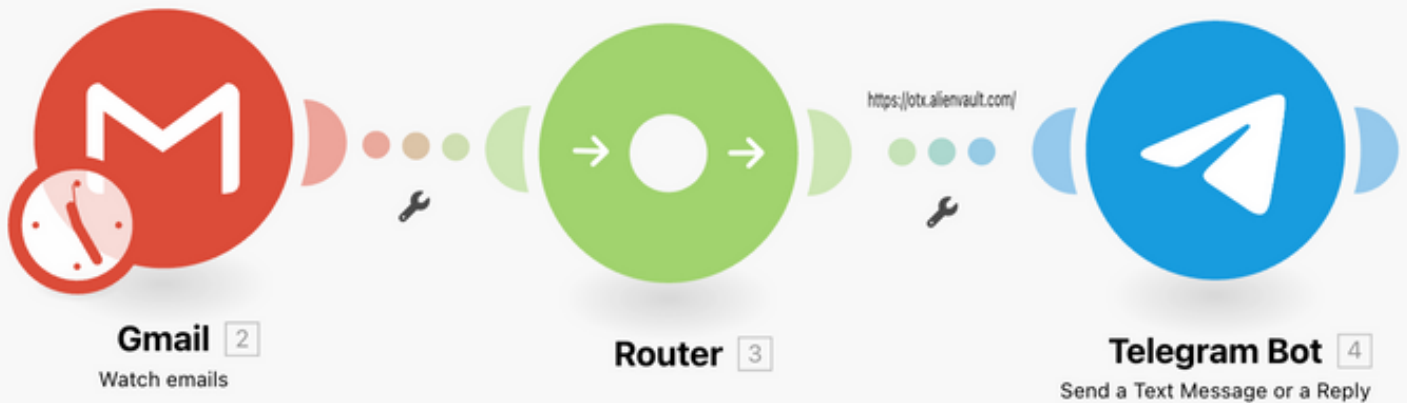
**Bug Bounty**



**OSINT**



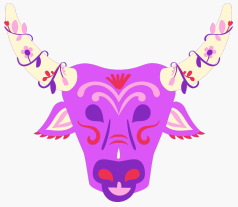
# Threat Pulse



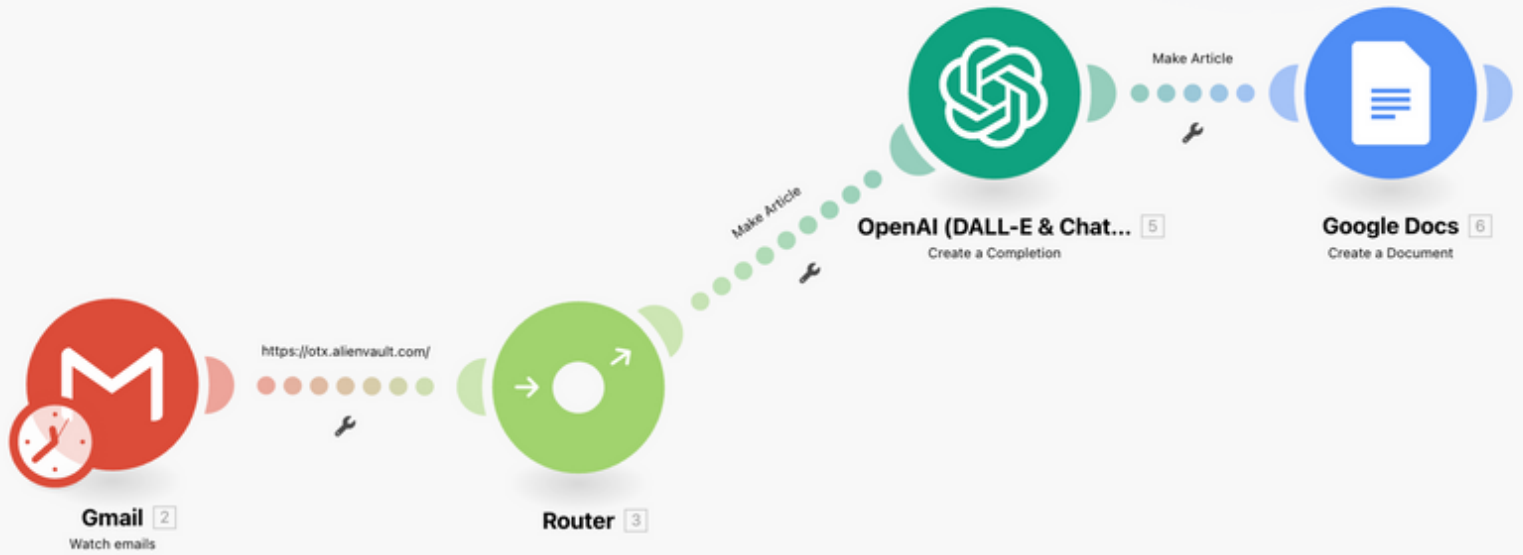
**1. Watch Email**

**2. IF OTX Pulse**

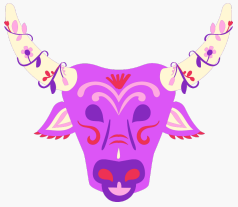
**3. Send to telegram bot**



# Threat Article



1. Watch Email
2. IF OTX Pulse
3. Make with Chatgpt
4. Create Document



# Threat Hype



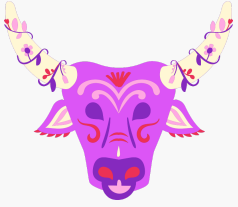
**1. Watch Email**

**2. IF OTX pulse**

**3. Search Related Tweet**

**4. Read and Summarize**

**5. Send to Discord**



# Threat POC

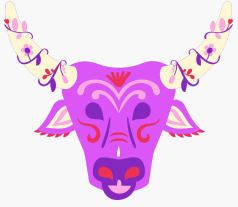


1. Watch Email

2. IF OTX pulse

3. Search Related POC

4. Send to Discord



# Threat IOC



**1. Get Latest CVE**

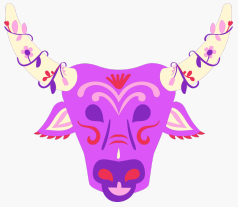
**2. Get OTX IOC**

**3. Search POC**

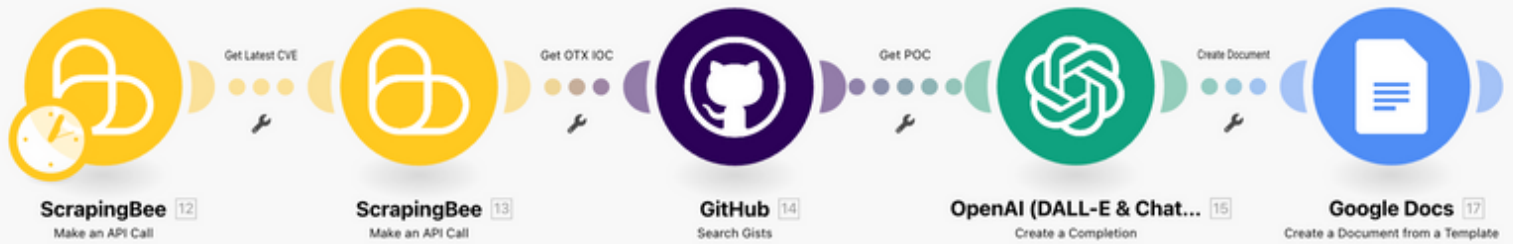
**4. Generate Yara Rule**

**5. Send to Email**





# Threat Knowledge Base



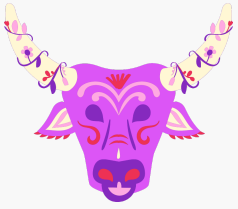
**1. Get Latest CVE**

**2. Get OTX IOC**

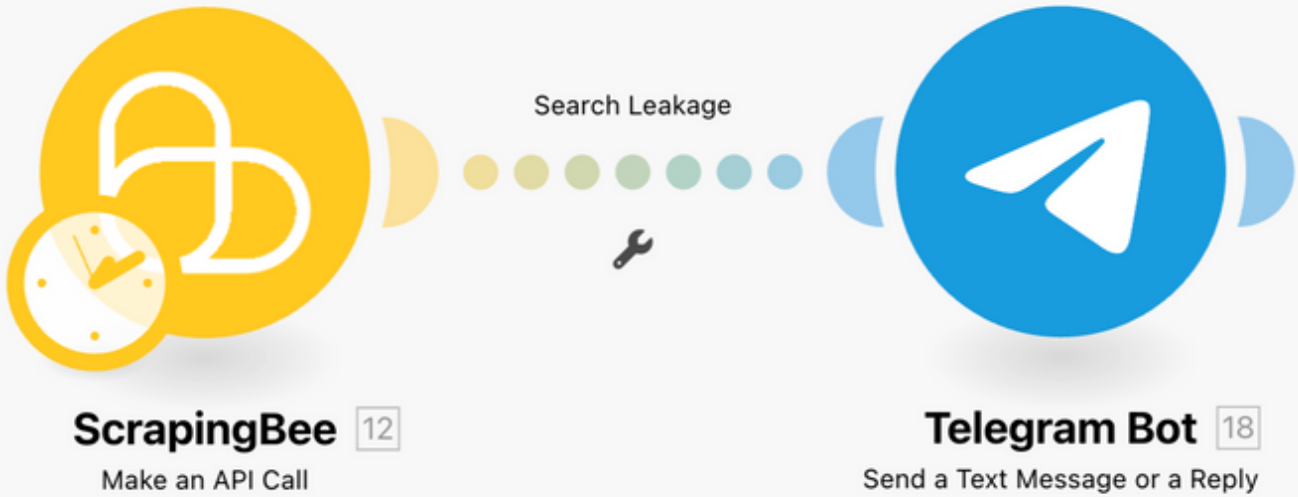
**3. Search POC**

**4. Threat Background**

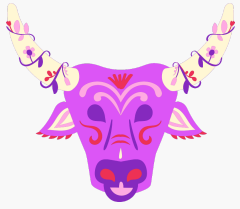
**5. Create Document**



# Leakage



1. Search Leakage from Dataset
2. Send to Telegram



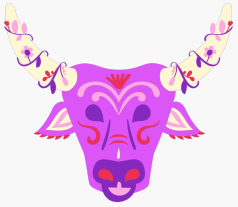
# Issue Tracking



**1. Watch Issue in Airtable**

**2. Send Alert to Slack**

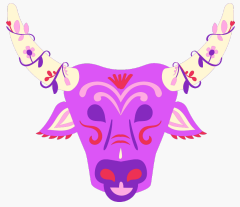
**3. Send Alert to Gmail**



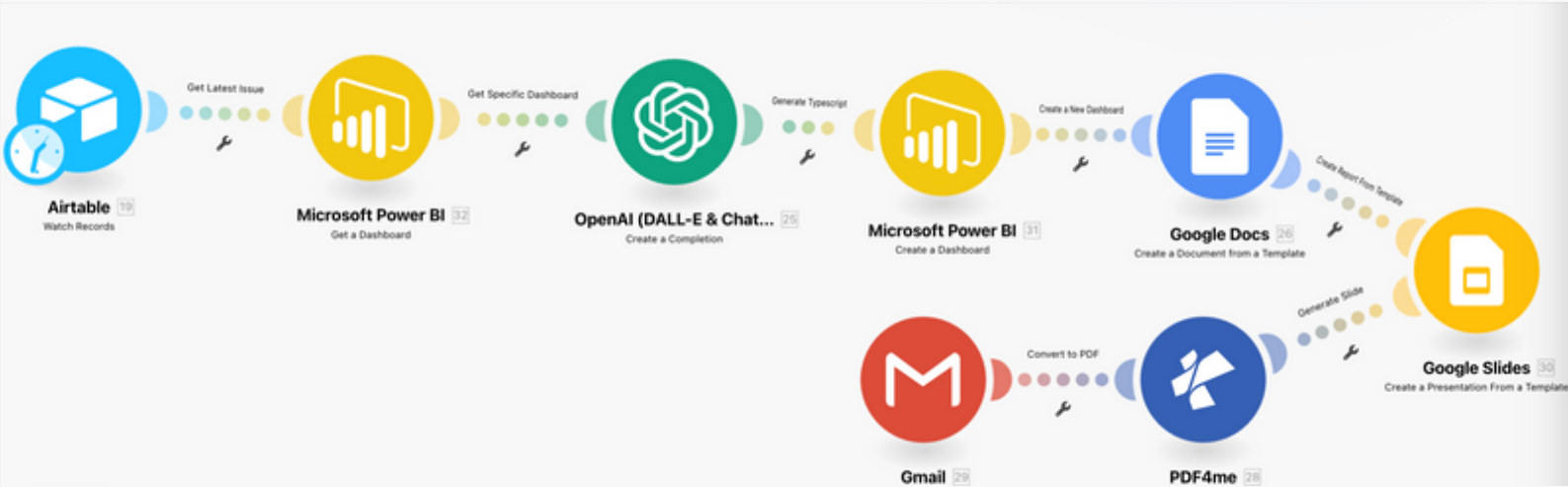
# CEO Friendly



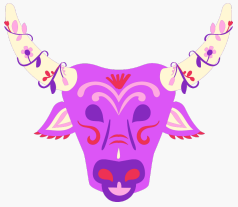
- 1. Watch Issue in Airtable**
- 2. Generate Typescript**
- 3. Create Document from Template**
- 4. Create Slide from Template**
- 5. Convert to PDF**
- 6. Send to Email**



# PR Friendly



1. Watch Issue in Airtable
2. Get PowerBI Specific Dashboard
3. Generate Typescript
4. Create a new Dashboard
5. Create Document from Template
6. Create Slide from Template
7. Convert to PDF
8. Send to Email



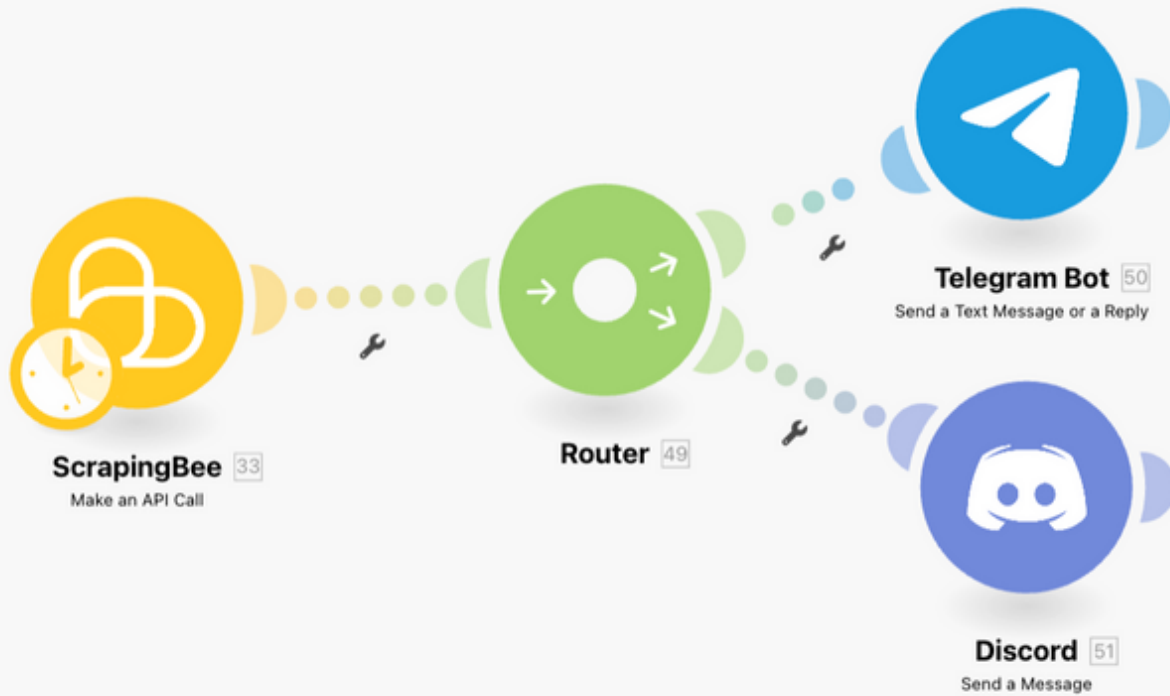
# Security Feed



1. Get Latest Threats
2. Append Latest Threats RSS
3. Generate News
4. Translate to Whatever
5. Search for News Image
6. Normalize Context
7. Send to Telegram
8. Send to Website



# Latest Hackerone Program



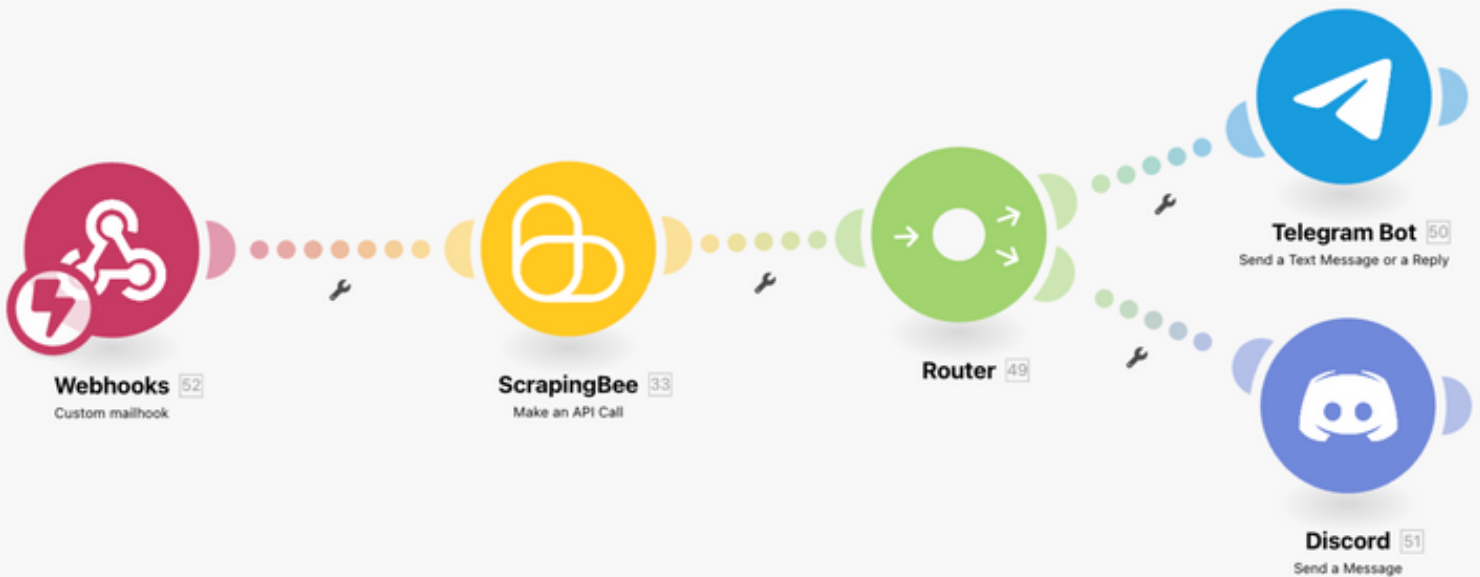
1. Get Latest Program

2. Send to Telegram

3. Send to Discord



# Asset Discovery(Automate)



**1. Trigger When Asset Visibility  
Changed**

**2. Run and Find New Asset**

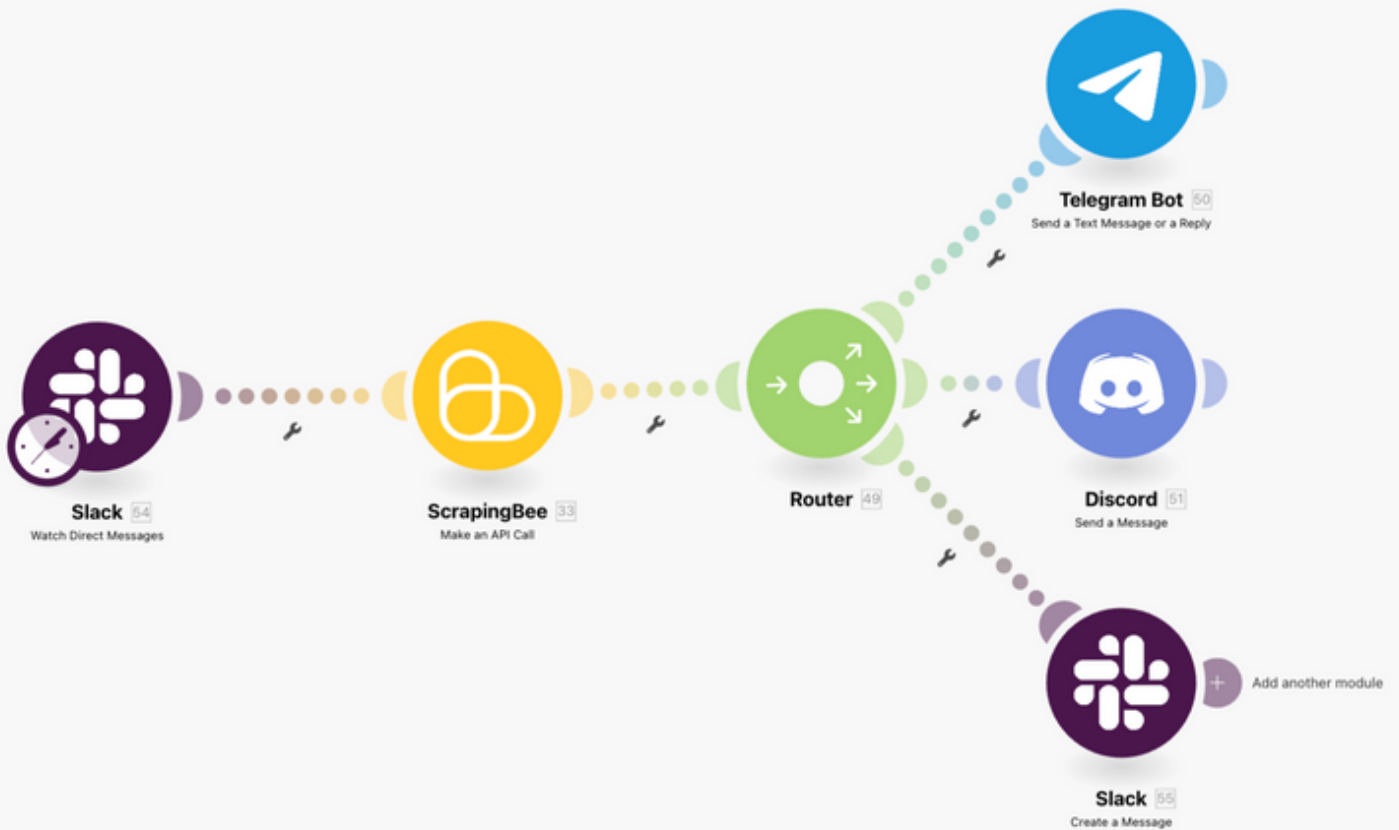
**3. Send Newest Asset to Telegram**

**4. Send Newest Asset to Discord**





# Asset Discovery(Semi-Automate)



**1. Trigger When New Message**

**2. Run and Find New Asset**

**3. Send Newest Asset to Telegram**

**4. Send Newest Asset to Discord**



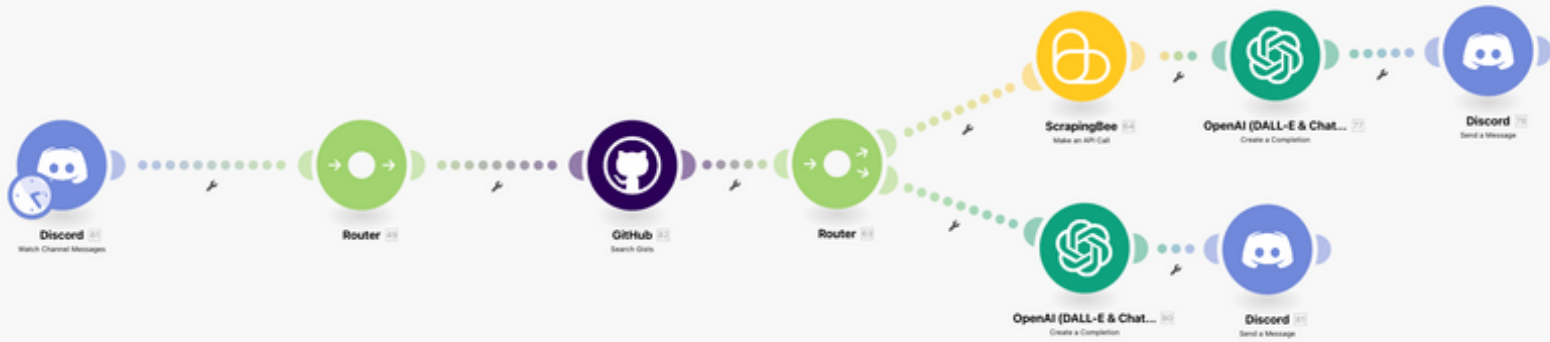
# Hunter Bot



1. Trigger When New Asset
2. Run and Enumerate
3. Take Screenshot
4. Run for Known Vuln with nuclei
5. Run for Specific Vuln with Bug Hunt Workflow
6. Generate Report for Known Vuln
7. Generate Report for Specific Vuln
8. Send to Discord
9. Send to Discord



# Exploit Developer



1. **Trigger When New Request**
2. **Search for Exist Exploit**
3. **If Exist Then Clone**
  - a. **Change Exploit for Scenrario**
  - b. **Send to Discord**
4. **Else Write a Scenario**
  - a. **Send to Discord**



# Bounty Pulse



1. Trigger When New Activity

2. Find Methodology

3. Find Similar Method

4. If Unique Then

a. Write a Template

b. Test and Append

c. Notify via Telegram

5. Else

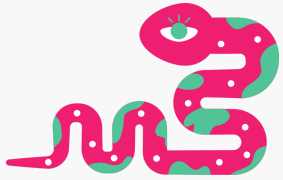
a. Notify via Telegram



# Program Pulse



1. Trigger When New Program
2. More Info about background
3. Search in Twitter
  - a. Text Aggregator
  - b. Add to Telegram
  - c. Append to Excel
4. Find History
  - a. Text Aggregator
  - b. Add to Telegram
  - c. Append to Excel
5. Search in RSS
  - a. Text Aggregator
  - b. Add to Telegram
  - c. Append to Excel
6. Search in Rocketreach
  - a. Text Aggregator
  - b. Add to Telegram
  - c. Append to Excel



# Twitter Activity #1



**1. Request Twitter User**

**2. Search Tweets**

**a. Add to Airtable**

**b. Normalize Tweets**

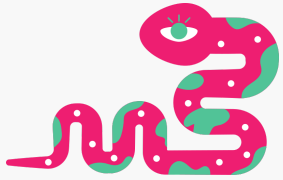
**c. Append to PowerBI**

**3. Search Mentions**

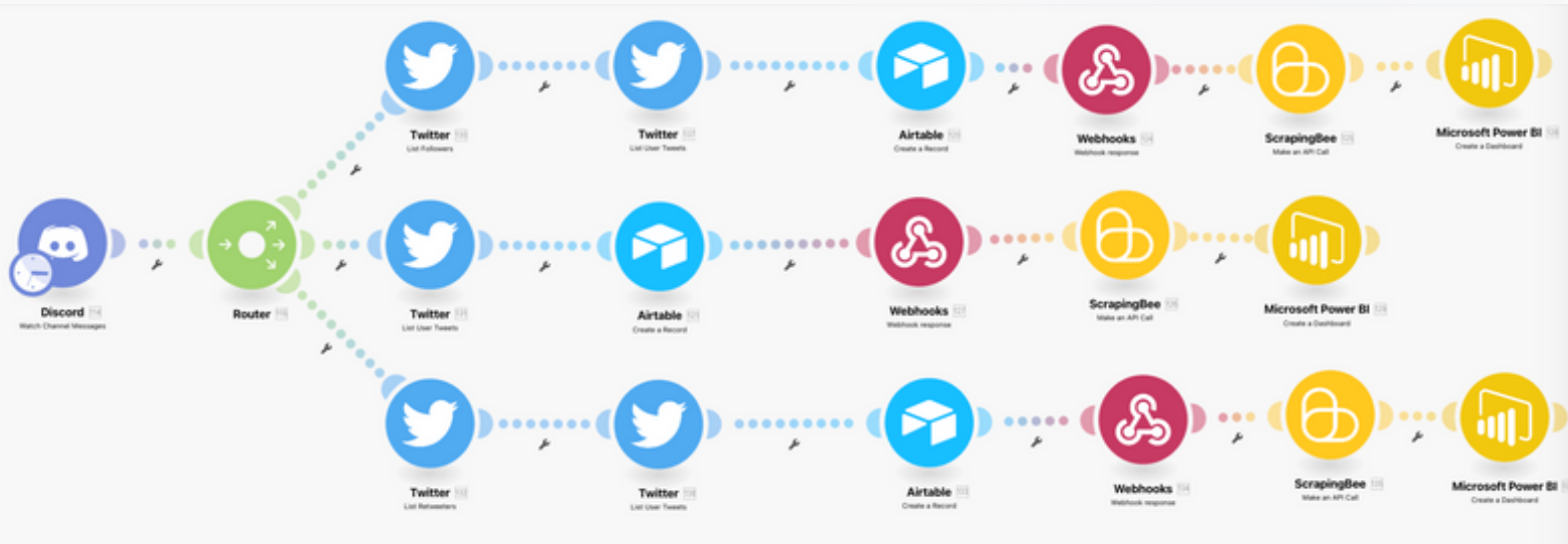
**a. Add to Airtable**

**b. Normalize Tweets**

**c. Append to PowerBI**



# Twitter Activity #2



1. Request Twitter User

2. List Followers

a. Get Tweets

b. Add to Airtable

c. Normalize Tweets

d. Append to PowerBI

3. List User Tweets

a. Add to Airtable

b. Normalize Tweets

c. Append to PowerBI

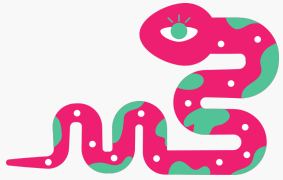
4. List Retweeters

a. Get Tweets

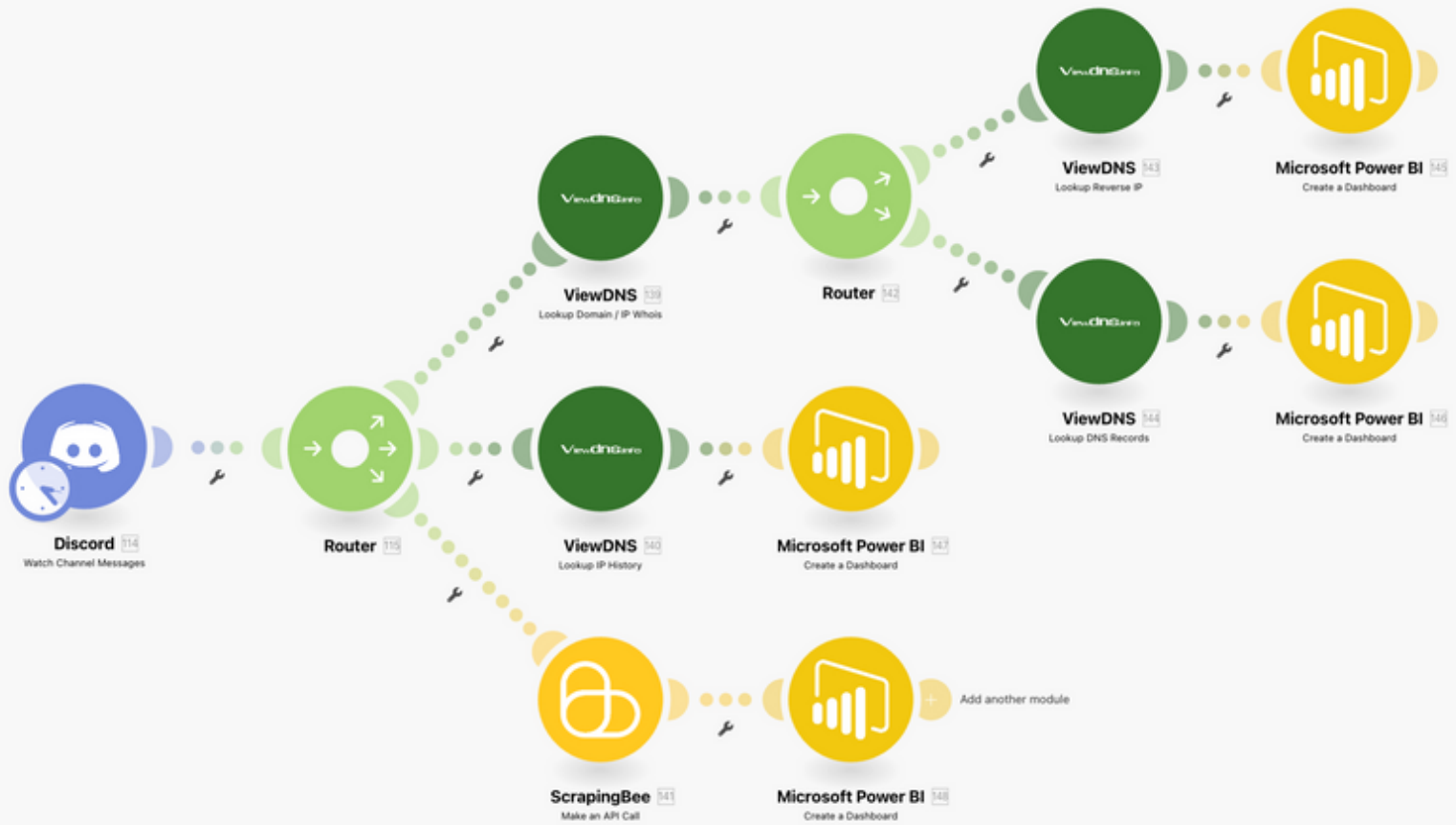
b. Add to Airtable

c. Normalize Tweets

d. Append to PowerBI



# Website Info



1. Request Website Info

2. Lookup Domain/IP

a. Lookup Reverse IP

b. Create PowerBI Dashboard

3. Lookup IP History

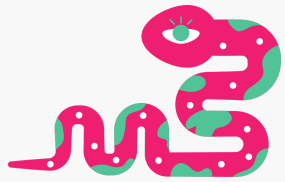
a. Lookup Reverse IP

b. Create PowerBI Dashboard

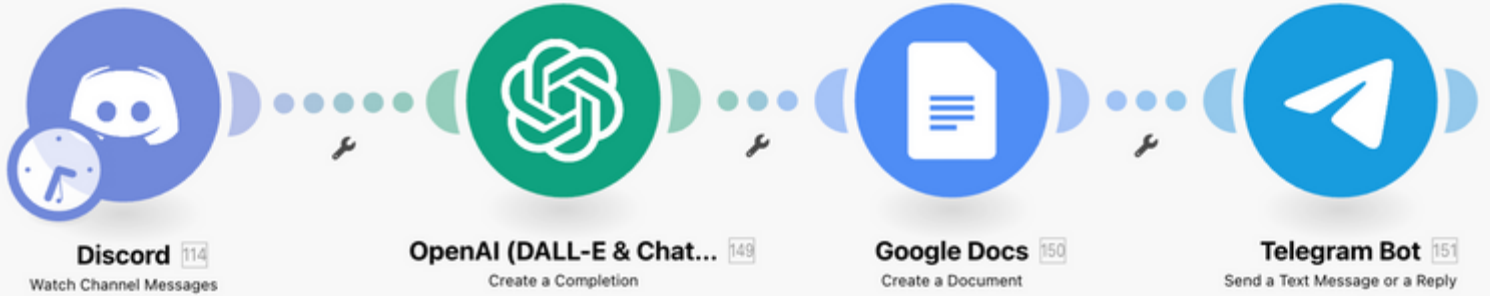
4. Run For Enumeration

a. Create PowerBI Dashboard

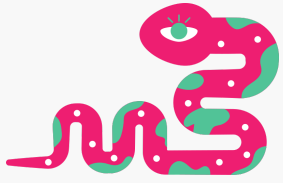




# Youtube Typscript



1. Request Youtube Video
2. Watch and Generate Typscript
3. Create Document
4. Notify via Telegram



# Employee Profile #1



**1. Request Whois Employee**

**2. Search in RocketReach**

**3. Notify via Discord**



# Location Search #1



1. Request Whois Location

2. Get Location Data

3. If true Then

a. Search in Twitter

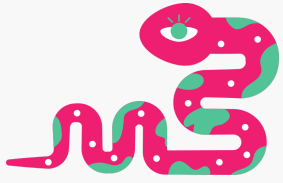
b. Send to Discord

4. Else

a. Search Specific

b. Search in Instagram Media

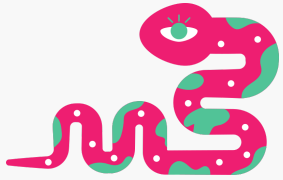
c. Send to Dicord



# Face Recognition #1



1. Request Whois Face
2. Extract with Google Cloud
3. Search in Dataset
4. Send to Discord



# LinkedIn Search #1



1. Request Whois LinkedIn
2. Get Org Employee
3. Search in Dataset
4. Send to Discord

