Tines Integration with QRadar and Virus total

PRESENTED BY:
AHMED ELHALWAGY
AHMED KHALED
ALI IBRAHIM
ANAS KHALIL
PRISKLLA NABIL
YOSEF KHALED

REQUIREMENTS

we INNOVATE
Innovate to inspire

- GREP SOME DESTINATION IPS FROM QRADAR AND SEARCH IF THEY ARE MALICIOUS USING VIRUS TOTAL
- IF THEY ARE MALICIOUS TINES SENDS US A EMAIL WITH THE MALICIOUS IPS

STEPS

1. CREATE ACCOUNT ON QRADAR FOR THE TIEMS SERVICE

ADMIN –> AUTHORIZED SERVICES –> ADD

Pablo Escobar	Admin	Admin	AhmedKhaled	Sun, 08/09/2024, 00:59	Tue, 31/12/2024, 19:43

- WE CREATED A SERVICE ACCOUNT NAMED PABLO ESCOBAR TO GET THE API TOKEN FROM IT.

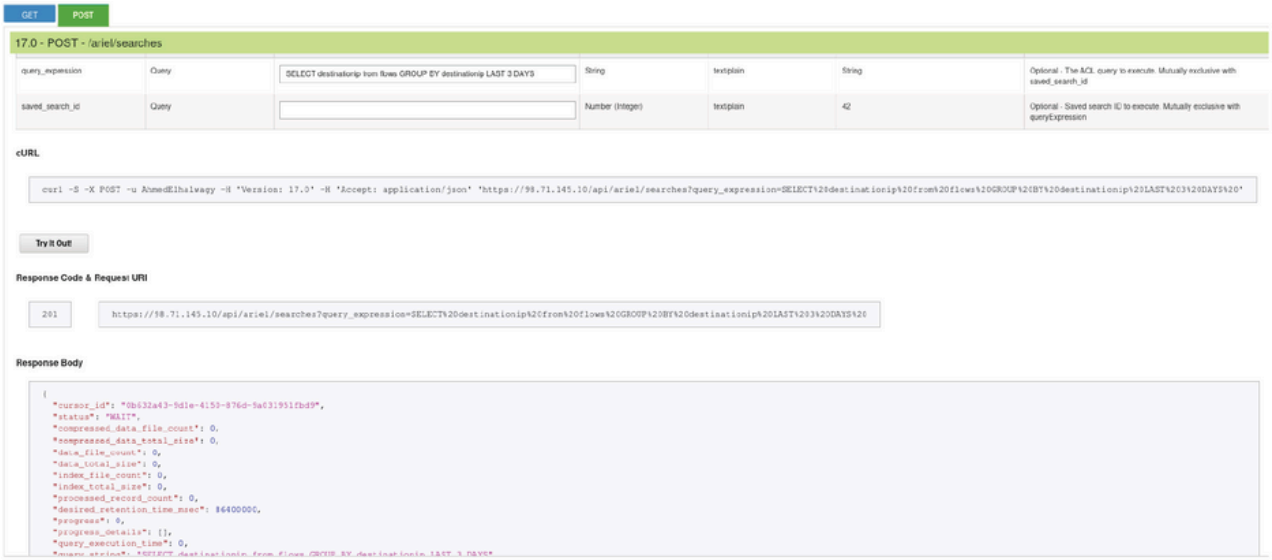
2. PREPARE OUR SEARCH QUERY ON QRADAR

```
SELECT destinationip as dest_ip from flows
GROUP BY destinationip LAST 3 DAYS
```

3. PREPARE OUR QRADAR API ENDPOINT

- AFTER VISITING HTTPS://98.71.145.10/API_DOC WE GO TO

ARIAL –> SEARCHES –> POST



HTTPS://98.71.145.10/API/ARIEL/SEARCHES?QUERY_EXPRESSION=SELECT%20DESTINATIONIP%20FROM%20FLOWS%20GROUP%20BY%20DESTINATIONIP%20LAST%203%20DAYS%20V

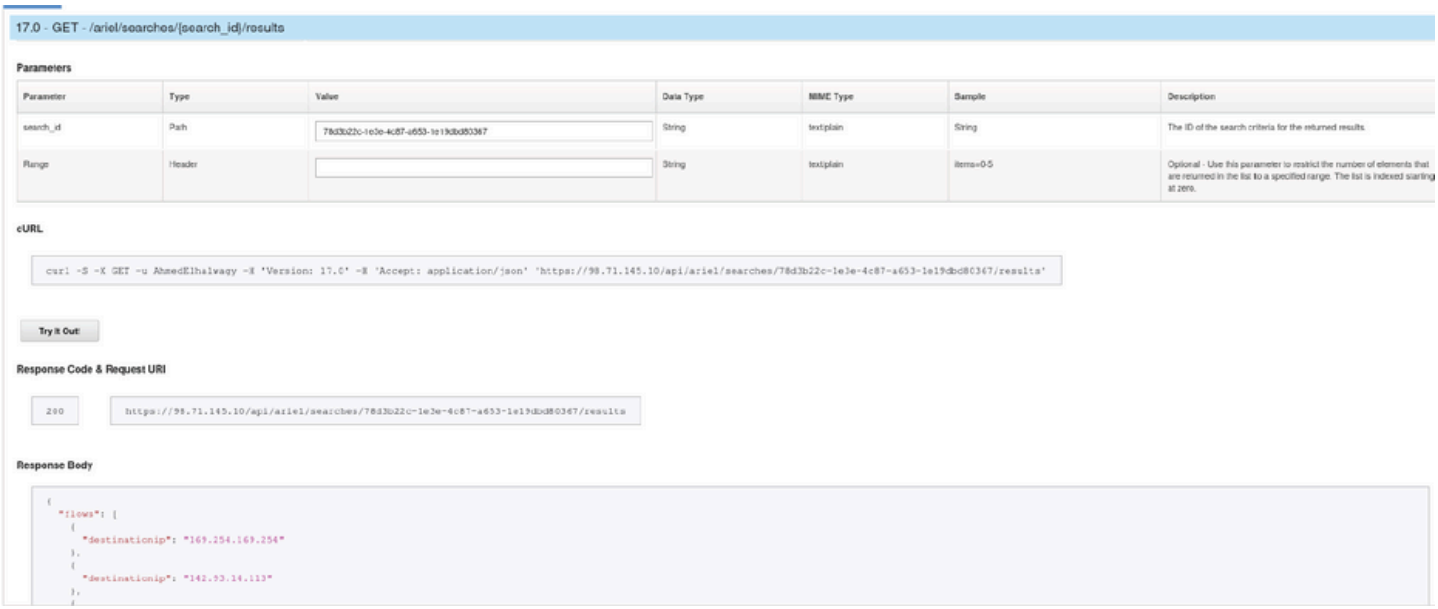
- NOW WE HAVE CREATED OUR SEARCH QUERY URI
- THEN WE COPY THE SEARCH ID (IN THE RESPONSE) AND DO A GET REQUEST TO

ARIAL –> SEARCHES –> SEARCH_ID –> RESULTS –> GET

STEPS

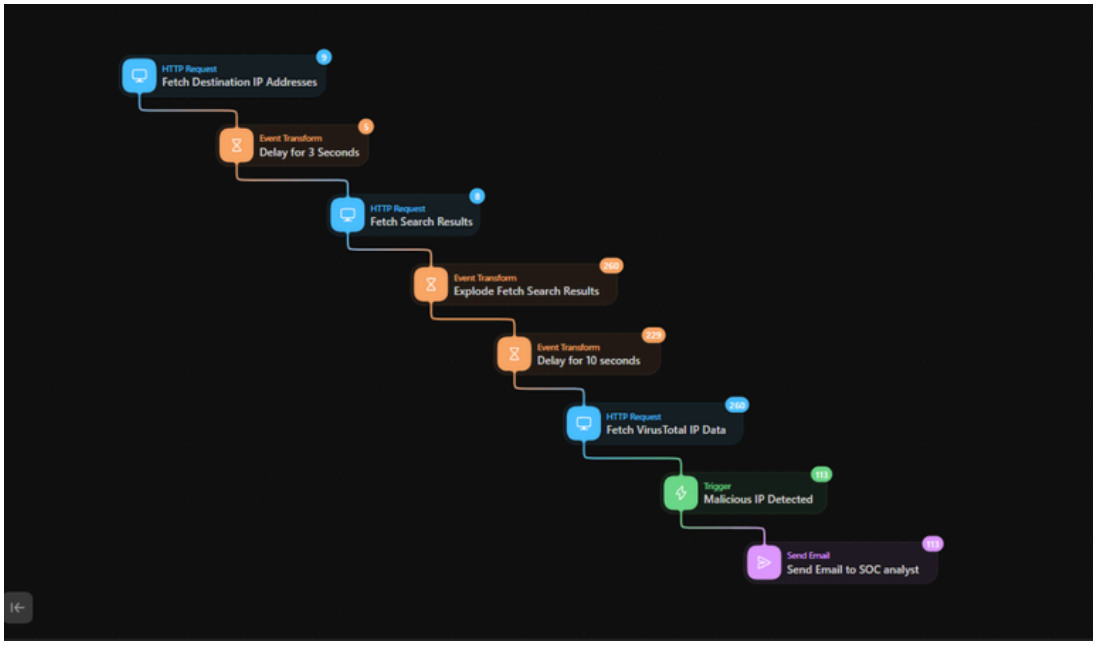
- **WITH PARAMETER:**

SEARCH_ID



HTTPS://98.71.145.10/API/ARIEL/SEARCHES/%20%3C%3CFETCH_DESTINATION_IP_ADDRESSES.BODY.SEARCH_ID%3E%3E/RESULTS

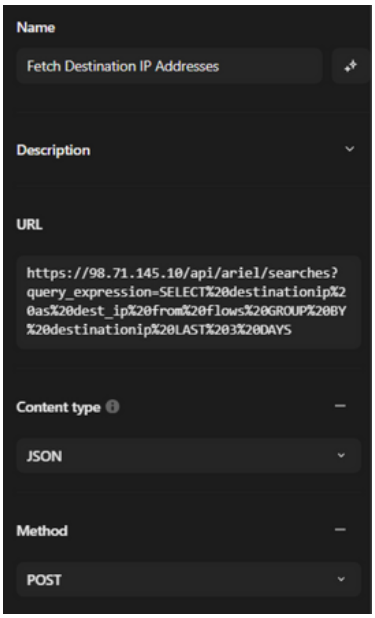
4. SOAR CONFIGURATION (TINES CONFIGURATION)

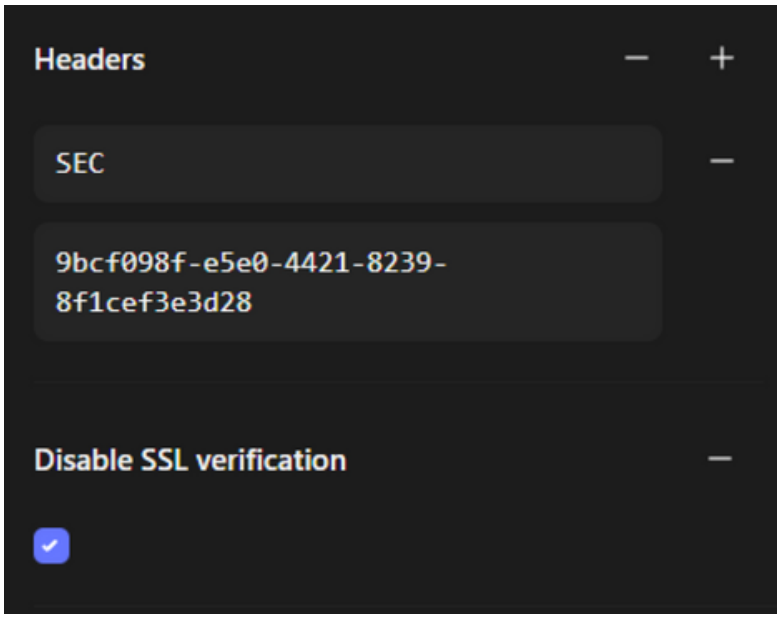


- THIS IS SIMPLY THE ARCHITECTURE

STEPS

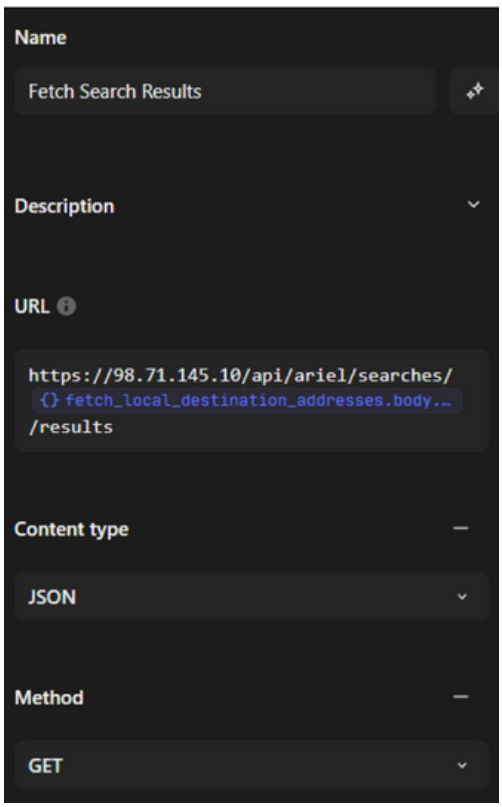
4.1.QRADAR QUERY





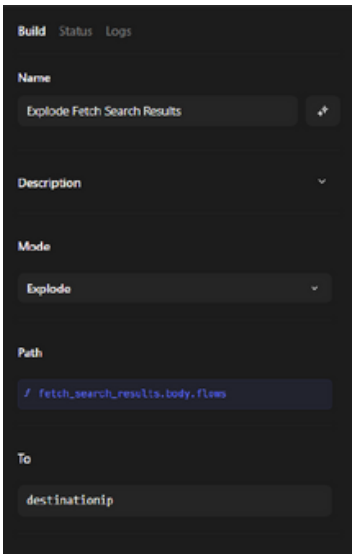
4.2. DELAY FOR 3 SECONDS

4.3. FETCH SEARCH RESULTS FROM QRADAR
WE EXTRACTED THE SEARCH_ID PARAMETER FROM THE PREVIOUS RESPONSE



STEPS

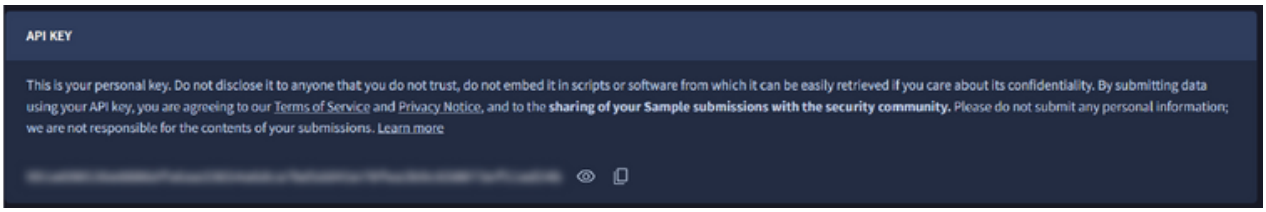
4.4. EVENT TRANSFORM MODULE EXPLODE TO EXTRACT THE DESTINATION IP ADDRESS AND PUT THEM INTO AN ARRAY



4.5. DELAY FOR 10 SECONDS

4.6. MAKE API REQUEST TO VIRUSTOTAL TO CHECK IF ANY OF THE IPS IS MALICIOUS

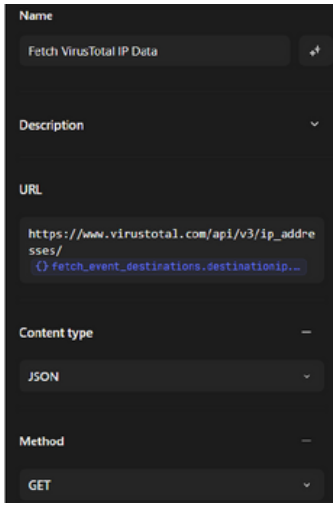
- WE FIRST NEED TO CREATE AN ACCOUNT ON VIRUS TOTAL
- GO TO API KEY

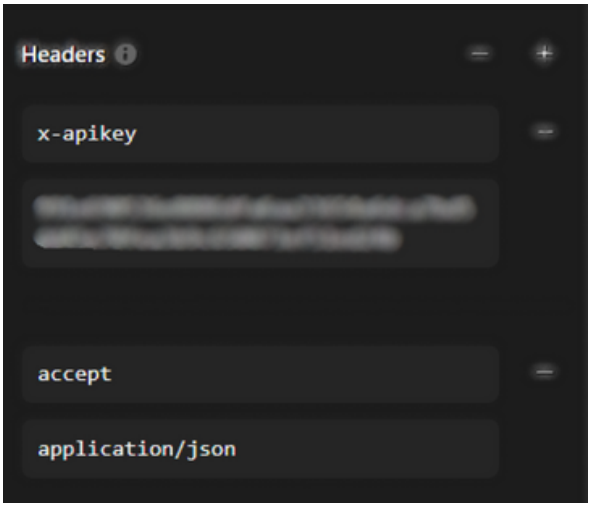


- FROM VIRUSTOTAL API DOCUMENTATION WE FOUND THAT WE WILL USE THIS URI

HTTPS://WWW.VIRUSTOTAL.COM/API/V3/IP_ADDRESSES/

- WE FETCHED THE DESTINATIONIP ARRAY FROM THE PREVIOUS TRANSFORM

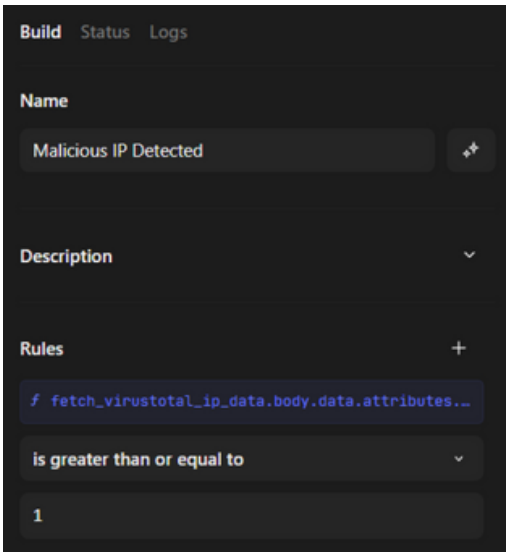




STEPS

7. TRIGGER IF THE RESPONSE FROM VIRUSTOTAL SAY THAT THE IP ADDRESS IS MALICIOUS

- IF THE MALICIOUS FAILED OF THE IP IN THE API RESPONSE IS GREATER THAN OR EQUAL 1 TRIGGER A MALICIOUS



8. IF THE TRIGGER TRUE SEND EMAIL SAYING

A MALICIOUS IP <<FETCH_VIRUSTOTAL_IP_DATA.BODY.DATA.ID>> DETECTED IN THE SYSTEM`