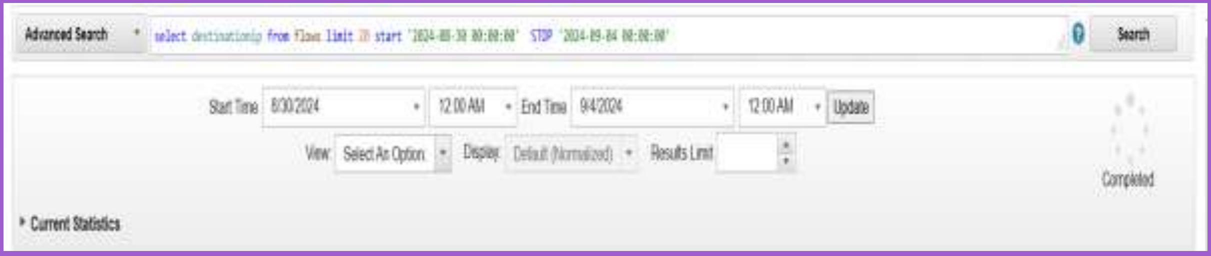
Tines
WE INNOVATE
WE INNOVATE
tines
QRADAR

- **This report is done by team iron man :**

Nour omar	Abdelrhman zaky
Shahd	Mohamed yousry
Mohamed ibrahim	Abdullah ahmed

Implement soar on qradar &and detect malicious ip ..

First we open q radar and make eql search about the ip that we want to check if it’s malicious or not in our network flow



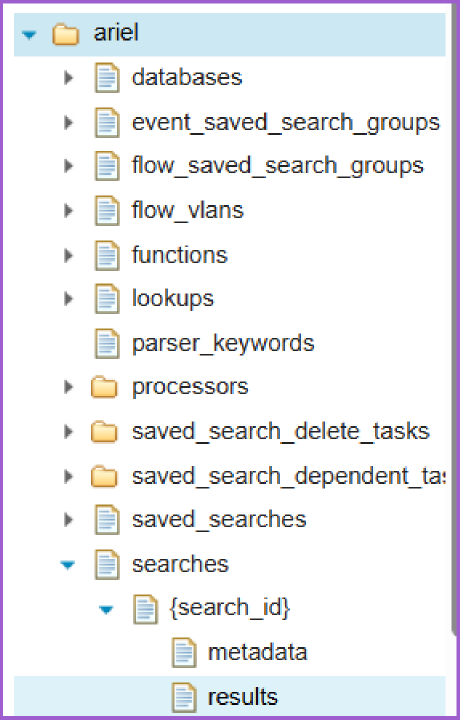
```
select destinationip from flows limit 20 start '2024-08-30 00:00:00' STOP '2024-09-04 00:00:00'
```

Start Time: 8/30/2024 12:00 AM End Time: 9/4/2024 12:00 AM

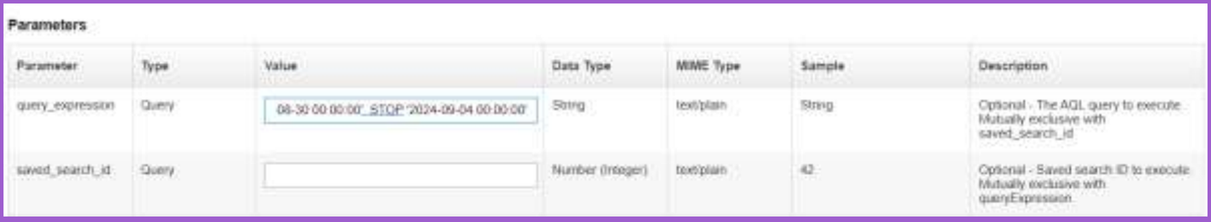
View: Select An Option Display: Default (Normalized) Results Limit:

Then after this we take the eql query that we write and go to qradar api_doc by using this url:https://98.71.145.10/api_doc

And then open ariel data base



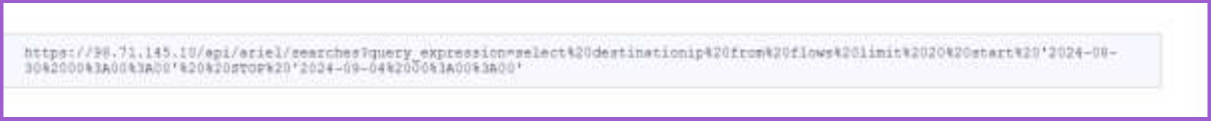
and then open searches and make in post and put our eql query in it and put in the path entry



Parameters

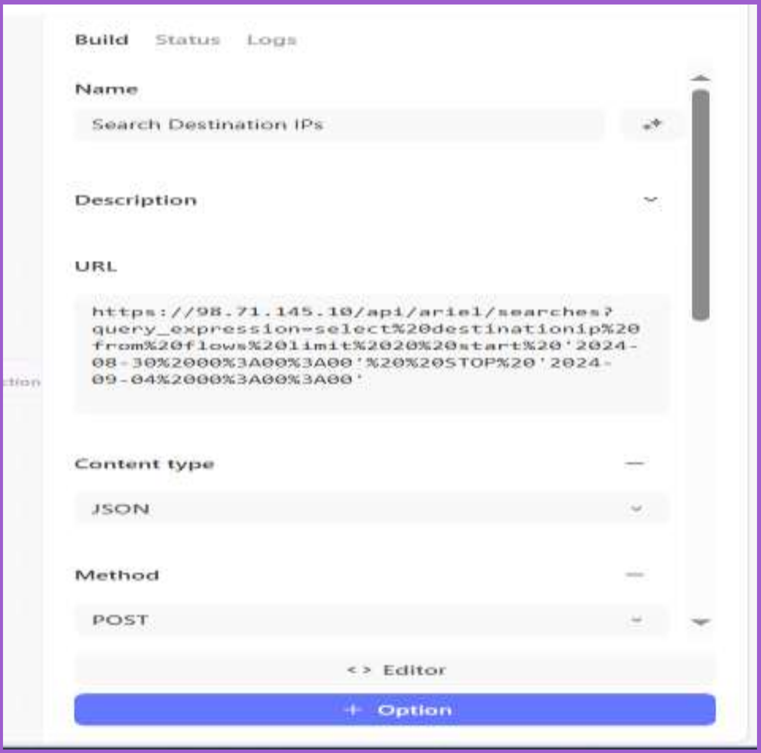
Parameter	Type	Value	Data Type	MIME Type	Sample	Description
query_expression	Query	08-30 00:00:00' STOP '2024-09-04 00:00:00'	String	text/plain	String	Optional - The AQL query to execute. Mutually exclusive with saved_search_id
saved_search_id	Query		Number (Integer)	text/plain	42	Optional - Saved search ID to execute. Mutually exclusive with queryExpression.

It will generate for us two things the url that we will use it on tines and the search id that we will put in results to to get the url of our results



```
https://98.71.145.10/api/ariel/searches?query_expression=select%20destinationip%20from%20flows%20limit%2020%20start%20'2024-08-
30%2000%3A00%3A00'%20%20STOP%20'2024-09-04%2000%3A00%3A00'
```

We take this url and put it in tines in the http request and make it post and deactivate the ssl as q radar is work on http not https and add header we name it SEC and it in the value entry the api of our q radar



Name

Search Destination IPs

Description

URL

```
https://98.71.145.10/api/ariel/searches?
query_expression=select%20destinationip%20
from%20flows%20limit%2020%20start%20'2024-
08-30%2000%3A00%3A00'%20%20STOP%20'2024-
09-04%2000%3A00%3A00'
```

Content type

JSON

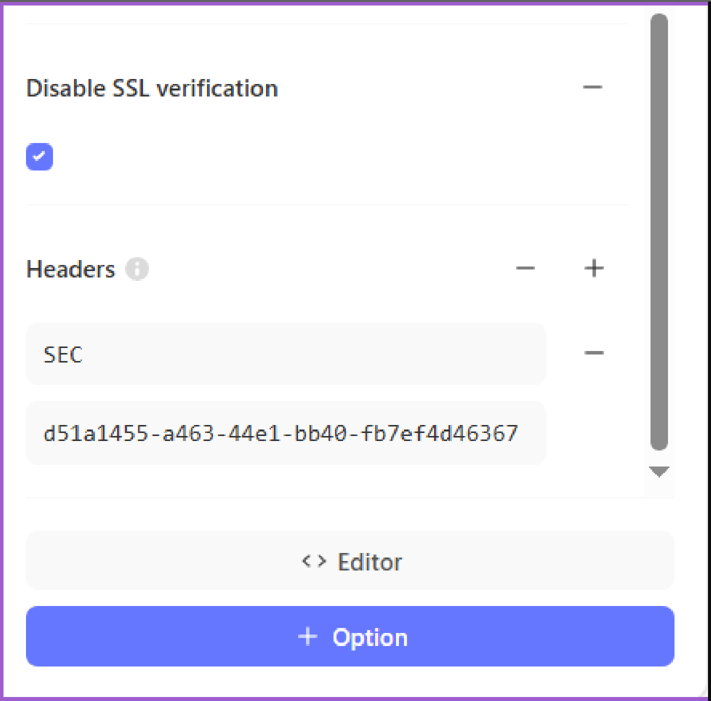
Method

POST

And we get this api

From admin tab at

Authorzed serveices



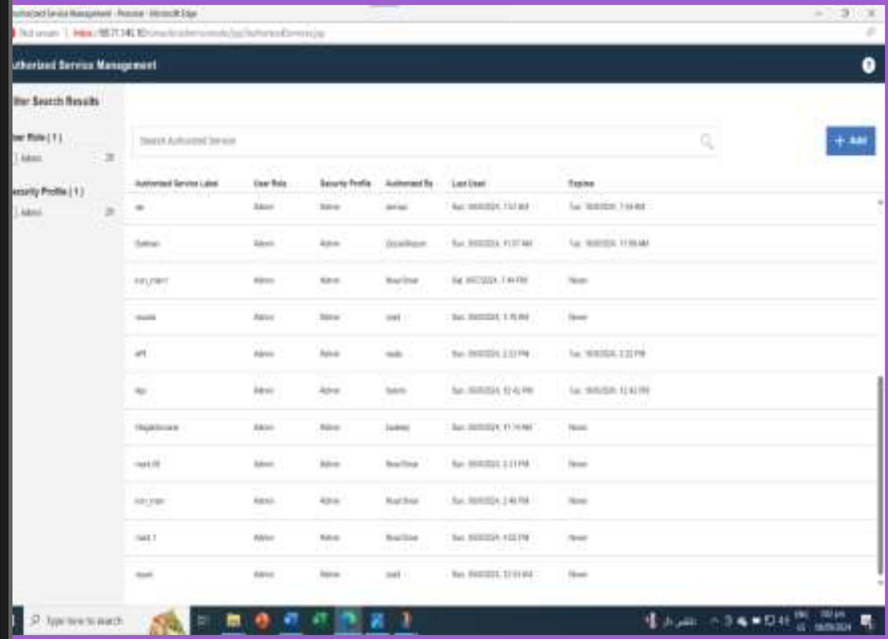
Disable SSL verification

☑

Headers

SEC

d51a1455-a463-44e1-bb40-fb7ef4d46367



Authorized Service Management

Filter Search Results

User Role (1)

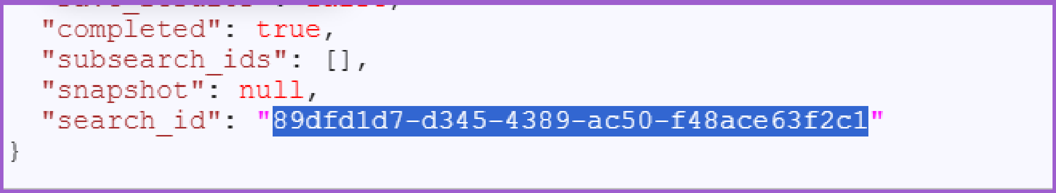
□ Admin 20

Security Profile (1)

□ Admin 20

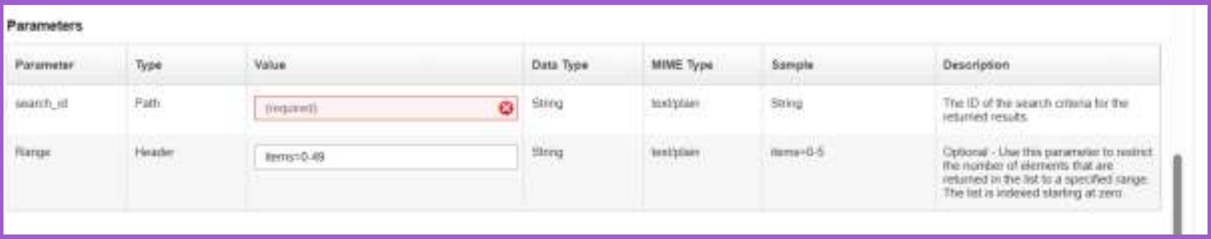
Authorized Service Label	User Role	Security Profile	Authorized By	Last Used	Expires
[illegible]	Admin	Admin	[illegible]	[illegible]	[illegible]
Batman	Admin	Admin	[illegible]	[illegible]	[illegible]
iron_man	Admin	Admin	[illegible]	[illegible]	Never
[illegible]	Admin	Admin	[illegible]	[illegible]	Never
[illegible]	Admin	Admin	[illegible]	[illegible]	[illegible]
[illegible]	Admin	Admin	[illegible]	[illegible]	[illegible]
[illegible]	Admin	Admin	[illegible]	[illegible]	Never
[illegible]	Admin	Admin	[illegible]	[illegible]	Never
iron_man	Admin	Admin	[illegible]	[illegible]	Never
[illegible]	Admin	Admin	[illegible]	[illegible]	Never
[illegible]	Admin	Admin	[illegible]	[illegible]	Never

And we add new one we named it by our team iron_man and generate the api key.



```
  "completed": true,
  "subsearch_ids": [],
  "snapshot": null,
  "search_id": "89dfd1d7-d345-4389-ac50-f48ace63f2c1"
}
```

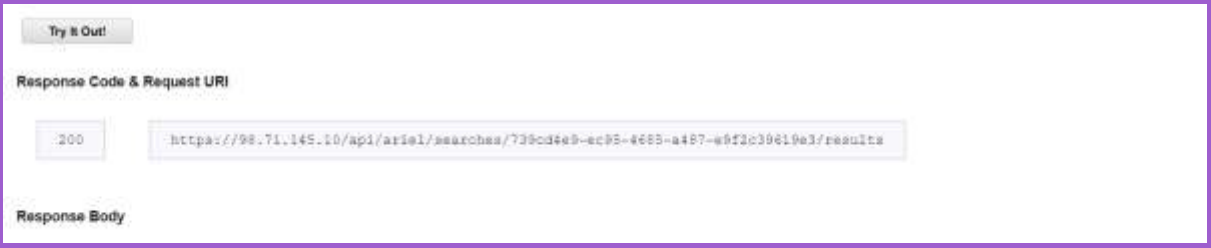
Then we take this and open the results and put it in search id entery to get the url of the result to put in tines we also make the same steps like we make in search



Parameters

Parameter	Type	Value	Data Type	MIME Type	Sample	Description
search_id	Path	(required)	String	text/plain	String	The ID of the search criteria for the returned results.
Range	Header	items=0-49	String	text/plain	items=0-5	Optional - Use this parameter to restrict the number of elements that are returned in the list to a specified range. The list is indexed starting at zero.

The url that we put in tines



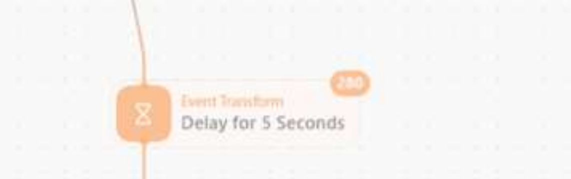
Response Code & Request URI

200 https://98.71.145.10/api/ariel/searches/739cd4e9-ec95-4685-a487-e9f2c39619e3/results

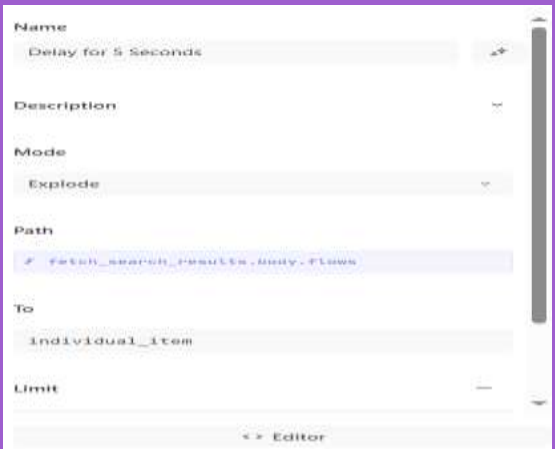
Response Body

Then in tines we do the follow :

1. We add the event transform



2. Then we configure it by the follow



Name
Delay for 5 Seconds

Description

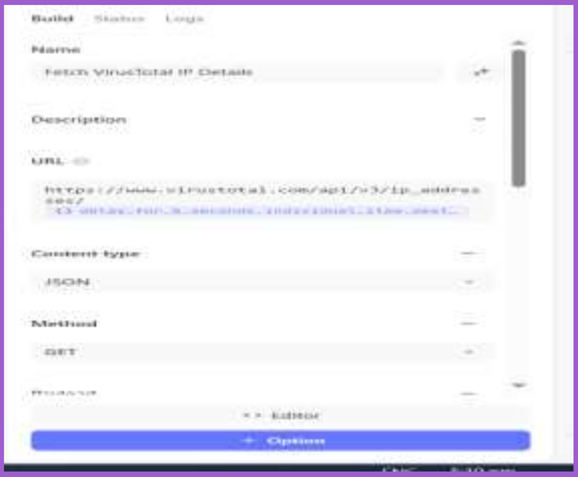
Mode
Explode

Path
fetch_search_results.body.flows

To
individual_item

Limit

3. Then we add another http request and we connect it with the viroustotal to check the ip that we get from q radar if it’s malicious or not and we configure it as follow



Name
Fetch VirusTotal IP Details

Description

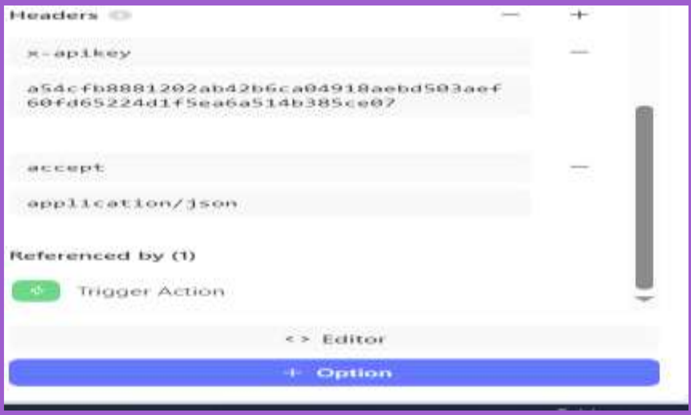
URL
https://www.virustotal.com/api/v3/ip_addresses/
delay_for_5_seconds.individual_item.[illegible]

Content type
JSON

Method
GET

Payload

then we add two header
first header we will
call it x-apikey
and put in it the api of
virous total and the sec.
Header we will name it
accept and we will put in the value application/jason



Headers

x-apikey

a54cfb8881202ab42b6ca04918aebd503aef
60fd65224d1f5ea6a514b385ce07

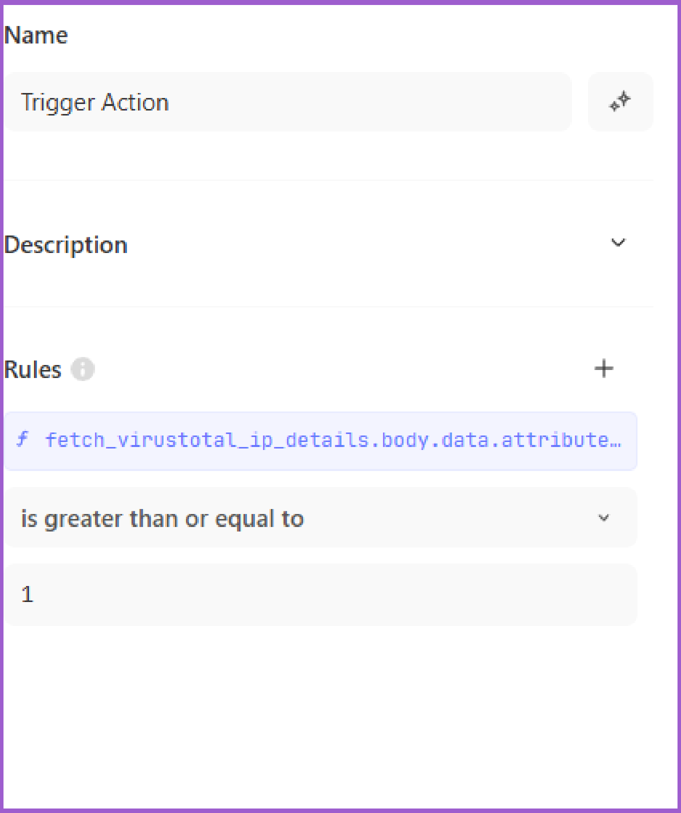
accept

application/json

Referenced by (1)

Trigger Action

4. We will add the trigger and we will make the function in it to greater than or equal and we will put the value 1 so if the virus total check that the ip is malicious by 1 or more it will sent me email



Name

Trigger Action

Description

Rules

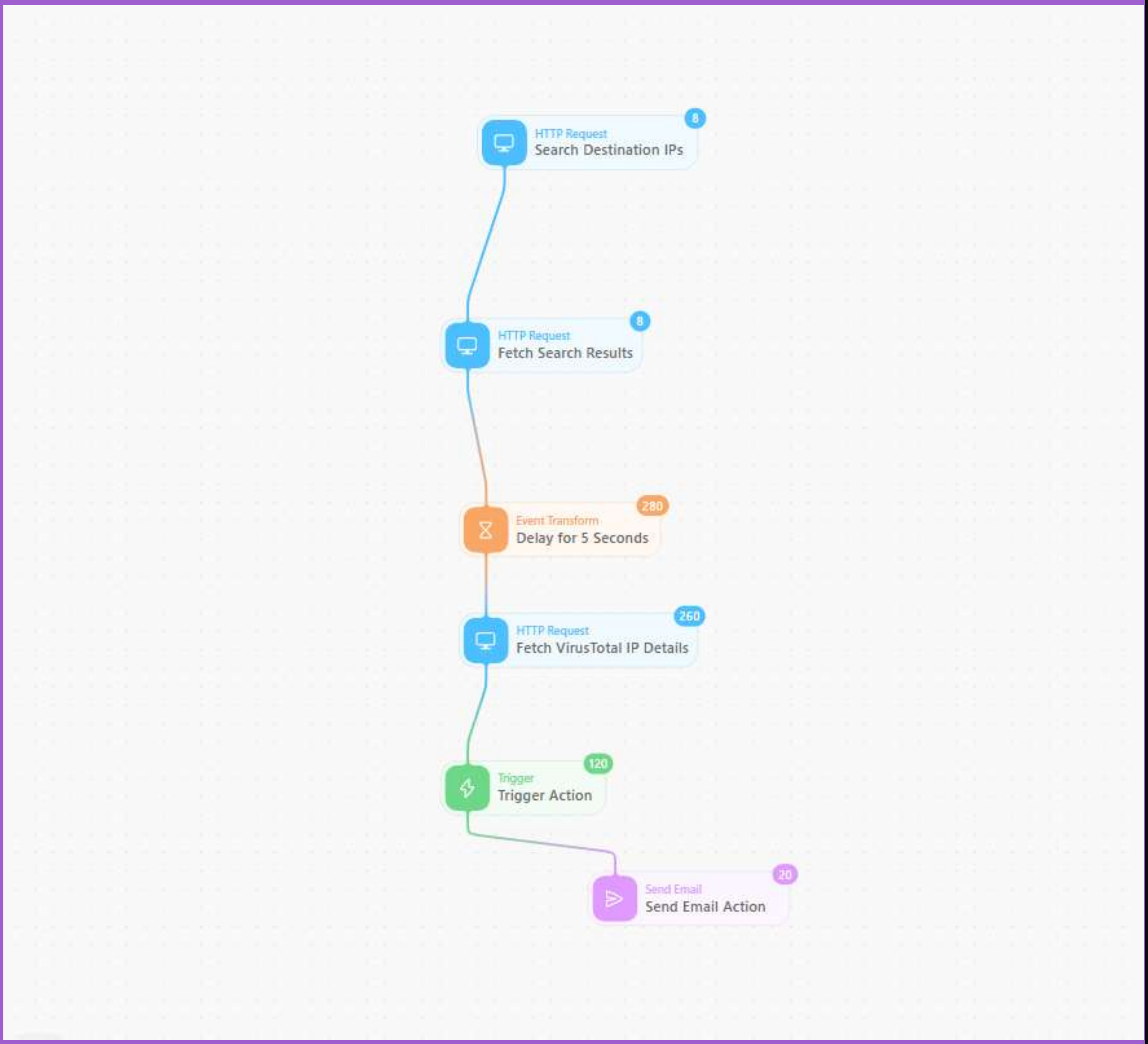
```
ƒ fetch_virustotal_ip_details.body.data.attribute…
```

is greater than or equal to

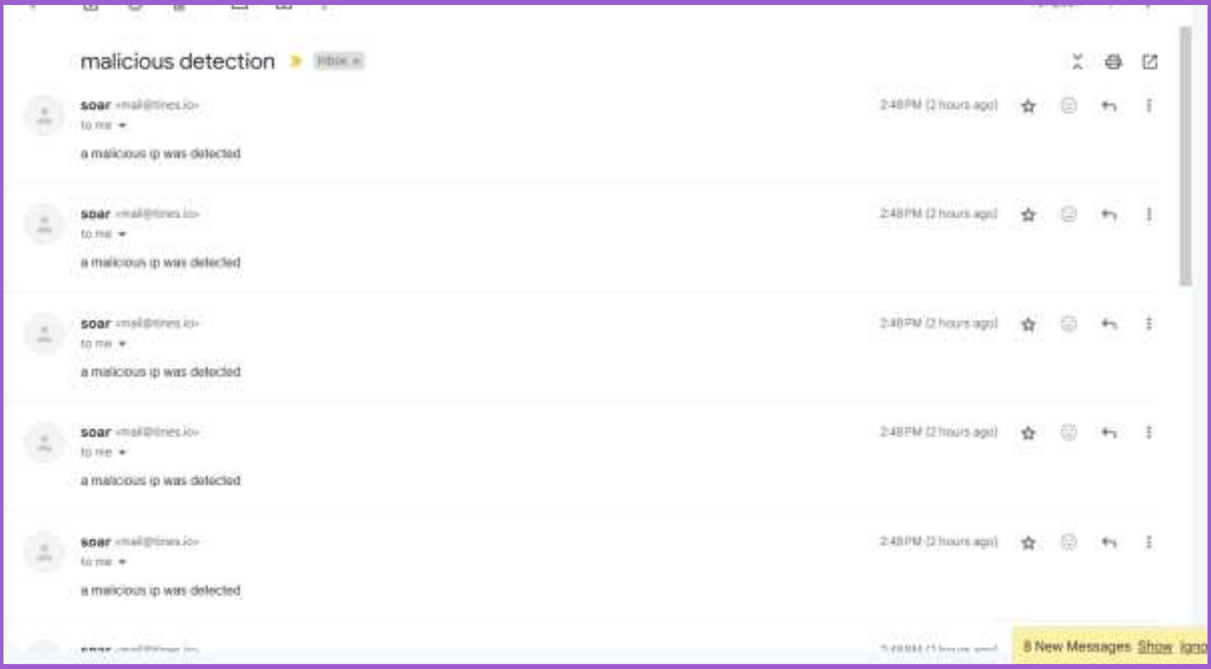
1

5. Then we will add the (send email tool) to send us email if soar cheks a malicious ip

6. So the final diagram will be



And then we run it send email that it find a malicious ip



malicious detection Inbox

soar <mail@tines.io>
to me
2:48 PM (2 hours ago)

a malicious ip was detected

soar <mail@tines.io>
to me
2:48 PM (2 hours ago)

a malicious ip was detected

soar <mail@tines.io>
to me
2:48 PM (2 hours ago)

a malicious ip was detected

soar <mail@tines.io>
to me
2:48 PM (2 hours ago)

a malicious ip was detected

soar <mail@tines.io>
to me
2:48 PM (2 hours ago)

a malicious ip was detected