

Tines Integration with QRadar and Virus total

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

REQUIREMENTS

- 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](https://98.71.145.10/API_DOC) WE GO TO

ARIAL → SEARCHES → POST

GET POST

17.0 - POST - /ariel/searches

query_expression	Query	SELECT destinationip from flows GROUP BY destinationip LAST 3 DAYS	String	text/plain	String	Optional. The ACL 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

cURL

```
curl -X POST -u Admin@ihaiwag -H 'Version: 17.0' -H 'Accept: application/json' 'https://98.71.145.10/ariel/searches?query_expression=SELECT%20destinationip%20from%20flows%20GROUP%20BY%20destinationip%20LAST%203%20DAYS%20'
```

Try It Out

Response Code & Request URI

201 https://98.71.145.10/ariel/searches?query_expression=SELECT%20destinationip%20from%20flows%20GROUP%20BY%20destinationip%20LAST%203%20DAYS%20

Response Body

```
{
  "cursor_id": "0b32a43-9d1e-4150-876d-5a31951fb49",
  "status": "WAIT",
  "compressed_data_file_count": 0,
  "compressed_data_total_size": 0,
  "data_file_count": 0,
  "data_total_size": 0,
  "index_file_count": 0,
  "index_total_size": 0,
  "processed_record_count": 0,
  "desired_retention_time_msec": 86400000,
  "progress": 0,
  "progress_details": {},
  "query_execution_time": 0,
  "source_action": "SELECT destinationip from flows GROUP BY destinationip LAST 3 DAYS"
}
```

[HTTPS://98.71.145.10/API/ARIEL/SEARCHES?](https://98.71.145.10/API/ARIEL/SEARCHES?)

[QUERY_EXPRESSION=SELECT%20DESTINATIONIP%20FROM%20FLOWS%20GROUP%20BY%20DESTINATIONIP%20LAST%203%20DAYS%20V](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

17.0 - GET - /ariel/searches/[search_id]/results

Parameters

Parameter	Type	Value	Data Type	MIME Type	Sample	Description
search_id	Path	78d3b22c-1e3e-4c87-a653-1e19dbd80367	String	text/plain	String	The ID of the search criteria for the returned results.
Range	Header		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.

cURL

```
curl -S -X GET -u AhmedElhalwasy -H 'Version: 17.0' -H 'Accept: application/json' 'https://98.71.145.10/api/ariel/searches/78d3b22c-1e3e-4c87-a653-1e19dbd80367/results'
```

Try It Out

Response Code & Request URI

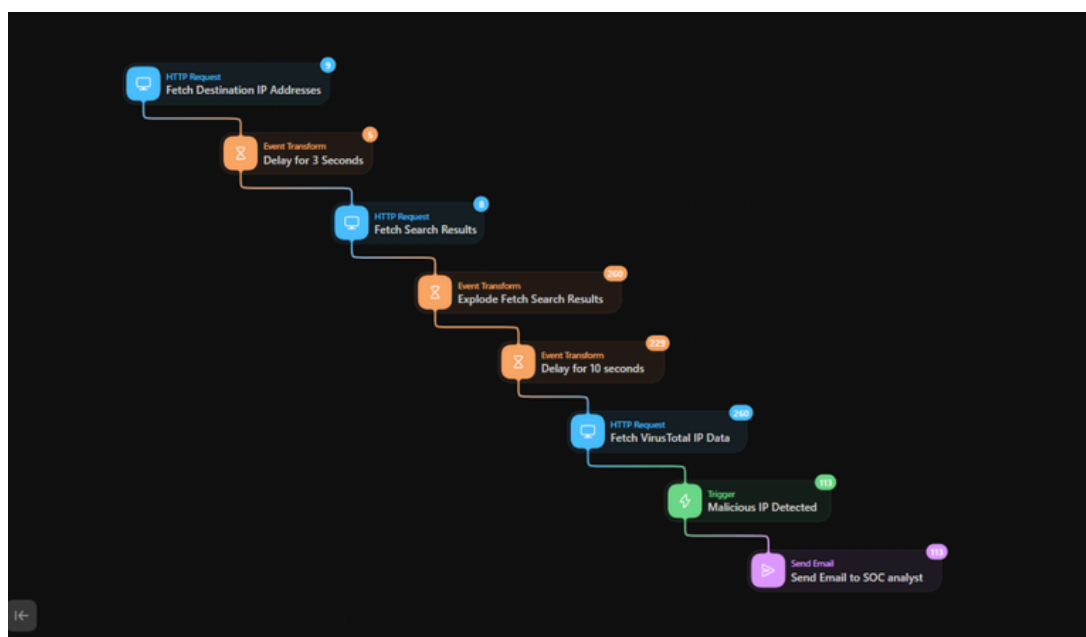
200 https://98.71.145.10/api/ariel/searches/78d3b22c-1e3e-4c87-a653-1e19dbd80367/results

Response Body

```
{
  "flows": [
    {
      "destinationip": "169.254.169.254"
    },
    {
      "destinationip": "142.92.34.113"
    }
  ]
}
```

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

A screenshot of a REST client configuration interface. The 'Name' field is 'Fetch Destination IP Addresses'. The 'Description' field is empty. The 'URL' field contains a query expression: `https://98.71.145.10/api/ariel/searches?query_expression=SELECT%20destinationip%20as%20dest_ip%20from%20flows%20GROUP%20BY%20destinationip%20LAST%203%20DAYS`. The 'Content type' is set to 'JSON'. The 'Method' is set to 'POST'.

A screenshot of a REST client configuration interface. The 'Name' field is 'Fetch Destination IP Addresses'. The 'Description' field is empty. The 'URL' field contains a query expression: `https://98.71.145.10/api/ariel/searches?query_expression=SELECT%20destinationip%20as%20dest_ip%20from%20flows%20GROUP%20BY%20destinationip%20LAST%203%20DAYS`. The 'Content type' is set to 'JSON'. The 'Method' is set to 'POST'.

4.2. DELAY FOR 3 SECONDS

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

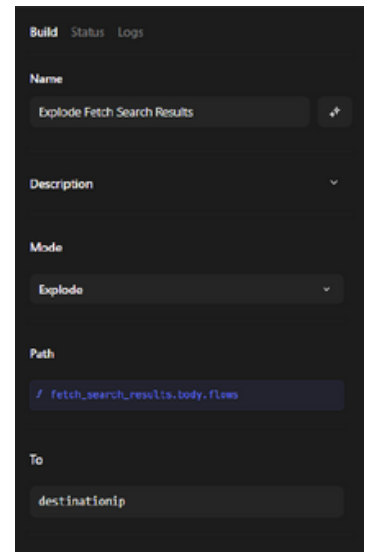
A screenshot of a REST client configuration interface. The 'Name' field is 'Fetch Search Results'. The 'Description' field is empty. The 'URL' field contains a query expression: `https://98.71.145.10/api/ariel/searches/{> fetch_local_destination_addresses.body...}/results`. The 'Content type' is set to 'JSON'. The 'Method' is set to 'GET'.



STEPS

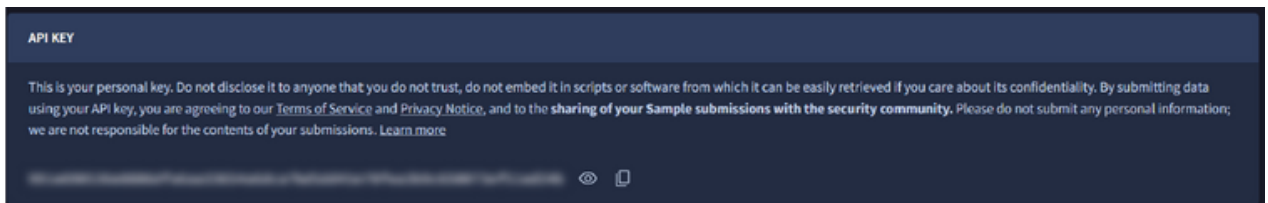
4.4. EVENT TRANSFORM MODULE EXPLODE TO EXTRACT THE DESTINATION IP ADDRESS AND PUT THEM INTO AN ARRAY

4.5. DELAY FOR 10 SECONDS



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

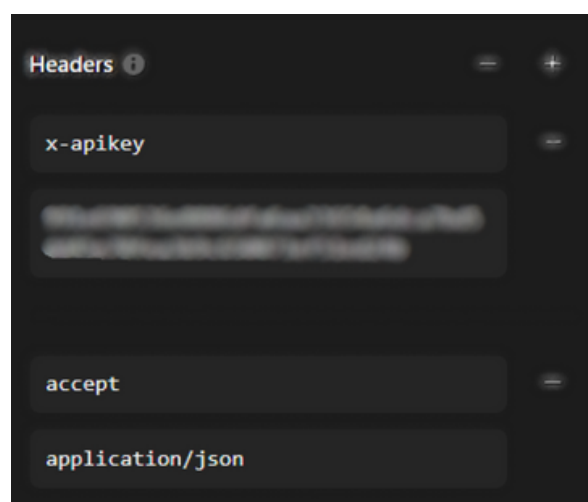
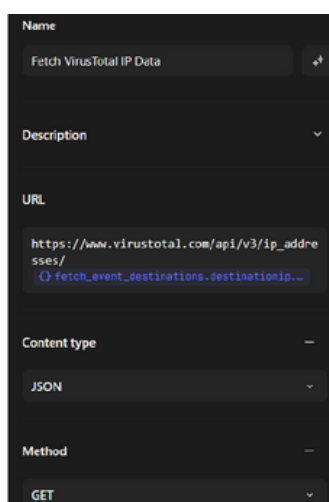
- WE FIRST NEED TO CREATE AN ACCOUNT ON VIRUS TOTAL
- GO TO API KEY



- 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

Build Status Logs

Name

Malicious IP Detected

Description

Rules

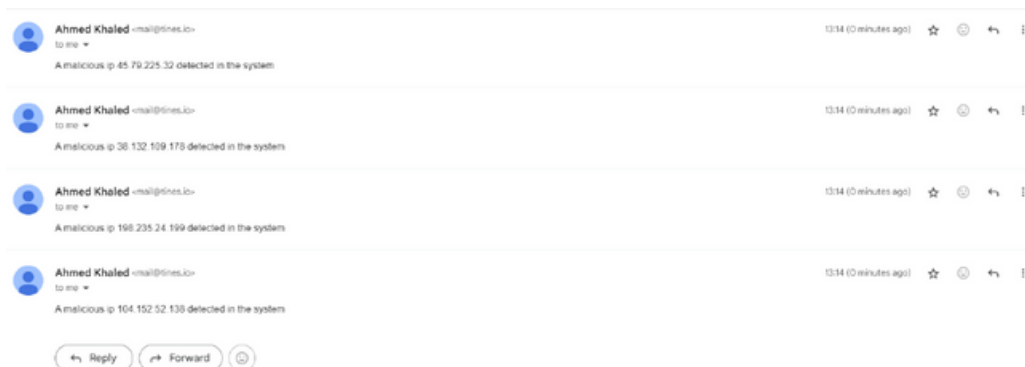
`f fetch_virustotal_ip_data.body.data.attributes...`

is greater than or equal to

1

8. IF THE TRIGGER TRUE SEND EMAIL SAYING

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



Recipients

List

`ahmedkhaled@prines.io`

+ Add Item

Reply to

`ahmedkhaled@prines.io`

Sender name

SOAR solution

Subject

malicious ip detected

Body

A malicious ip
(`fetch_virustotal_ip_data.body.data.id`)
detected in the system

