Microsoft

Azure Sentinel Level 400 #7

Technical Overview

Ofer Shezaf

About module #6: Rule writing

Overview

- In this module you will learn how write Azure Sentinel Playbooks.

Pre-requisites

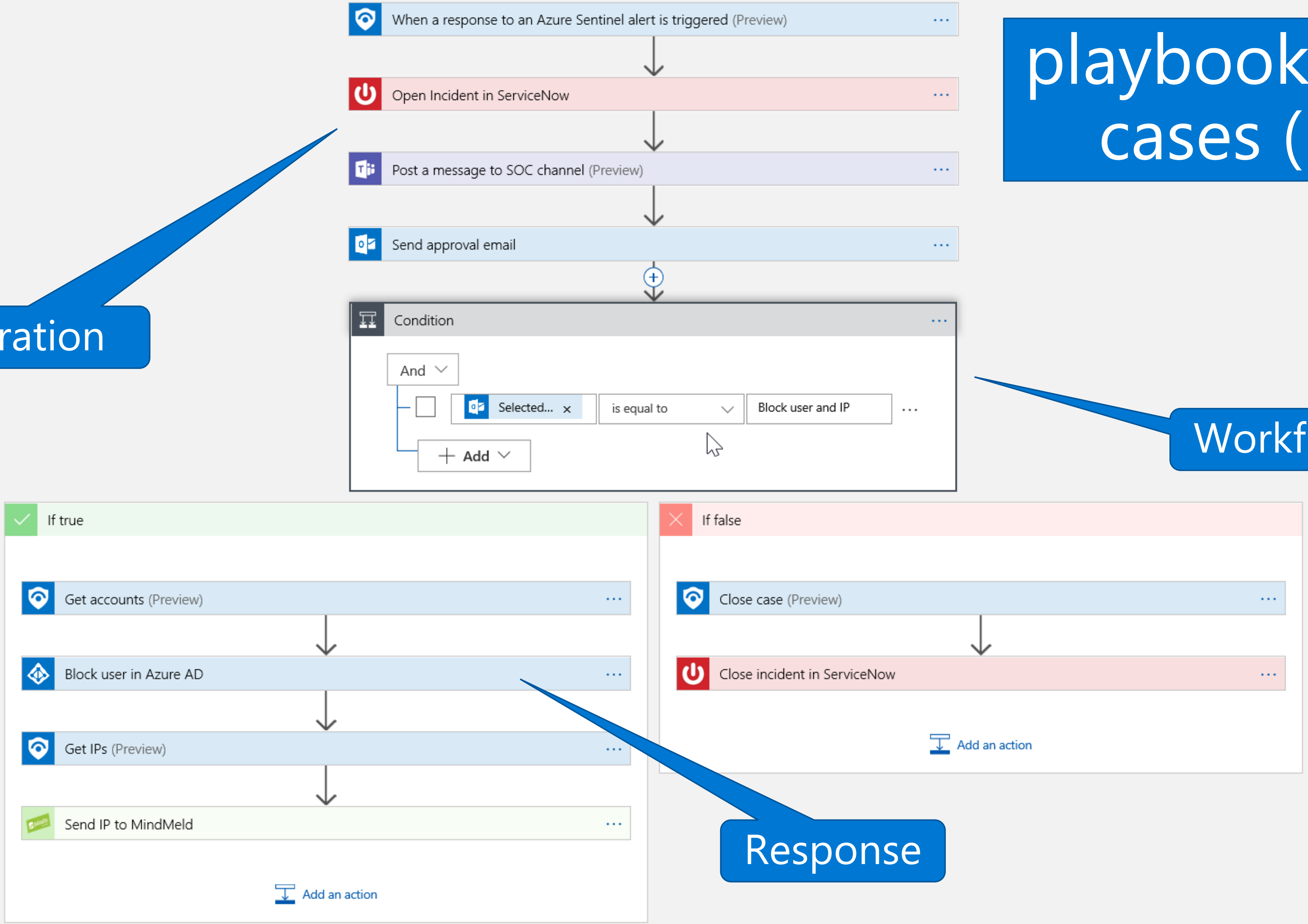
- Azure Sentinel Overview module.

Agenda

- Playbooks use cases
- When is a playbook triggered
- Playbook development
- Creating a workbook walkthrough

Playbook use cases

playbook use cases (1)



When a response to an Azure Sentinel alert is triggered (Preview)

Open Incident in ServiceNow

Post a message to SOC channel (Preview)

Send approval email

Condition

And

Selected... × | is equal to | Block user and IP

+ Add

If true

Get accounts (Preview)

Block user in Azure AD

Get IPs (Preview)

Send IP to MindMeld

Add an action

If false

Close case (Preview)

Close incident in ServiceNow

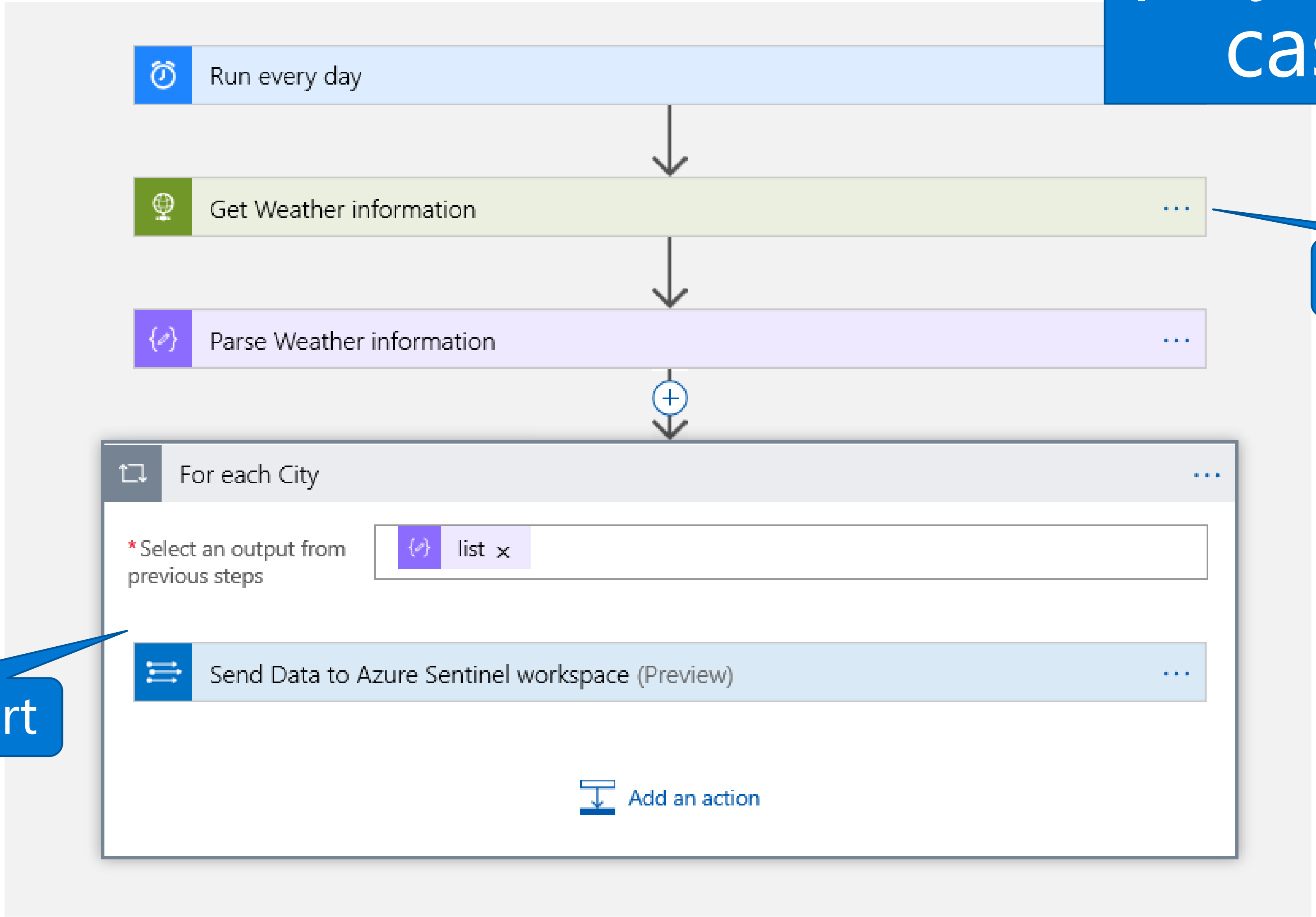
Add an action

integration

Workflow

Response

playbook use cases (2)



Run every day

Get Weather information

Parse Weather information

For each City

*Select an output from previous steps: list

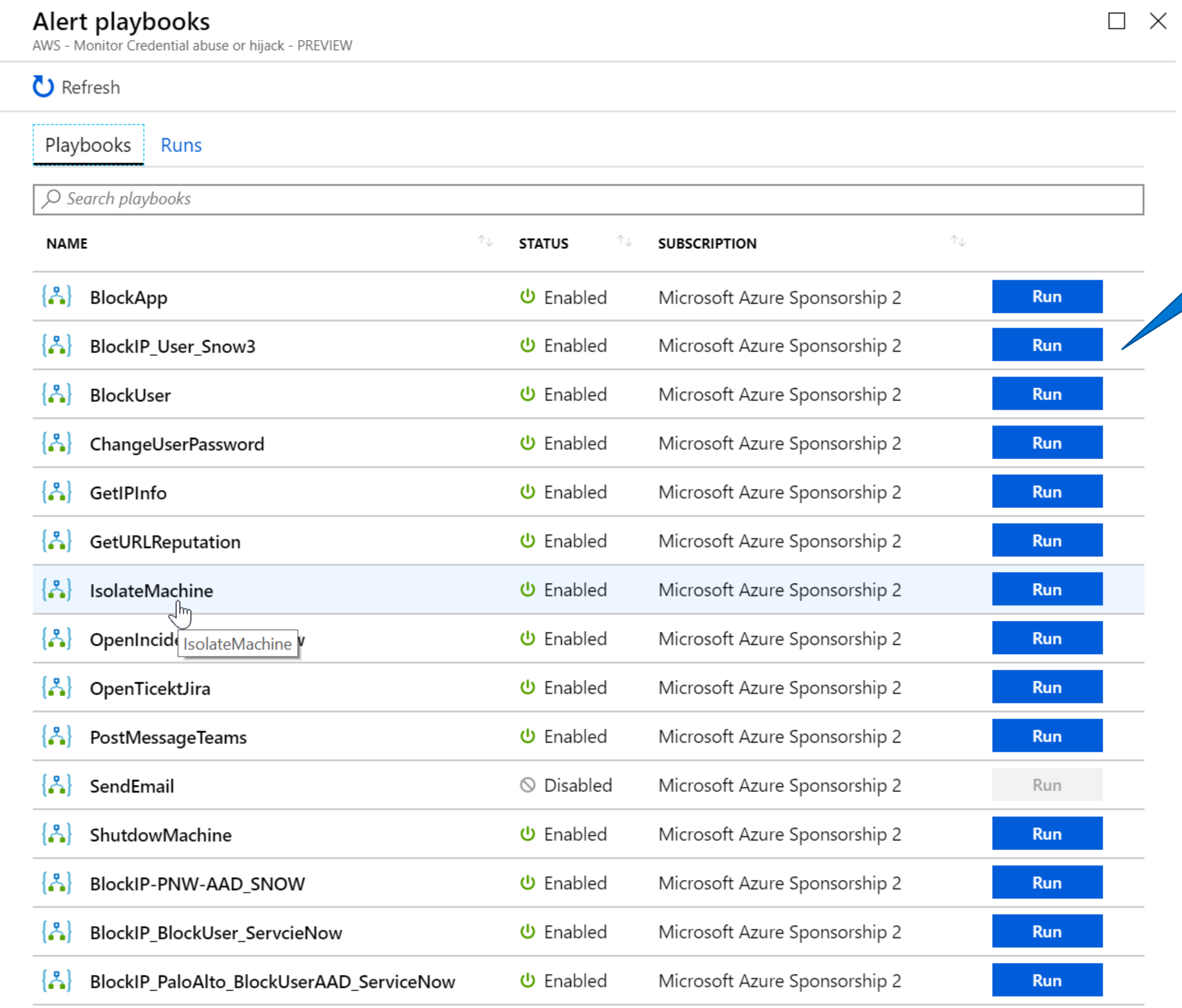
Send Data to Azure Sentinel workspace (Preview)

Add an action

Enrichment

Data import

Triggers

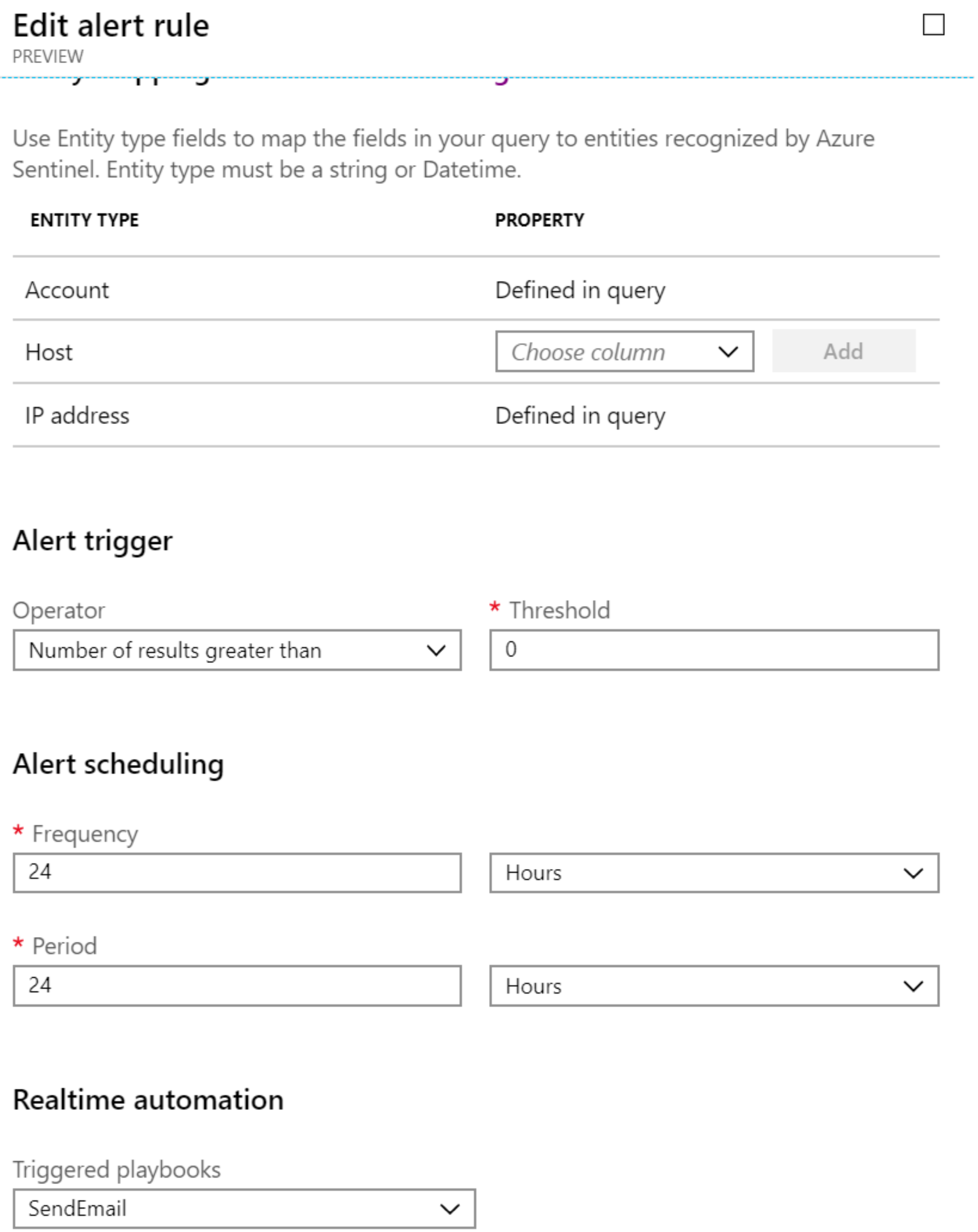


Alert playbooks

AWS - Monitor Credential abuse or hijack - PREVIEW

NAME	STATUS	SUBSCRIPTION	
BlockApp	Enabled	Microsoft Azure Sponsorship 2	Run
BlockIP_User_Snow3	Enabled	Microsoft Azure Sponsorship 2	Run
BlockUser	Enabled	Microsoft Azure Sponsorship 2	Run
ChangeUserPassword	Enabled	Microsoft Azure Sponsorship 2	Run
GetIPInfo	Enabled	Microsoft Azure Sponsorship 2	Run
GetURLReputation	Enabled	Microsoft Azure Sponsorship 2	Run
IsolateMachine	Enabled	Microsoft Azure Sponsorship 2	Run
OpenIncide w	Enabled	Microsoft Azure Sponsorship 2	Run
OpenTicektJira	Enabled	Microsoft Azure Sponsorship 2	Run
PostMessageTeams	Enabled	Microsoft Azure Sponsorship 2	Run
SendEmail	Disabled	Microsoft Azure Sponsorship 2	Run
ShutdowMachine	Enabled	Microsoft Azure Sponsorship 2	Run
BlockIP-PNW-AAD_SNOW	Enabled	Microsoft Azure Sponsorship 2	Run
BlockIP_BlockUser_ServcieNow	Enabled	Microsoft Azure Sponsorship 2	Run
BlockIP_PaloAlto_BlockUserAAD_ServiceNow	Enabled	Microsoft Azure Sponsorship 2	Run

Manually on an alert



Edit alert rule

PREVIEW

Use Entity type fields to map the fields in your query to entities recognized by Azure Sentinel. Entity type must be a string or Datetime.

ENTITY TYPE	PROPERTY
Account	Defined in query
Host	Choose column ⌄ Add
IP address	Defined in query

Alert trigger

Operator: Number of results greater than

* Threshold: 0

Alert scheduling

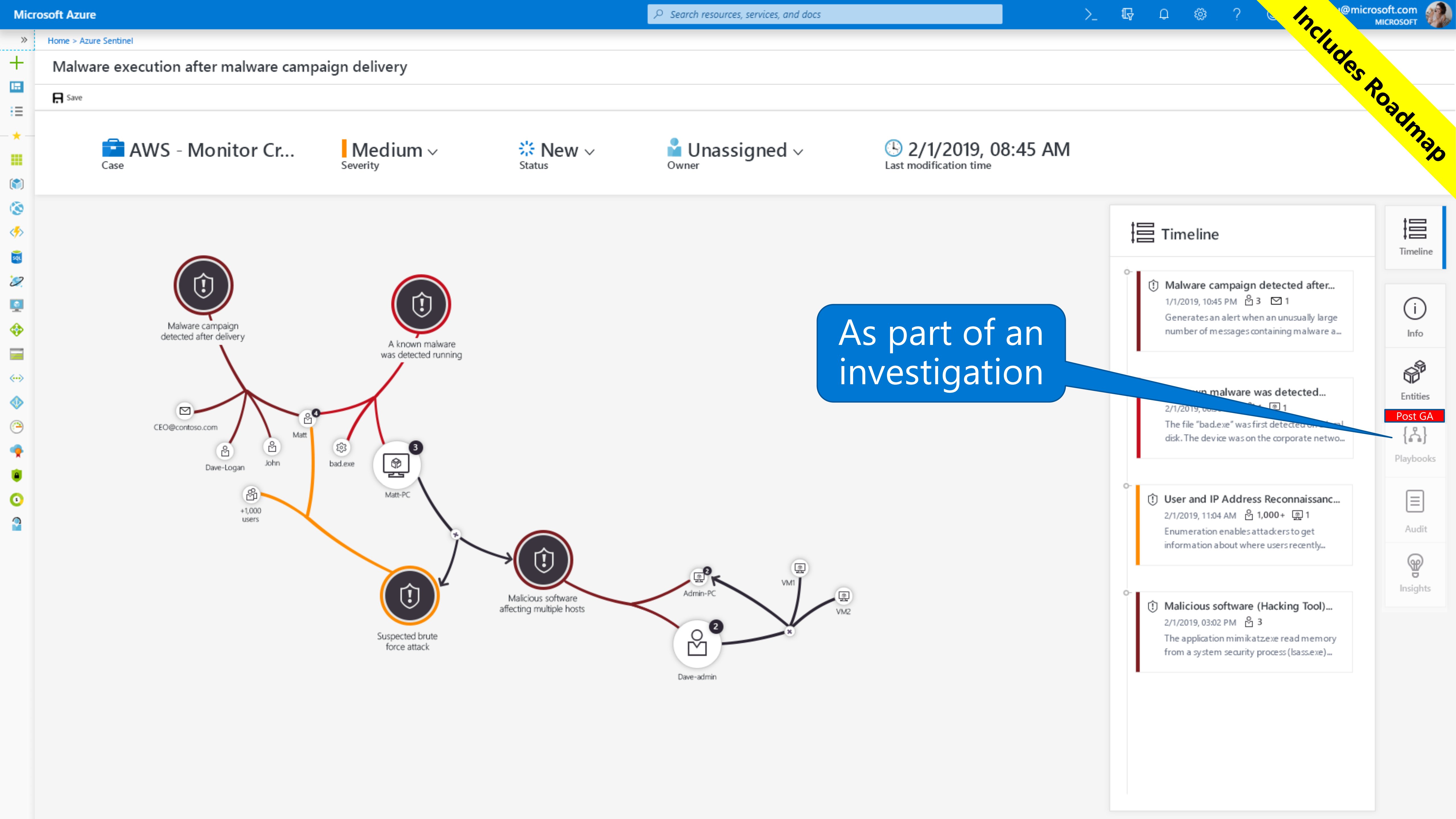
* Frequency: 24 Hours

* Period: 24 Hours

Realtime automation

Triggered playbooks: SendEmail

Automatically when an alert trigges



Malware execution after malware campaign delivery

AWS - Monitor Cr...	Medium	New	Unassigned	2/1/2019, 08:45 AM
Case	Severity	Status	Owner	Last modification time

Timeline

Malware campaign detected after...
1/1/2019, 10:45 PM 3 1
Generates an alert when an unusually large number of messages containing malware a...

wn malware was detected...
2/1/2019, 1
The file "bad.exe" was first detected disk. The device was on the corporate netwo...

User and IP Address Reconnaissanc...
2/1/2019, 11:04 AM 1,000+ 1
Enumeration enables attackers to get information about where users recently...

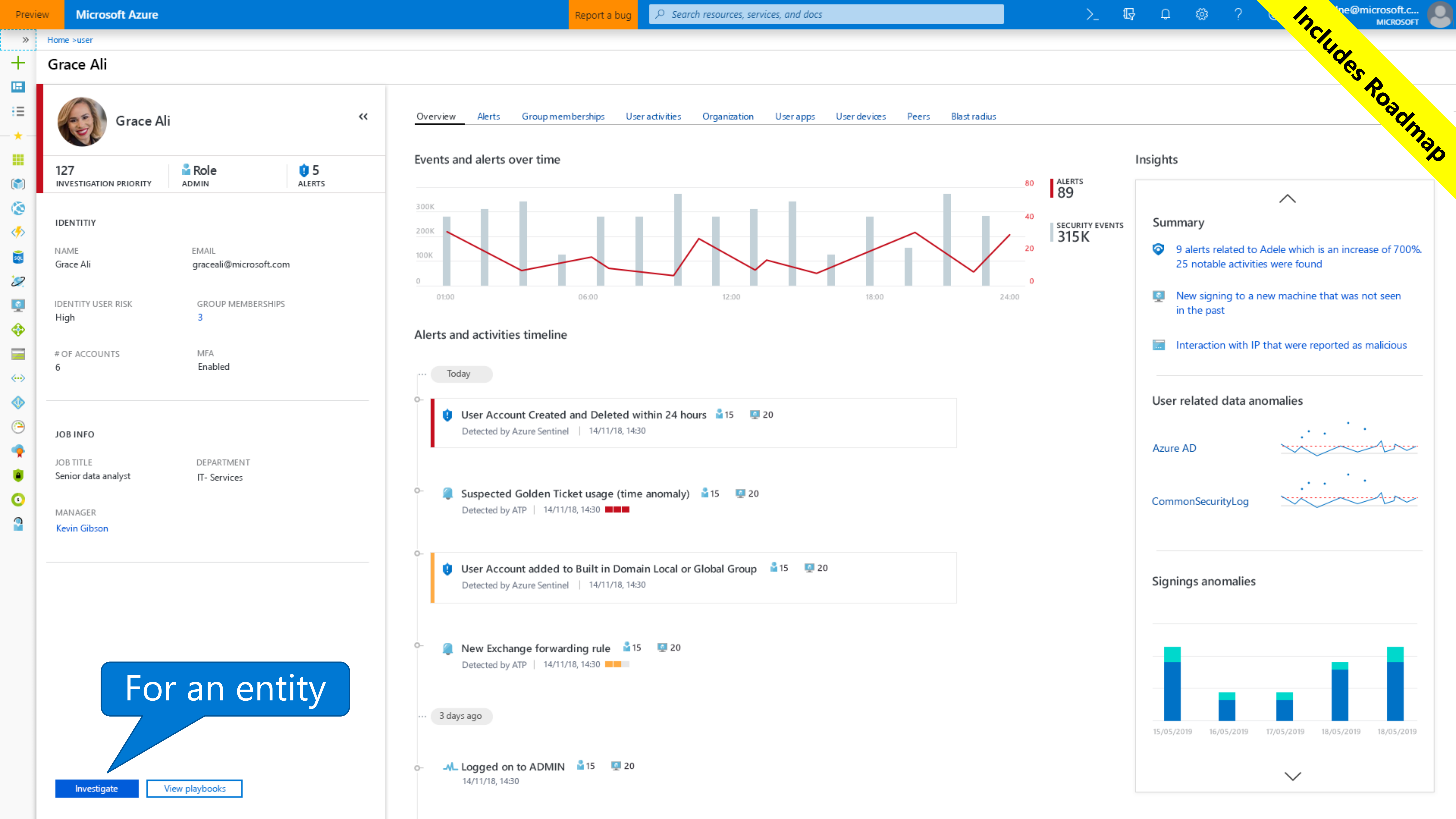
Malicious software (Hacking Tool)...
2/1/2019, 03:02 PM 3
The application mimikatz.exe read memory from a system security process (lsass.exe)...

Includes Roadmap

As part of an investigation

Post GA

Includes Roadmap



Home > user

Grace Ali

Grace Ali

127	Role	5
INVESTIGATION PRIORITY	ADMIN	ALERTS

IDENTITIY

NAME Grace Ali	EMAIL graceali@microsoft.com
IDENTITY USER RISK High	GROUP MEMBERSHIPS 3
# OF ACCOUNTS 6	MFA Enabled

JOB INFO

JOB TITLE Senior data analyst	DEPARTMENT IT- Services
MANAGER Kevin Gibson	

Investigate | View playbooks

For an entity

Overview | Alerts | Group memberships | User activities | Organization | User apps | User devices | Peers | Blast radius

Events and alerts over time

ALERTS 89

SECURITY EVENTS 315K

Alerts and activities timeline

Today

- User Account Created and Deleted within 24 hours 15 20
  Detected by Azure Sentinel | 14/11/18, 14:30
- Suspected Golden Ticket usage (time anomaly) 15 20
  Detected by ATP | 14/11/18, 14:30
- User Account added to Built in Domain Local or Global Group 15 20
  Detected by Azure Sentinel | 14/11/18, 14:30
- New Exchange forwarding rule 15 20
  Detected by ATP | 14/11/18, 14:30

3 days ago

- Logged on to ADMIN 15 20
  14/11/18, 14:30

Insights

Summary

- 9 alerts related to Adele which is an increase of 700%. 25 notable activities were found
- New signing to a new machine that was not seen in the past
- Interaction with IP that were reported as malicious

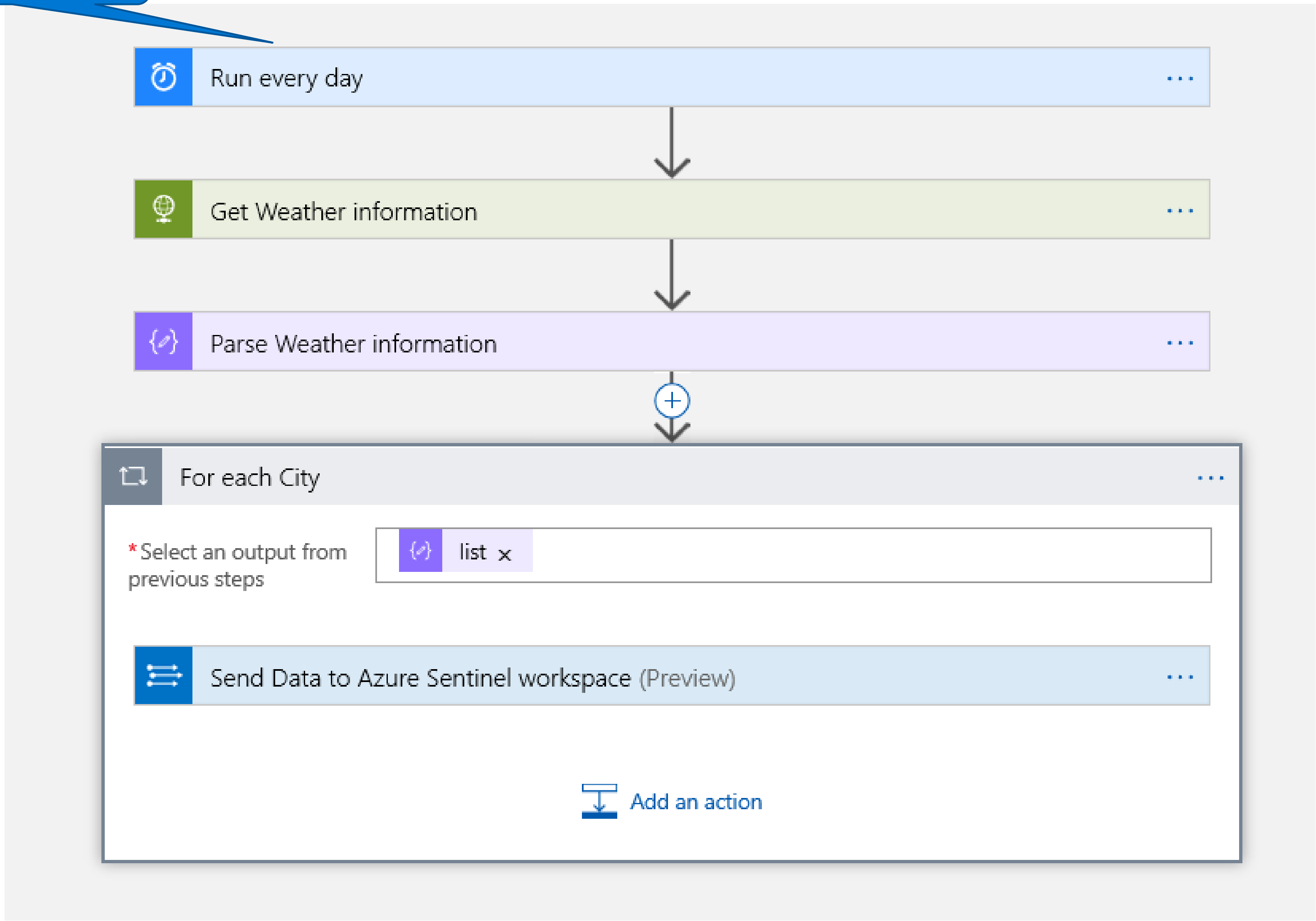
User related data anomalies

Azure AD

CommonSecurityLog

Signings anomalies

Scheduled



Run every day

Get Weather information

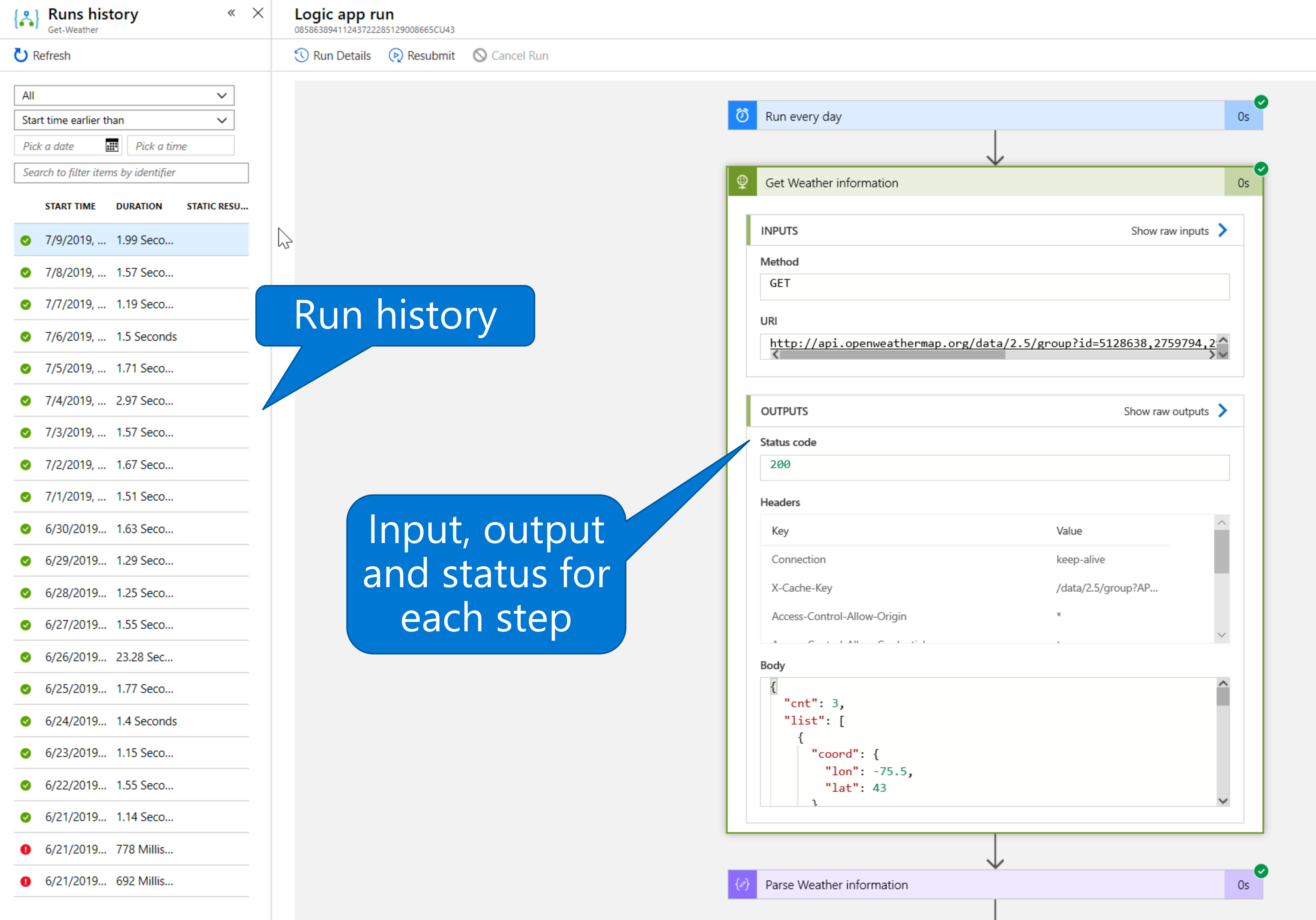
Parse Weather information

For each City

*Select an output from previous steps: list

Send Data to Azure Sentinel workspace (Preview)

Development



Runs history
Get-Weather

Refresh

All

Start time earlier than

Pick a date Pick a time

Search to filter items by identifier

	START TIME	DURATION	STATIC RESU...
✓	7/9/2019, ...	1.99 Seco...	
✓	7/8/2019, ...	1.57 Seco...	
✓	7/7/2019, ...	1.19 Seco...	
✓	7/6/2019, ...	1.5 Seconds	
✓	7/5/2019, ...	1.71 Seco...	
✓	7/4/2019, ...	2.97 Seco...	
✓	7/3/2019, ...	1.57 Seco...	
✓	7/2/2019, ...	1.67 Seco...	
✓	7/1/2019, ...	1.51 Seco...	
✓	6/30/2019...	1.63 Seco...	
✓	6/29/2019...	1.29 Seco...	
✓	6/28/2019...	1.25 Seco...	
✓	6/27/2019...	1.55 Seco...	
✓	6/26/2019...	23.28 Sec...	
✓	6/25/2019...	1.77 Seco...	
✓	6/24/2019...	1.4 Seconds	
✓	6/23/2019...	1.15 Seco...	
✓	6/22/2019...	1.55 Seco...	
✓	6/21/2019...	1.14 Seco...	
!	6/21/2019...	778 Millis...	
!	6/21/2019...	692 Millis...	

Logic app run
08586389411243722285129008665CU43

Run Details Resubmit Cancel Run

Run every day 0s

Get Weather information 0s

INPUTS Show raw inputs

Method
GET

URI
http://api.openweathermap.org/data/2.5/group?id=5128638,2759794,2

OUTPUTS Show raw outputs

Status code
200

Headers

Key	Value
Connection	keep-alive
X-Cache-Key	/data/2.5/group?AP...
Access-Control-Allow-Origin	*

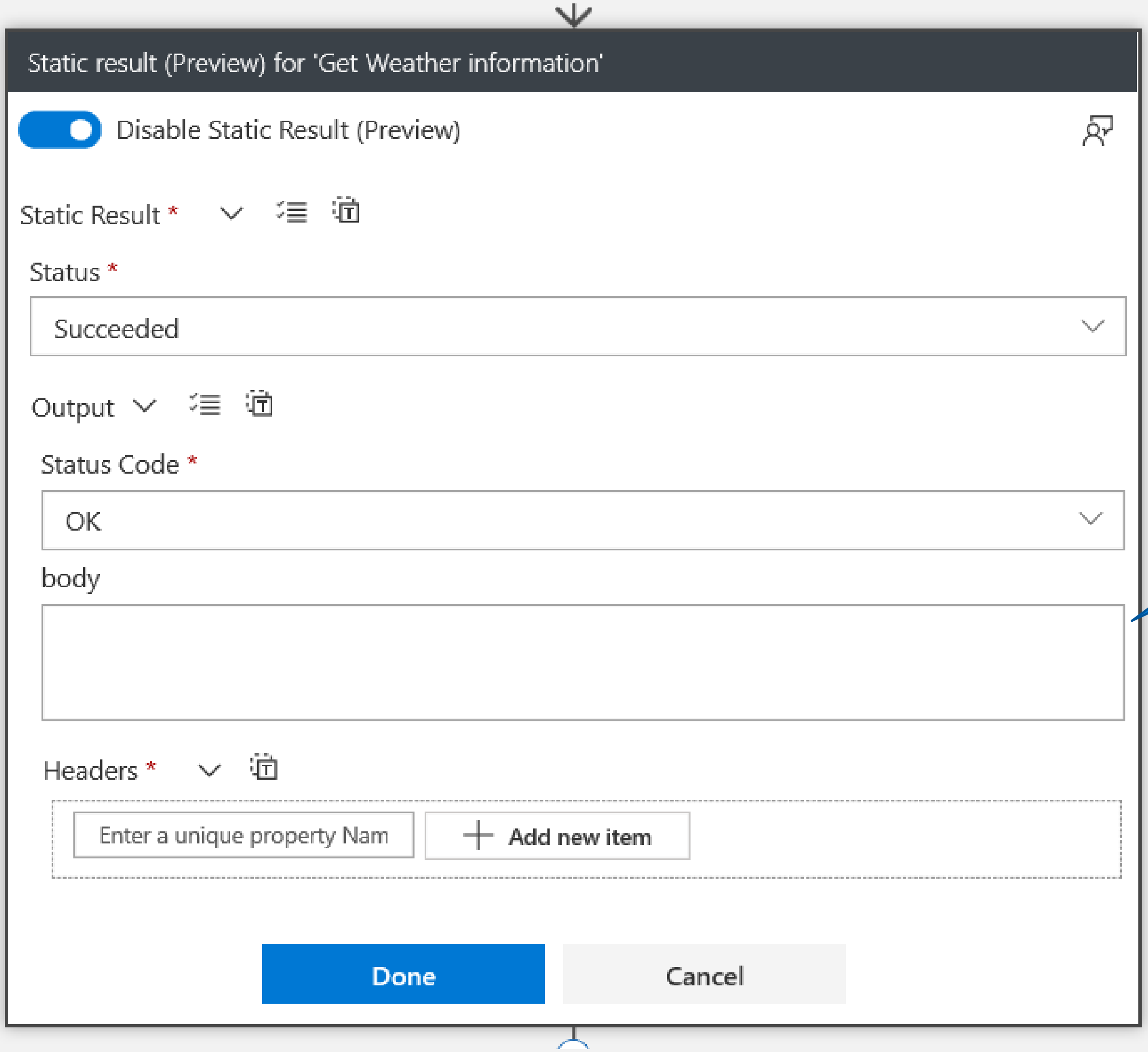
Body

```
{
  "cnt": 3,
  "list": [
    {
      "coord": {
        "lon": -75.5,
        "lat": 43
```

Parse Weather information 0s

Run history

Input, output and status for each step



Static result (Preview) for 'Get Weather information'

Disable Static Result (Preview)

Static Result *

Status *

Succeeded

Output

Status Code *

OK

body

Headers *

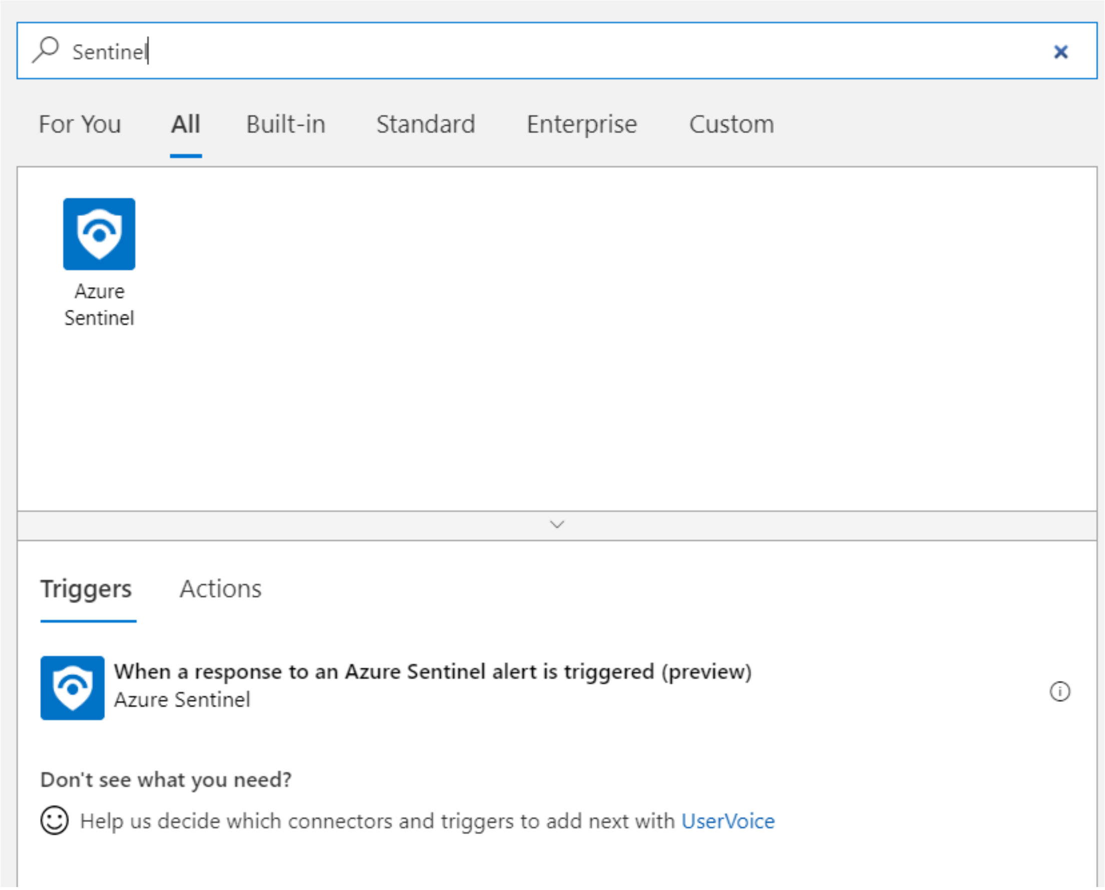
Enter a unique property Nam

Inject input

Creating a playbook

Trigger

- Populates the alert in the playbook
- One time set up of a connection



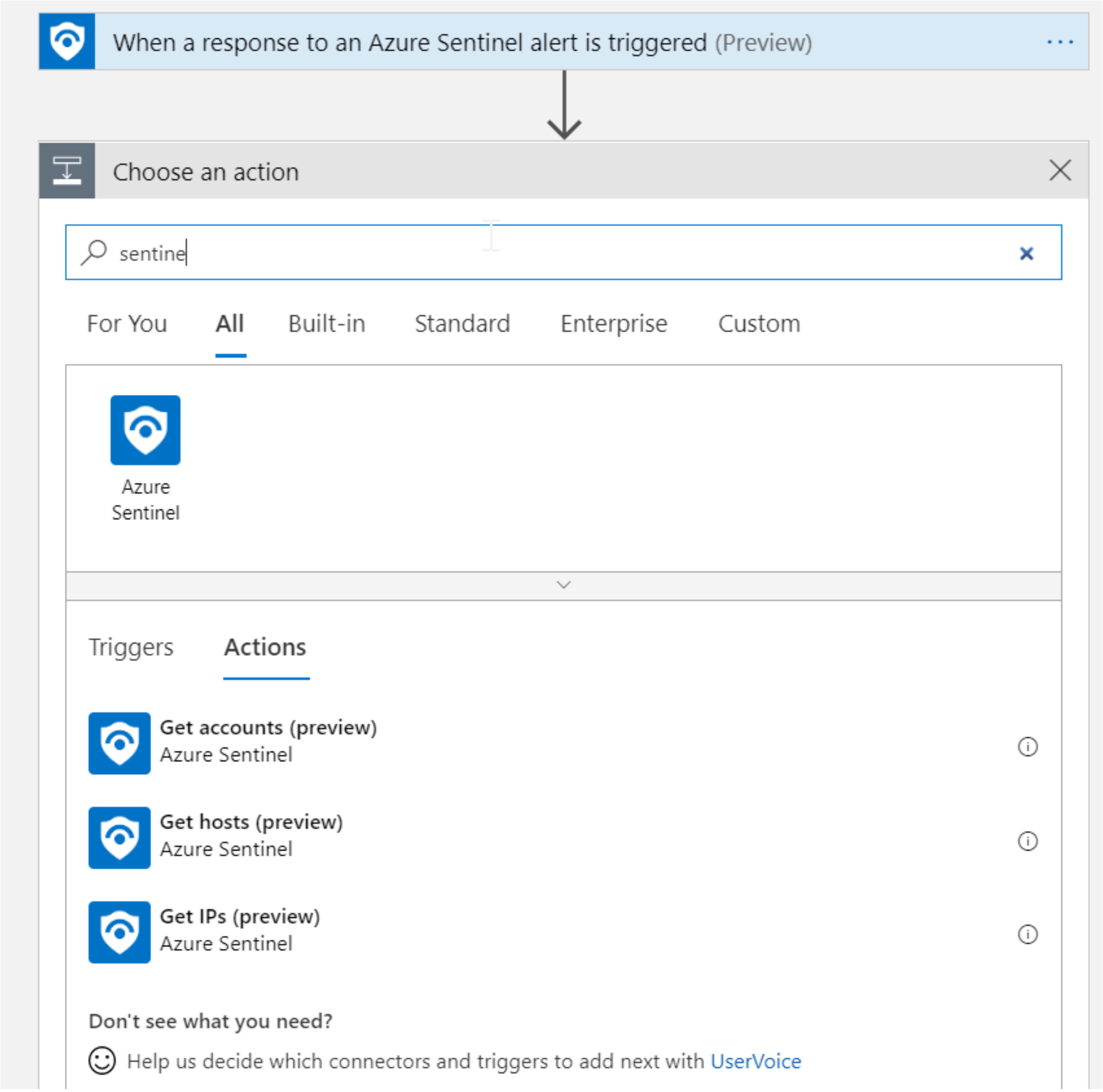
When a response to an Azure Sentinel alert is triggered (preview)
Azure Sentinel

Don't see what you need?

Help us decide which connectors and triggers to add next with UserVoice

Extract parameters

- Extract specific values from the entities field



When a response to an Azure Sentinel alert is triggered (Preview)

Choose an action

sentine

Get accounts (preview)
Azure Sentinel

Get hosts (preview)
Azure Sentinel

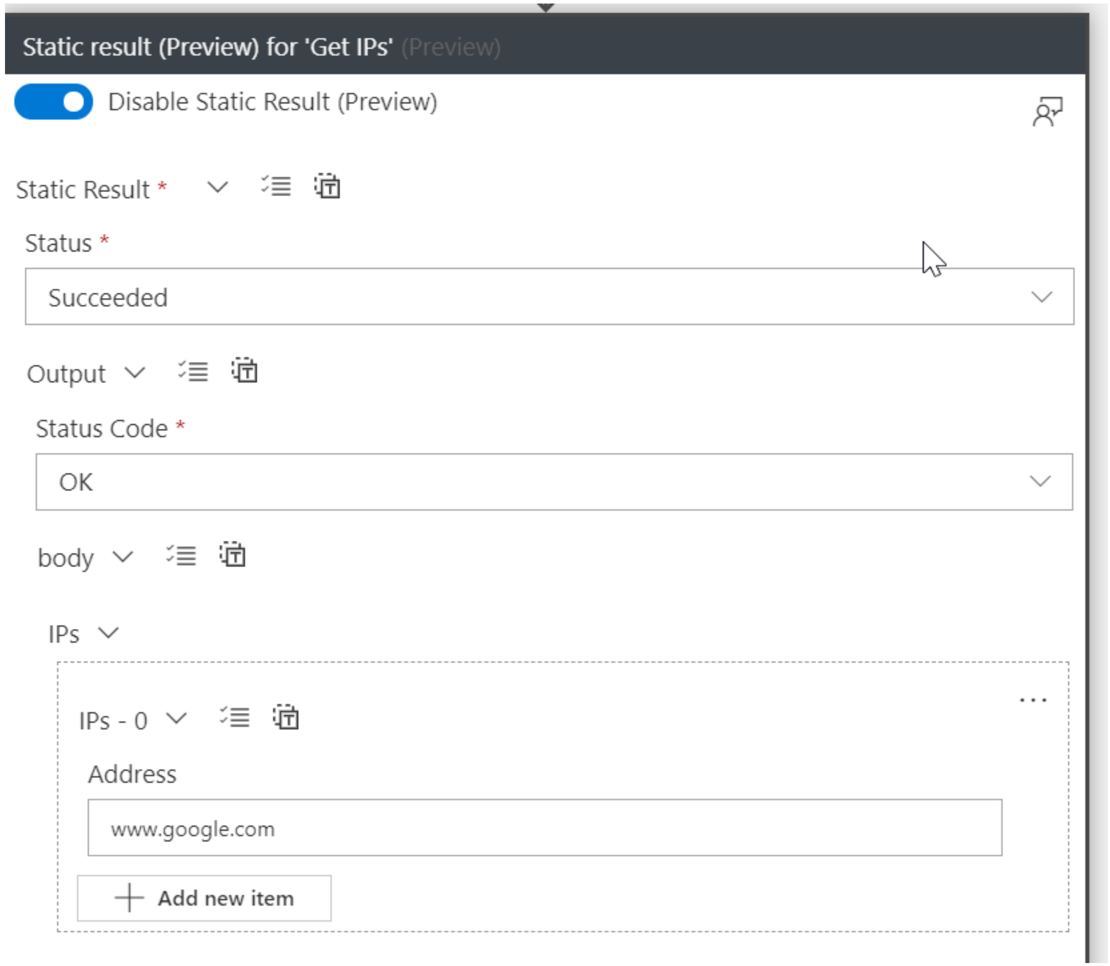
Get IPs (preview)
Azure Sentinel

Don't see what you need?

Help us decide which connectors and triggers to add next with UserVoice

Provide static values for testing

- Any action can return static values



Static result (Preview) for 'Get IPs' (Preview)

Disable Static Result (Preview)

Static Result *

Status *

Succeeded

Output

Status Code *

OK

body

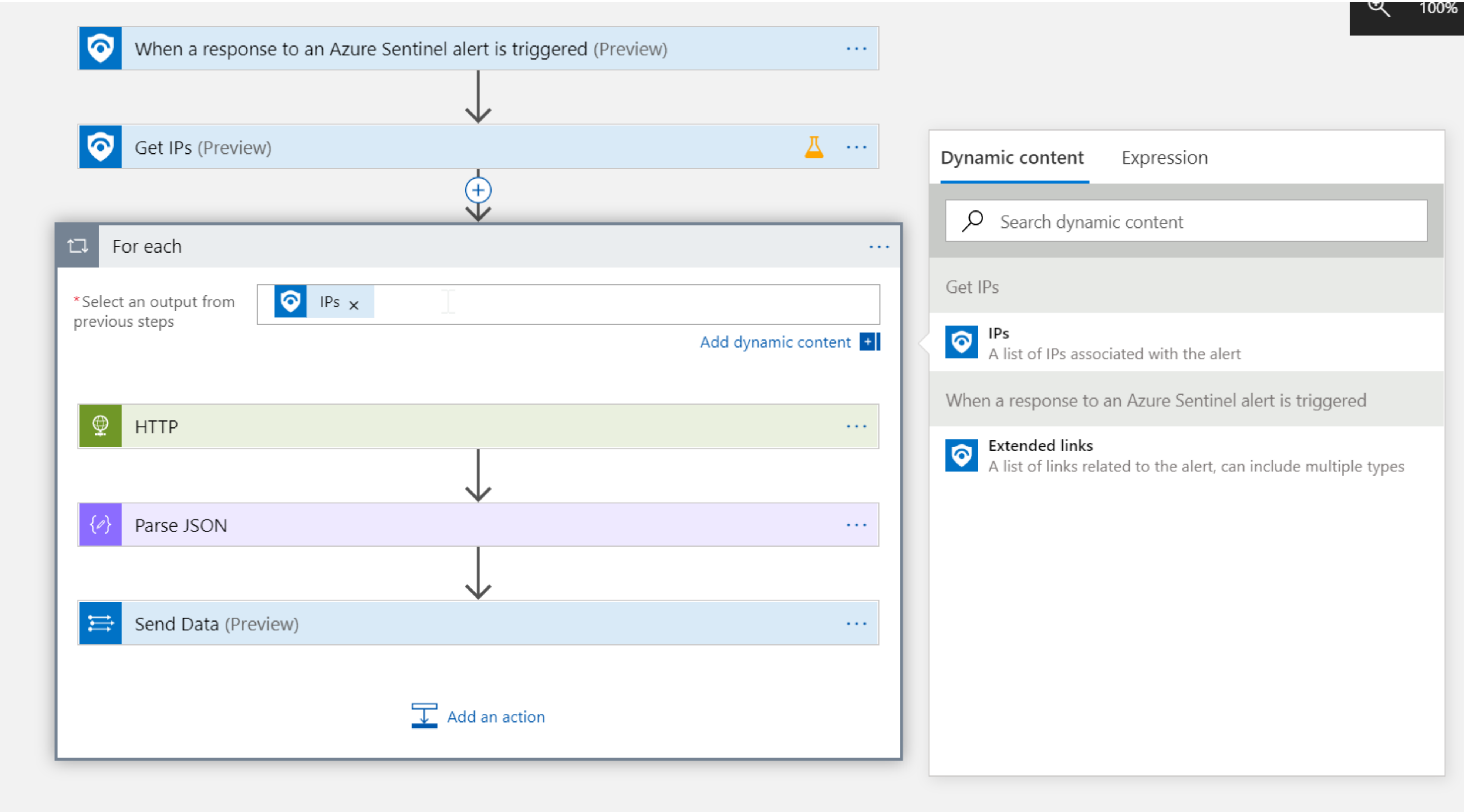
IPs

IPs - 0

Address

www.google.com

Iterate through the entity



When a response to an Azure Sentinel alert is triggered (Preview)

Get IPs (Preview)

For each

*Select an output from previous steps

IPs ×

Add dynamic content

HTTP

Parse JSON

Send Data (Preview)

Add an action

Dynamic content

Expression

Search dynamic content

Get IPs

IPs

A list of IPs associated with the alert

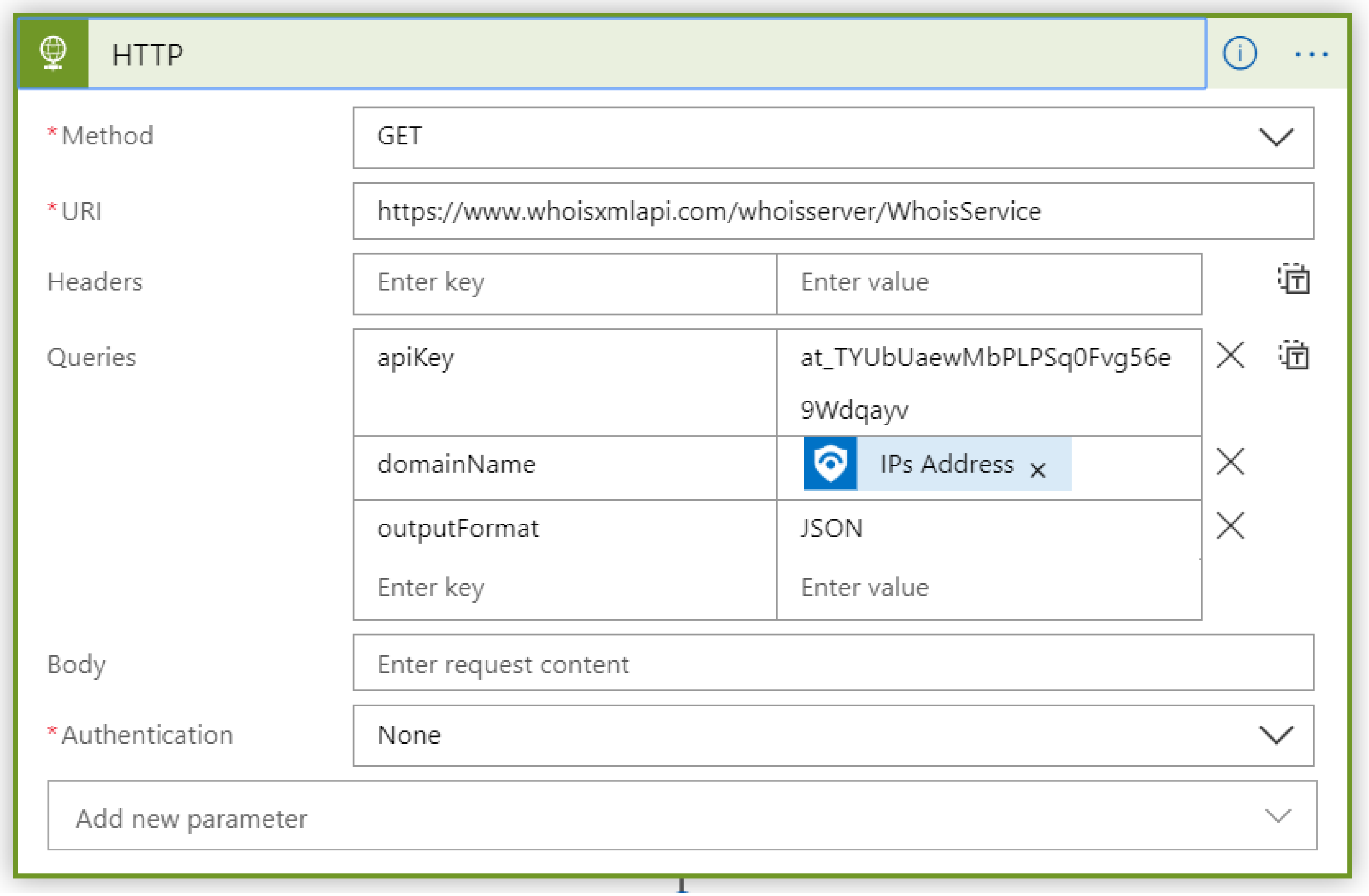
When a response to an Azure Sentinel alert is triggered

Extended links

A list of links related to the alert, can include multiple types

Call an external API

- Results returned in the “Body” parameter
- Also supports static values



HTTP

*Method: GET

*URI: https://www.whoisxmlapi.com/whoisserver/WhoisService

Headers: Enter key | Enter value

Queries:

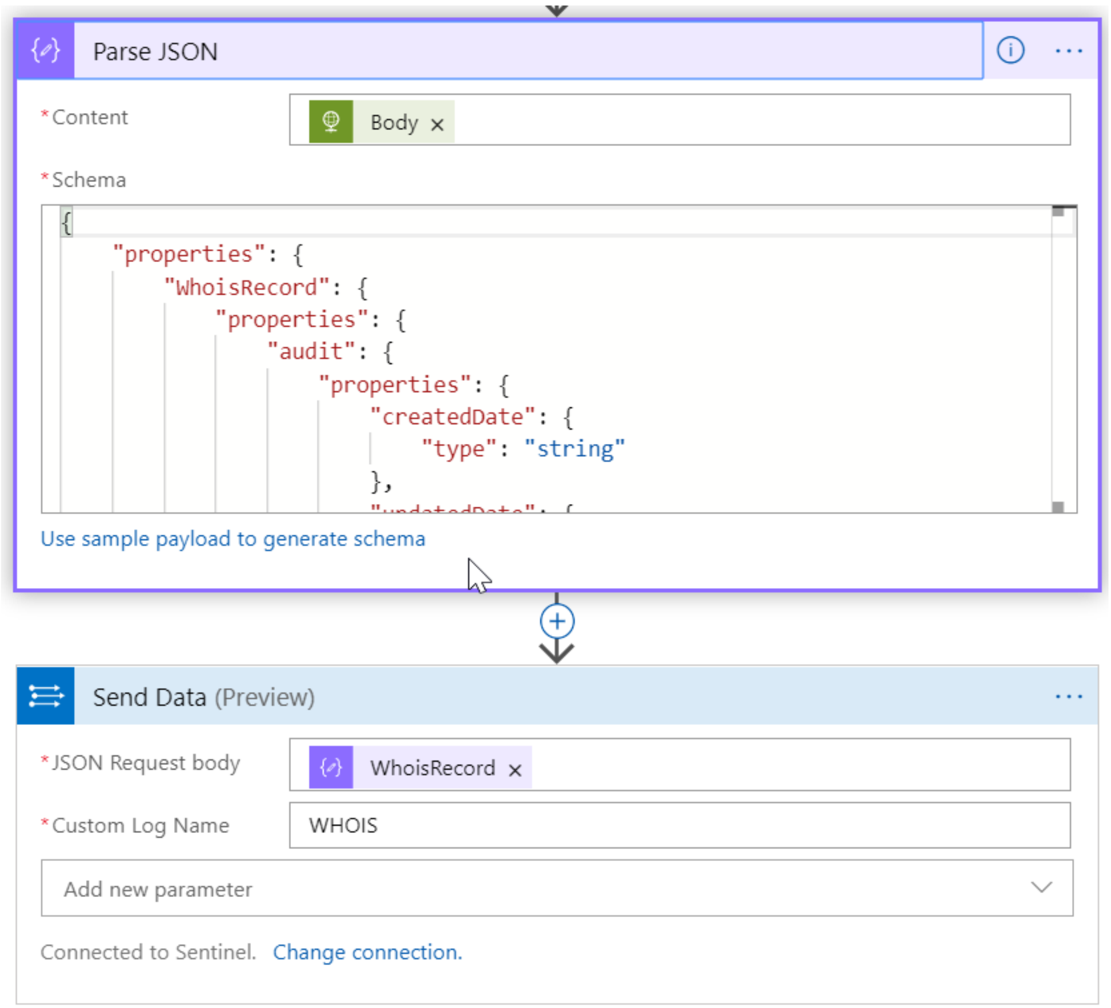
apiKey	at_TYUbUaewMbPLPSq0Fvg56e9Wdqayv
domainName	IPs Address
outputFormat	JSON
Enter key	Enter value

Body: Enter request content

*Authentication: None

Parse and write to the Workspace

- Parsing the JSON enables using each element as a playbook parameter



Parse JSON

*Content: Body ×

*Schema

```
{
    "properties": {
        "WhoisRecord": {
            "properties": {
                "audit": {
                    "properties": {
                        "createdDate": {
                            "type": "string"
                        },
                        "updatedDate": {
```

Use sample payload to generate schema

Send Data (Preview)

*JSON Request body: WhoisRecord ×

*Custom Log Name: WHOIS

Add new parameter

Connected to Sentinel. Change connection.