

O365 Integration into Snow EM - Inbound Action – Action is where the O365_Snow_InboundActionScript.js data is pasted in.

O365-ATP-Create-Event

UpdateDelete

✔ This form has annotations - click ? to toggle them - (click here to never show this again)

✕

Name

O365-ATP-Create-Event

Target table

Event [em_event]

Action type

Record Action

Application

Global

i

Active

☒

Stop processing

☐

When to run

▼

Type

New

Order

90

Conditions

Add Filter Condition

Add "OR" Clause

Required roles

From

O365 API

Q

i

Headers

▼

contains

▼

Office365Alerts@microsoft.

AND

OR

✕

Condition

Actions

▼

Field actions

-- choose field --

To

-- value --

Script

ab

ab

1

current.source = ' ';

2

current.resource = ' ';

3

current.description = email.body_text;

4

current.time_of_event = new GlideDateTime();

5

current.message_key = new GlideDateTime();

6

7

if(email.body.severity!=undefined){

8

current.event_class=email.body.severity;}

9

10

// if(email.body.description!=undefined){

11

// current.description=email.body.description;}

12

13

if(email.body.severity!=undefined){

Event Rules – (Note I am mapping Severity to Source Instance since there is an Image before the Severity Word).

<

Event Rule

O365-ATP-Default_Event_Rule

Active ☒

Save

Insert and Stay

Update

Event Rule Info

Event Filter

Transform and Compose Alert Output

Threshold

Binding

Transform and Compose Alert Output

Compose Alert fields by adding free text and by dragging variables from the right pane.
Click Event Raw values to create **new regex expressions**.

Description

Node

Type

Resource

Message Key

Severity

Metric Name

Source Instance

Source

Classification

Additional Information

☐ Manual attributes

Event Input

Expressions

Metric Name

△Test - email Notification from O365ATP to SNOWEM

Event Raw Info

Description

A high-severity alert has been triggered△Test - email N

Node

dt [REDACTED]

Type

FileActivity

Resource

O365 Security [REDACTED]

Message key

2 [REDACTED]

Severity

Metric Name

Source instance

●High

Source

O365-ATP

Resolution state

New

CI type

Classification

0

Event Field Mappings – (This is important since we are passing original values to Source Instance. We need to convert them to ServiceNOW severity and map it to Severity field.

<

≡

Event Field Mapping
O365-ATP-severity

Update

Delete

* Name

O365-ATP-severity

Active

☒

* Source

O365-ATP

* Order

100

* Mapping type

Single field

▼

* From field

event_class

* To field

severity

Event Mapping Pairs

◀◀

◀

1

to 6 of 6

▶

▶▶

⌵

	≡ Key ▲	≡ Value
	<u>High</u>	1
	<u>Low</u>	3
	<u>Medium</u>	2
	● <u>High</u>	1
	● <u>Low</u>	3
	● <u>Medium</u>	2
	Insert a new row...	

Update

Delete

Response time(ms): 1208 Network: 10 server: 728 browser: 470