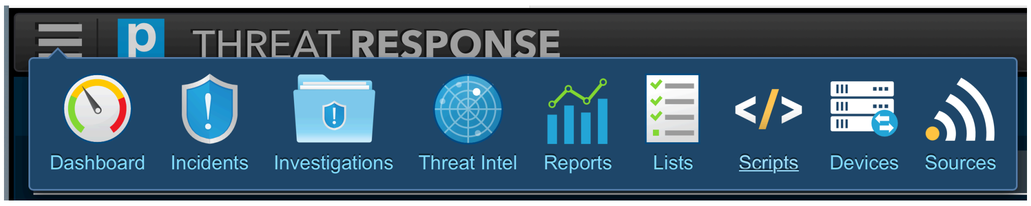
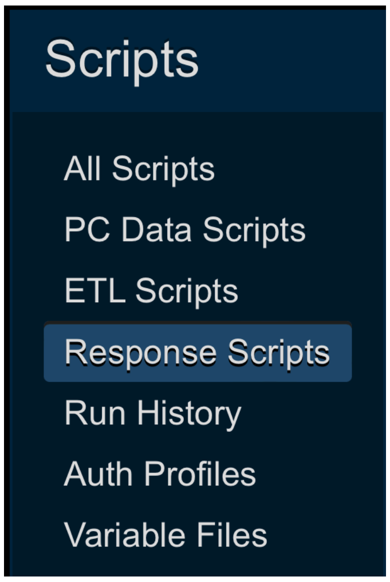
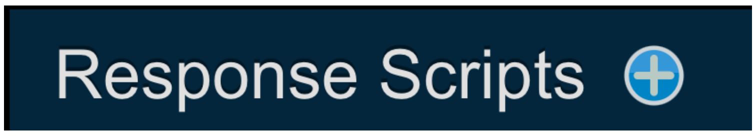
PTR-Sentinel



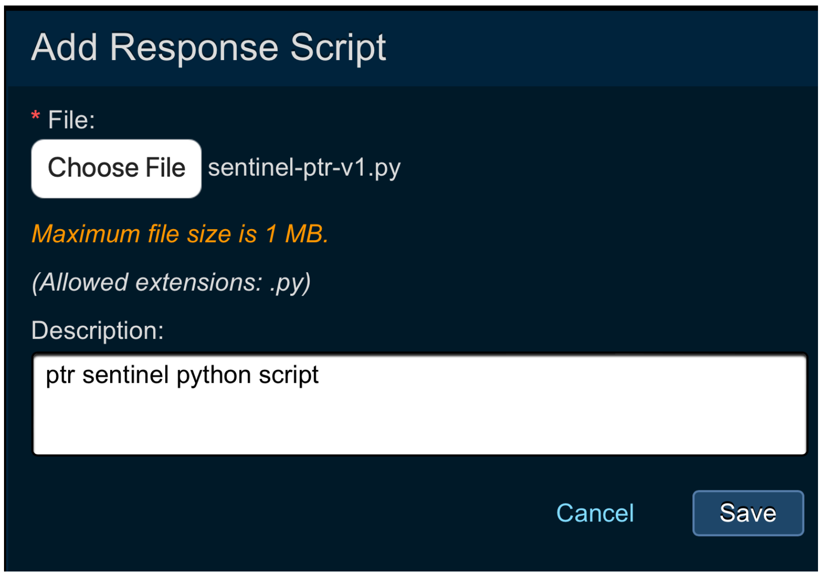
Select Scripts from the top level menu option



Select Response Scripts



Select the PLUS icon



Add Response Script

* File:

Choose File sentinel-ptr-v1.py

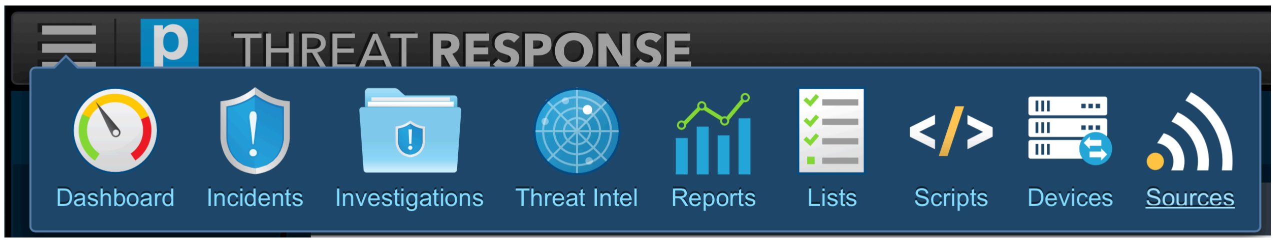
Maximum file size is 1 MB.

(Allowed extensions: .py)

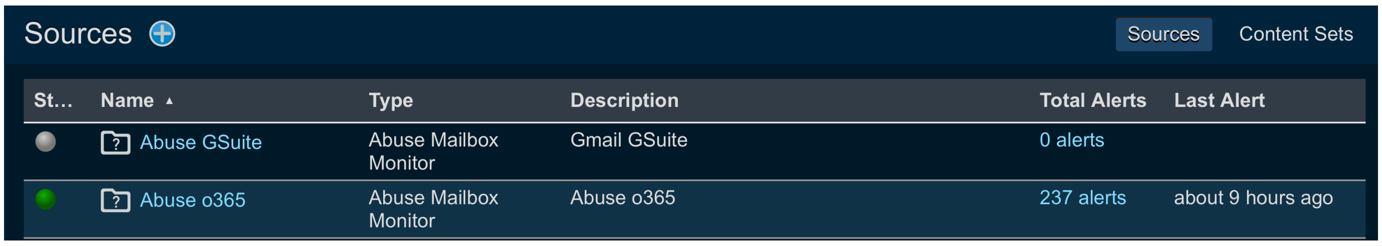
Description:

ptr sentinel python script

Choose File and browse to the desired Python

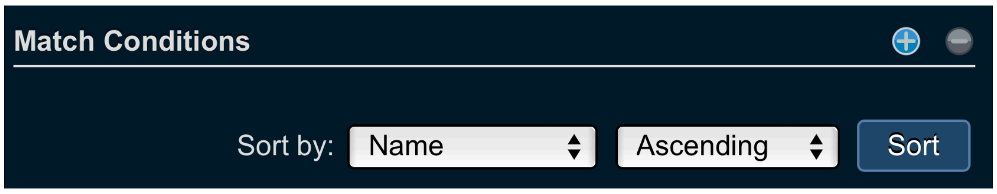


Select Sources



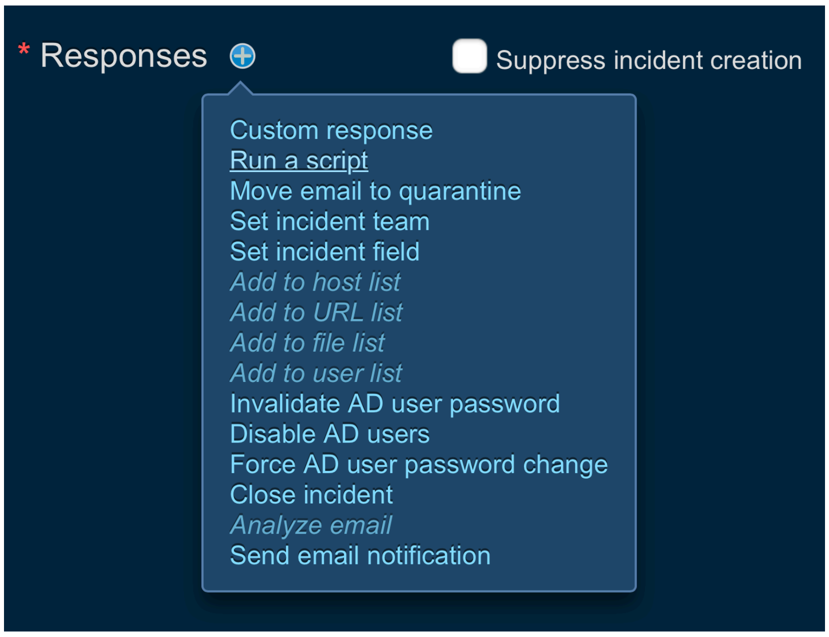
St...	Name ▲	Type	Description	Total Alerts	Last Alert
●	Abuse GSuite	Abuse Mailbox Monitor	Gmail GSuite	0 alerts	
●	Abuse o365	Abuse Mailbox Monitor	Abuse o365	237 alerts	about 9 hours ago

Choose the alert source that you want to trigger the Python script

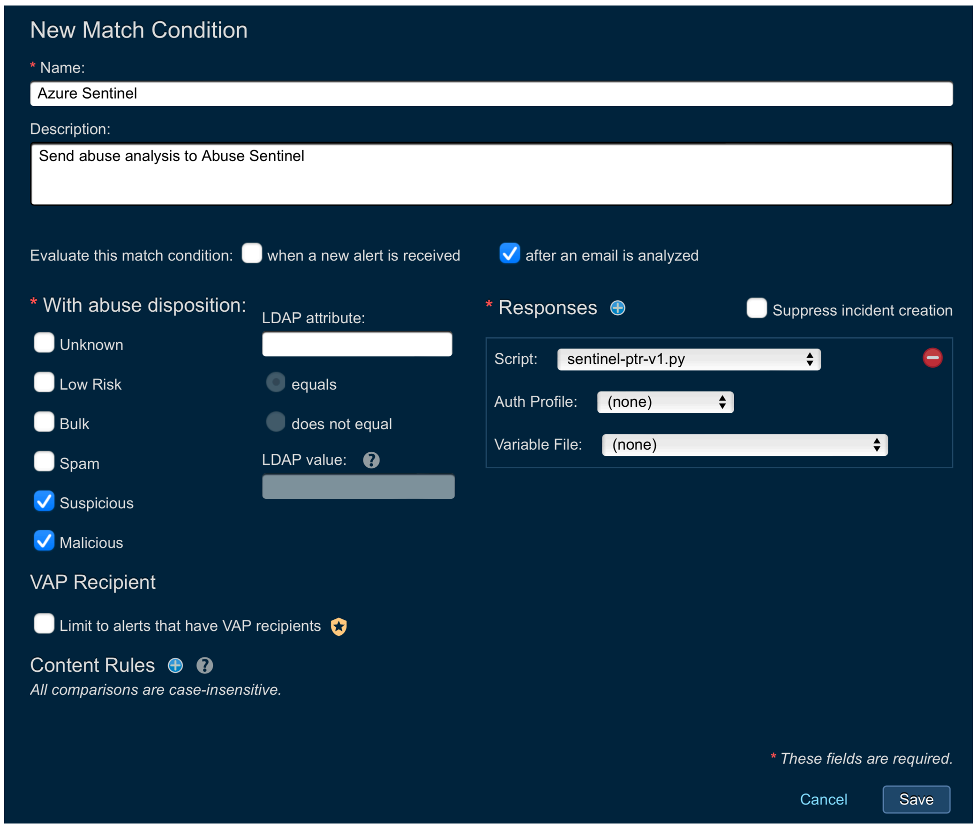


Sort by: Name Ascending

Create a new match condition from within the selected alert source



Select the Run a script response action



New Match Condition

* Name: Azure Sentinel

Description: Send abuse analysis to Abuse Sentinel

Evaluate this match condition: □ when a new alert is received ☑ after an email is analyzed

* With abuse disposition:

- □ Unknown
- □ Low Risk
- □ Bulk
- □ Spam
- ☑ Suspicious
- ☑ Malicious

LDAP attribute:

○ equals

○ does not equal

LDAP value:

* Responses □ Suppress incident creation

Script: sentinel-ptr-v1.py

Auth Profile: (none)

Variable File: (none)

VAP Recipient

□ Limit to alerts that have VAP recipients

Content Rules

All comparisons are case-insensitive.

** These fields are required.*

Select the previously uploaded Python script from the earlier steps and select save