Proofpoint Threat Response 4.5.0 – Release Notes

March 2019

Overview

Proofpoint Threat Response (PTR) and Threat Response Auto Pull (TRAP) 4.5.0 deliver several new features that advance the capabilities of the **Closed Loop Email Analysis and Response (CLEAR)** solution, enhance abuse mailbox monitoring and improve on the ability for customized responses to incidents.

TRAP Features

PhishAlarm Analyzer integration with Proofpoint threat intelligence

PTR/TRAP 4.5.0 enables enrichment and external analysis of email alerts that in turn provide multiple benefits:

1. Upgrade the capabilities of PhishAlarm Analyzer by adding Proofpoint's threat intelligence for employee-reported abuse messages.
2. Enable the submission of suspicious messages to Proofpoint.

PTR/TRAP 4.5.0 includes a new type of response action that submits reported email alerts for further analysis and re-scoring as enabled by PhishAlarm Analyzer (PAA). The capability to submit alerts for such analysis can be setup as an automated response or requested manually. PTR/TRAP updates the abuse disposition of the related incident based on the results of this analysis and maintains a history of changes to this field.

After being analyzed, these alerts can be resubmitted for an evaluation of match conditions using the updated abuse disposition so that an appropriate response action can be executed.

On upgrading from an older version to 4.5.0, the abuse mailbox source will have a pre-configured match condition that is enabled and re-submits emails to PhishAlarm Analyzer.

Disable User Accounts in Active Directory

PTR/TRAP 4.5.0 supports a new type of response that can disable one or more Microsoft Active Directory user accounts that were impacted by an alert. This can be useful in cases where an alert provides evidence that the user account may be under imminent danger and must be disabled before it can result in further damage. After the execution of this response, the Active Directory administrator would be required to re-enable the disabled user accounts.

Email Notifications for Quarantine and Undo Quarantine

PTR/TRAP 4.5.0 provides the ability to notify the recipient(s) of an email message which has been quarantined or removed from quarantine. These email notifications can be set up with plain-text templates in System Settings and can be customized depending on the match condition(s) that trigger the response. The emails can be additionally delivered to other email addresses including SMTP-supported distribution lists.

On upgrading from an older version to 4.5.0, the system will be setup with two default email templates for quarantine and undo quarantine actions.

Threat Response Features

Scripted Responses in Python

PTR/TRAP 4.5.0 supports python scripts that can be run as responses to match conditions. These response scripts can be set up with support for both Auth Profiles and Variable Files. This response framework provides a powerful, flexible way for administrators to setup orchestration workflows that can integrate with external systems that support Python API's. e.g. - helpdesk ticketing systems, third party.

General Features

Private Teams, Incidents and Investigations

Teams can be designated as *private* and assigned with *private incidents* and *private investigations*. These incidents and investigations are listed in reports and are accessible *only* to members of the assigned private teams. Even members who belong to the Admins or Script-Admins teams will not have access to these private incidents and investigations; but they can add themselves to a private team, if necessary.

Public incidents and *investigations* are listed in the reports and accessible for *any* team member.

Filter Incidents by Closed Date Range

The Incidents List report now includes the ability to filter closed incidents using a range of dates. This filter is visible only on the *Closed* tab.

TAXII & STIX 2.0 Support

PTR/TRAP 4.5.0 supports the addition of TAXII Servers that support TAXII v2.0 in addition to the older TAXI v1.x. This also includes support for STIX v2.0 wherein data is exchanged using JSON format. During the addition of a TAXII server under System Settings, the user can choose to specify the version of TAXII and optionally specify multiple media types.

Download and Upgrade Instructions

PTR/TRAP 4.5.0 requires a minimum of VMware ESXi 6.0. Please use Proofpoint CTS credentials to access downloaded images.

4.5.0 OVA File (Fresh Installs Only)
https://dl1.proofpoint.com/download/ThreatResponse/4.5.0/Proofpoint_Threat_Response_Installer-4.5.0.ova

4.5.0 IMG File (Upgrades Only)
https://dl1.proofpoint.com/download/ThreatResponse/4.5.0/Proofpoint_Threat_Response_Update-4.5.0.img

The API docs for PTR/TRAP 4.5.0 can be found at: https://ptr-docs.proofpoint.com/extensibility-guides/ptr-api/