Proofpoint Threat Response 5.2.0 – Release Notes

May 2020

Overview

Proofpoint Threat Response (PTR) and Threat Response Auto Pull (TRAP) version 5.2.0 delivers several key customer requests, including a new integration with Proofpoint Smart Search that reduces a multi-step message remediation workflow to a single click.

Moreover, version 5.2.0 includes multiple enhancements that strengthen the Proofpoint Targeted Attack Protection (TAP) integration with TRAP/PTR. Also, it accelerates system and UI performance for executing core TRAP/Threat Response workflows.

Lastly, this version provides additional "help" text for messages analyzed by Proofpoint Closed Loop Email Analysis and Response (CLEAR). This text enables messaging as well as security analysts to understand *why* a specific abuse disposition was assigned to an alert following message analysis.

New/Improved Integrations

Smart Search – "Export to TRAP"

A large number of PTR/TRAP customers also use Proofpoint Protection Server's (PPS) cloud-hosted offering, also known as Proofpoint On-Demand (PoD), in their mail environments. The execution of these products together enables you to find malicious/unwanted messages using PPS and then quarantine them using TRAP. Messages can be queried by similar *subject*, *sender address*, *URL*, *domain*, etc. and then PPS exports a CSV file of the results, TRAP, in turn, can use the results to target quarantines.

PTR/TRAP 5.2.0 adds a new integration with Proofpoint Smart Search, also known as "Proofpoint Smart Search – Export to TRAP." It allows you to use PPS Smart Search to "push" the results from a Smart Search query directly into your PTR/TRAP appliance with a **single click** by using the new **Export to TRAP** button available within the Smart Search Admin Portal interface.

This integration requires a new alert source called 'Proofpoint Smart Search - Export to TRAP' to be configured on your PTR/TRAP 5.2.0 (or above) appliance. Refer to the Export to TRAP Integration Guide for detailed instructions on how to set this up to work correctly.

Increased Lookback Period for TAP Alerts

PTR/TRAP 5.2.0 increases the lookback period for TAP alerts from **1 hour to 12 hours**. This means that in the event of a disaster or other meaningful outage, PTR/TRAP can now recover TAP alerts **up to 12 hours** in the past *on restart* and will continue to quarantine/remediate based on those alerts configured in your match conditions.

Searching for TAP Dashboard Threat URLs in PTR/TRAP

PTR/TRAP 5.2.0 introduces the capability to search for any URL threat found on the TAP Dashboard within the PTR/TRAP search interface and to return all incidents and alerts pertaining to that URL threat within PTR/TRAP.

PTR/TRAP 5.2.0 also introduces two new columns in the search results for alerts in both the basic and detailed search results view:

1. **Threat Hostname** (the subdomain and domain corresponding to the URL threat)
2. **Email Recipient** (the alert's target)

CLEAR Enhancements

"Suspiciousness" Classifier

PTR/TRAP 5.2.0 provides reasons for arriving at an abuse disposition value following a CLEAR analysis of a message. This reasoning is displayed on the **Threat Description** field in the **Incident Overview** and in a new **CLEAR analysis** section on the **Alert view**. It presents specific URLs or attachment names that were found to be malicious in each message where applicable.

Performance Enhancements

Automatic Backups Before Scheduled Purges

PTR/TRAP 5.2.0 allows administrators to schedule backups prior to executing regular purge operations. This enables the automation of regular backups of your database and thus keeps your appliance's systems "light" to ensure that the UI is fast. Backend performance benefits as well. The setting can be configured by filling in the checkbox when scheduling a new purge.

The data stored in a backup can be restored on any PTR/TRAP appliance with the same (or higher) version as needed. A successful backup operation is a prerequisite to the execution of any incident purges. This ensures that none of your data is ever lost without a copy.

Intelligent Backup Recommendations

Given the capability to configure a scheduled backup and purge operation in PTR/TRAP 5.2.0, the system also provides useful recommendations for scheduling such operations to make sure that system performance is optimal. These notifications will be displayed to both admin and non-admin PTR/TRAP users but can only be acted on by admin users since the recommendations could lead to the deletion of data. Non-admin users can acknowledge these recommendations and inform admin users to act. All notifications can be dismissed temporarily (for **7 days**).

General Enhancements

Importing Additional LDAP Object Classes

PTR/TRAP 5.2.0 allows you to import custom LDAP object classes within PTR/TRAP instead of being limited to the object class of "user" only. These can be used as attributes to configure match conditions with active directory actions following a CLEAR analysis or as data points for enrichment of alerts with target LDAP information.

Global Support for Azure AD authentication

PTR/TRAP 5.2.0 introduces the ability to configure Azure AD authentication for deployments in countries across the globe with different authentication endpoints. With this change, PTR/TRAP can now work with Azure AD endpoints across deployments globally.

Defect Fixes

Fixes Problems Causing Alert Loss With Scripted Poller Integrations (IMD/CASB)

PTR/TRAP 5.2.0 fixes memory-related issues with scripts running in PTR/TRAP versions 5.0.0-5.1.1.

Download Instructions

PTR/TRAP 5.2.0 can be deployed on VMWare or AWS. For VMWare deployments PTR/TRAP 5.2.0 requires a minimum of VMware ESXi 6.0. For AWS deployments, 'm5a.large' is the minimum recommended configuration for EC2 instances. Please use the Proofpoint CTS credentials to access the downloaded images.

- 5.2.0 OVA File (Fresh Installations and Upgrades from 3.x, 4.x) – Download OVA and SHA-256.
- 5.2.0 IMG File (Upgrades from 5.0.0) – Download IMG and SHA-256.
- 5.2.0 VHDX File (AWS AMI Installations) – Download VHDX and SHA-256.

The API documentation for PTR/TRAP 5.2.0 can be found here.

Installation Instructions

Please refer to the PTR Installation Guide or TRAP Installation Guide for instructions concerning the installation of 5.2.0. There are a few changes in the following sections in both guides.

- The virtual machine requirements include a slightly bigger HDD for the base system.
- The required ports for network communication include new entries for clustered deployments.
- The initial configuration wizard consists of a different set of steps as compared to older versions.

Upgrade Instructions: 3.x to 4.x

The upgrade process from a 3.x or a 4.x version requires a new virtual machine to be set up using the 5.2.0 OVA file. Data must be migrated from the older version of PTR/TRAP to 5.2.0. Refer to the Upgrade Guide for detailed instructions about upgrading an older version of PTR/TRAP to 5.2.0. The FAQ (Frequently Asked Questions) section contains answers to several common queries about the upgrade process.

VMWare Deployments - Upgrade Instructions From 5.0.0 and above

Upgrading from PTR/TRAP 5.0.0 and above can be completed "in place" (on the appliance) using the IMG file. Refer to the Console Guide for instructions.

Note: An issue in PTR/TRAP 5.0.0 prevents rolling back to 5.0.0 after the appliance has been upgraded and running 5.2.0. Before upgrading the appliance from 5.0.0 to 5.2.0, it is advisable to take a VM snapshot first.

AWS Deployments - Upgrade Instructions From 5.1.1

The upgrade process for AWS deployments requires a new EC2 instance to be set up using the 5.2.0 VHDX

file. Data must be migrated from the older version of PTR/TRAP to 5.2.0. Refer to the AMI Installation Guide for detailed instructions on deploying PTR/TRAP 5.2.0 on AWS.