Proofpoint Threat Response 5.3.0 – Release Notes

September 2020

Overview

PTR/TRAP 5.3.0 introduces a significantly improved approach to **Abuse Mailbox Monitoring** workflows by delivering key enhancements on many different fronts, namely the improvement of automation and the simplification of manual triaging workflows. It also brings some technology and security upgrades, and general enhancements that benefit our customers' overall security posture.

Closed Loop Email Analysis & Response (CLEAR)

Content Rules for Improving Abuse Mailbox Monitoring Automation

PTR/TRAP 5.3.0 enables security teams to add context to the CLEAR automation pipeline by defining message **content rules** in match conditions for the **Abuse Mailbox Monitor** alert source. This allows for the **automated processing** of mass internal emails and known vendor emails as well as the creation of separate workflows for executive submissions among other use cases.

Content rules are defined as criteria based on message content such as email headers, recipients, senders, URLs, attachments, or other attributes of a message. Please refer to the Content Rules Guide for detailed instructions on how to set this up correctly.

Download Original Message for Manual Investigation/Sandbox Submission

PTR/TRAP 5.3.0 allows security teams to download the original message corresponding to an abuse mailbox submission from the PTR/TRAP UI. This can be helpful in cases where an advanced analysis of a submitted message is required, such as visual inspection or sandboxing.

Email Notifications for CLEAR Incidents Requiring Manual Review

The current release makes it possible for email notifications to be configured to *trigger* based on a team or an incident field update for incidents. Such communication can be used to notify the team whenever an incident receives an 'unknown' or 'suspicious' abuse disposition, thus implying that it requires **manual review**.

Detailed information on the topic of setting up notifications for 'unknown' and 'suspicious' incidents can be obtained here.

Subject and Sender Values on Incident List for Abuse Incidents

This release adds the **Subject** and **Sender** values for the latest alert to the **incident list** view for **abuse mailbox monitor incidents**, thus allowing incidents with known/recognized emails to be triaged as well as taking bulk action directly from the **incident list**.

False Negative Reporting for CLEAR Submissions

CLEAR analysis of a message can result in an ”unknown” abuse disposition, in which case Proofpoint Threat Intelligence defers the final decision on the message to the customer's security team. If an analysis, carried out by the security team, reveals a threat in the message, PTR/TRAP 5.3.0 gives a customer the opportunity to report it back to Proofpoint. This allows Proofpoint Threat Research to review such threats and ensure a more appropriate disposition in the future.

For customers who use the Proofpoint Protection Server (PPS) and Targeted Attack Protection (TAP) as their email gateway solution, this process also allows messages, confirmed as malicious/spam by Proofpoint Threat Researchers, to be blocked *pre-delivery*.

Note: Customers must exercise caution and ensure that messages without actual threats are not reported as False Negatives to Proofpoint. Any attempts to do so would be considered detrimental to Proofpoint's Threat Intelligence and may necessitate Proofpoint to disable this feature going forward.

Reporting the Value of Automation From CLEAR

This release presents a new ”abuse dispositions” report to measure the direct automation value received from CLEAR. Essentially, the report sorts any abuse incidents into categories based on the abuse disposition. (There are six abuse dispositions.) Incidents assigned any one of the following abuse dispositions, namely “Malicious,” “Spam,” “Low Risk,” or “Bulk,” are fully automated by TRAP and the sum of the counts (under these *buckets)* represents the automation value received from CLEAR.

Predesigned Email Templates for Responding to End Users

Lastly, this release introduces six new email templates to be used in conjunction with the six abuse dispositions for the purpose of communicating deployment best practices identified and recommended by Proofpoint. They are located under the *Email Templates* section (under *Email Notifications*) on the *System Settings* screen. Note that the templates each have a “V2” tag alongside their names for easy identification.

General Improvements

Dashboard Loading Enhancements

The PTR/TRAP Dashboard is the landing page of choice for a lot of security teams using PTR/TRAP. PTR/TRAP 5.3.0 substantially improves the loading performance of the dashboard, by, for example, reducing the time range of data loaded onto the view by default. The dashboard now loads only 7 days of data instead of 90 days. Note that 90 days of data can be obtained by using the drop-down menu on the top right-hand side of the dashboard.

Additionally, the dashboard now supports a “manual” refresh mode as well as the pre-existing “auto” refresh behavior. The “manual” refresh mode will be the default selection as most users do not require the screen to be refreshed automatically (at regular [short] intervals). Customers who use the dashboard as a display for monitoring activity can choose to change the refresh mode to “auto” by using the settings on the top right-hand side of the dashboard.

Matched Conditions, Alerts, and Matched Alert Counts

PTR/TRAP 5.3.0 introduces a new subsection under ***Alerts*** called ***Matched Conditions***. The subsection has been designed to capture all the match conditions that an alert has triggered, including the timestamps. This makes it easy to track an alert and any match conditions associated with it.

Similarly, match conditions under ***Alert Sources*** now display a count for the number of alerts matched. Thus, we can understand match conditions that have proved effective in providing automation value.

This feature is very useful for identifying content rule match conditions that are effective in providing automation value with respect to abuse mailbox monitoring.

Visibility of Licensing Information

PTR/TRAP 5.3.0 provides visibility of the expiry date of valid licenses on the licensing page to ensure that licenses are renewed before they expire.

Use of Appropriate Terminology

PTR/TRAP 5.3.0 introduces changes to its terminology base to reaffirm Proofpoint's strong support for social equality. The following expressions are being changed *permanently*:

1. Quarantine Whitelist (under the *System Settings* section) -> Quarantine Skiplist (under the *System Settings* section)
2. Whitelist (under the *Lists* section) -> Allowlist (under the *Lists* section)

Technology/Security Upgrades and Key Defect Fixes

Platform Operating System Update to CentOS 7.8

PTR/TRAP 5.3.0 introduces an update to the underlying platform operating system (OS) on which PTR/TRAP runs. Essentially, the platform OS has been upgraded to CentOS version 7.8. This update better overall security and reliability of PTR/TRAP.

Progress Indicator for Master Secret Upload

PTR/TRAP 5.3.0 introduces a UI dialog describing the status of a **Master Secret** upload to the PTR/TRAP management console. This UI dialog ensures that a user is notified when a restart of system services is in progress. Ultimately, this prevents conflict when old backup files are being uploaded.

Team Sync Doesn't Update LDAP Group Changes in TRAP

PTR/TRAP 5.3.0 resolves the issue that prevents LDAP group changes from being synced to teams in TRAP.

High Availability and LDAP Conflicts

PTR/TRAP 5.3.0 addresses the issue that prevents the configuration of **High Availability** when **LDAP sync** is enabled on the product.

Download Instructions

PTR/TRAP 5.3.0 requires a minimum of VMware ESXi 6.0. Please use the Proofpoint CTS credentials to access the downloaded images.

- 5.3.0 OVA File (Fresh Installations and Upgrades From 3.x, 4.x) – Download OVA and SHA-256.
- 5.3.0 IMG File (Upgrades From 5.x) – Download IMG and SHA-256.
- 5.3.0 VHDX File (AWS AMI Installations) – Download VHDX and SHA-256.

The API documentation for PTR/TRAP 5.3.0 can be found here.

Installation Instructions

Please refer to the PTR Installation Guide or TRAP Installation Guide for instructions concerning the installation of 5.3.0. 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.

Please refer to the PTR AWS Installation Guide for instructions concerning the installation of 5.3.0 on AWS.

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 5.3.0 OVA file. Data must be migrated from the older version of PTR/TRAP to 5.3.0. Refer to the Upgrade Guide for detailed instructions about upgrading an older version of PTR/TRAP to 5.3.0. The FAQ (Frequently Asked Questions) section contains answers to several common queries about the upgrade process.

Upgrade Instructions From 5.x

Upgrading from PTR/TRAP 5.x to 5.3.0 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 5.3.0. Before upgrading the appliance from 5.0.0 to 5.3.0, it is advisable to take a VM snapshot first.

AWS Deployments – Upgrade Instructions

The upgrade process for AWS deployments requires a new EC2 instance to be set up using the 5.3.0 VHDX file. Data must be migrated from the older version of PTR/TRAP to 5.3.0. Refer to the AMI Installation Guide for detailed instructions on deploying PTR/TRAP 5.3.0 on AWS.