Proofpoint Threat Response 5.5.0 – Release Notes

April 2021

Overview

PTR/TRAP 5.5.0 introduces a new integration with **Proofpoint Smart Search** (Proofpoint-hosted Admin Portal Interface only) to simplify threat hunting and responding to incidents based on messages reported to the Abuse Mailbox. Incident responders can find messages based on similar tells with a single click in PTR/TRAP.

PTR/TRAP 5.5.0 also introduces key improvements to the management of match conditions for CLEAR (Abuse Mailbox). These improvements include new features such as *creating* content sets, *duplicating* a match condition, and *sorting* and *auditability* of match condition "matches." Furthermore, support for content rules has now been extended to the TAP alert source.

And lastly, this release improves the platform with the ability to automatically transfer new backups to remote locations, email notifications for outage monitoring and the ability to purge alerts not belonging to incidents.

CLEAR and TRAP Enhancements

BEC / EAC Email Threat Searches and Incident Response

In the context of searching for Business Email Compromise (BEC) and Email Account Compromise (EAC) threats, PTR/TRAP customers that use Proofpoint Protection Server (PoD only) can benefit from a new integration between PTR/TRAP and the PPS Admin Portal. Incident responders can pivot from PTR/TRAP into Smart Search to find similar messages based on a given sender, recipient, or return-path with a single click.

A new **View Similar Messages** link on the **Alerts tab** for incidents cross launches users into the new Admin Portal interface for Proofpoint Smart Search and prepopulates the search box with the appropriate search query and a time range (last 7 days).

Any messages deemed worthy of quarantine can then be exported to TRAP with a few clicks as part of incident response. This speeds up the process of threat searching and incident response for messages in a BEC/EAC context where sender, recipient and return-path are important attributes for discovering threat lures.

Note: The 'View Similar Messages' links can be toggled on or off under 'System Settings > Contextual Data Sources > Smart Search Similar Messages'.

Content Rules for TAP Alerts

PTR/TRAP 5.5.0 adds content rule support for match conditions and alert filters on the Proofpoint TAP alert source. Customers who need to separate TRAP operations across email domains, business units, or geographies can now filter out alerts into separate TRAP instances using content rules in alert filters based on the email recipient's domain. The list of supported fields for writing content rules in the TAP source includes

1. Recipient
2. Sender
3. Message ID
4. Threat URL
5. Attachment Hash

6. Attachment Name
7. Subject (*Only available for some TAP alert types)*

Content Sets for Related Attribute Values in Content Rules

PTR/TRAP 5.5.0 enables the creation of centralized sets of related content attributes, for use in content rules, across multiple match conditions on the Proofpoint TAP or Abuse Mailbox Monitor alert sources. For instance, content sets may be created with a list of common internal sender email addresses, known vendor domains, executive email lists, or common email subjects and then referenced in multiple content rules to define desired workflows for any of these scenarios.

A key advantage of using content sets is that updates such as adding new entries or removing existing ones only need to be made to the content set. These updates will propagate to individual content rules automatically.

Match Condition Management – UX Improvements

PTR/TRAP 5.5.0 highlights an improved user experience with respect to the management of match conditions.

Better Look and Feel

The alert source side panel has been widened with increased spacing between match conditions, for clarity, readability, and ease of navigation.

Sorting Options

Match conditions can be sorted by

- Name of Match Condition
- Initial Timestamp
- Last Updated Timestamp
- Enabled Status

Note that the list of match conditions is arranged alphabetically by default.

Enabled/Disabled Indicators

The listing also includes a new green/gray indicator. It denotes the enabled/disabled state of a match condition. The colored icons serve as a useful way to examine any disabled match conditions.

Duplicating a Match Condition

Match conditions, including criteria, content rules, and responses, can be duplicated by using the new **Duplicate** icon button beside each match condition.

Auditing Historical Matches

The number of matched alerts is now clickable and shows the alerts “matched” by this match condition over time.

Note that alerts that have been purged from the system but had previously “matched” will be included in the count; they will not, however, appear in the pop-up list of matches as they no longer exist in the system.

Platform Improvements

Connection Failure Notification

This release introduces a new type of email notification to the product called **Connection Failure**. Once configured, this notification is designed to alert a recipient to a connectivity outage between PTR/TRAP and any critical external services.

PTR/TRAP 5.5.0 supports monitoring for the following services:

1. Exchange and Microsoft 365 mail servers
2. G Suite (Google Workspace) mail servers
3. LDAP servers
4. Proofpoint TAP alert source
5. Abuse Mailbox Monitor alert source(s)
6. Proofpoint Smart Search – Export to TRAP alert source
7. Scripted Poller alert source(s)

A connection failure notification is triggered after 15 consecutive minutes of failure to connect to a specified service. Thereafter, notifications are generated at one-minute intervals throughout the duration of the outage.

Note that in the event of an expected or known outage, this notification can be disabled and reenabled from the **Email Notifications** section under **System Settings**.

Purging Alerts Without Incidents

Manual and Scheduled Incident Purges under **System Settings** now provide an additional option to include alerts that are not associated with incidents. By checking this option, orphaned or suppressed alerts lying latent in the system will be cleared as a part of the purge operation.

Purging such alerts should speed up alert processing and reduce processing errors or timeouts since these latent, orphaned alerts tend to slow down alert processing and linking significantly.

Note that the deletion of orphaned alerts or incidents is treated as an add-on operation to regular incident purges. Checking this option will not stop alerts/incidents belonging to regular closed incidents from being purged.

SCP Server for System Backups

On the **Appliance Management** Console on port 8080, PTR/TRAP 5.5.0 provides the option to configure a Secure Copy Protocol (SCP) server as a remote location for backing up a system configuration and incident data. The SCP server must be configured with any requisite access credentials.

Copying a Backup to a configured Remote Location Automatically – AWS S3 Bucket / SCP Server

On the **Appliance Management Console** on port 8080, PTR/TRAP 5.5.0 provides the option to copy a system backup into either or both of the following automatically:

- A configured AWS S3 bucket

- A configured SCP server

Once the automatic copy is enabled, it works in conjunction with the scheduled purge and backup capability within the product to create new backups and transfer them over to the specified remote location automatically.

Backups Status Page

On the **Appliance Management** Console on port 8080, PTR/TRAP 5.5.0 adds a new **Backups Status** page. It provides details on the success or failure status of previous backup operations as well as the status of the associated transfer to an SCP location or an S3 bucket.

Bug Fixes

Occasional Failures to Attach Original Email to Abuse Feedback Template

PTR/TRAP 5.5.0 fixes an issue that caused an occasional failure to attach an original reported message back with the abuse feedback email template to the end user.

Occasional Failures to Deliver Email Notifications Based on Team Assigned Match Conditions

PTR/TRAP 5.5.0 fixes an issue that caused an occasional failure to generate an email notification when a team is assigned to an incident, as part of a match condition.

Removed Alert Linking Based on Schema URLs in the Message

For end-user reported abuse messages, PTR/TRAP 5.5.0 improves alert-linking behavior based on the combination of sender address and URL. Messages are no longer linked on Web schema URLs from w3.org or Microsoft Schema URLs from schemas.microsoft.com.

Security Hardening and Vulnerability Fixes

Further to the CentOS 7.9 version upgrade in PTR/TRAP 5.4.2, PTR/TRAP 5.5.0 adds even more security enhancements with package upgrades for several common system libraries.

Threat Response/TRAP API Enhancements

API to Fetch Investigation Details

PTR/TRAP 5.5.0 provides a new API to fetch the details of an investigation being conducted across multiple incidents. This API requires the specification of the investigation ID and returns all available information about that investigation, including any incident IDs.

Optionally, the API response can include full incident data for each incident linked to the investigation. Additionally, the API response can include full alert data for each of these incidents.

Download Instructions

PTR/TRAP 5.5.0 requires a minimum of VMware ESXi 6.0. Please use the Proofpoint CTS credentials to access the downloaded images.

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

The API documentation for PTR/TRAP 5.5.0 can be found here.

Installation Instructions

Please refer to the PTR Installation Guide or TRAP Installation Guide for instructions concerning the installation of 5.5.0. 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 5.5.0 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 5.5.0 OVA file. Data must be migrated from the older version of PTR/TRAP to 5.5.0. Refer to the Upgrade Guide for detailed instructions about upgrading an older version of PTR/TRAP to 5.5.0. 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 5.5.0 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 5.5.0. Before upgrading the appliance from 5.0.0 to 5.5.0, 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 5.5.0 VHDX file. Data must be migrated from the older version of PTR/TRAP to 5.5.0. Refer to the AMI Installation Guide for detailed instructions for deploying PTR/TRAP 5.5.0 on AWS.