Proofpoint Threat Response v4.2.0 Release Notes

September 2018

Release Summary

Threat Response 4.2.0 is a minor release that adds enhancements to the Abuse Mailbox Monitoring functionality. It adds support for Modern Auth for Office 365 and extends the email notifications feature.

Please refer to the following for more detailed information:

1. Platform Features & Enhancements
2. Threat Response Auto-Pull (TRAP) Enhancements
3. Download Instructions

Recommendations

As with any software upgrade it is recommended that a full system backup be created prior to starting the upgrade. Backups can be initiated in the Appliance Management Console. This backup, as well as an export of the Master Secret, should be downloaded and stored in a secure location.
If any issues are encountered during or after upgrading, please open a support ticket at: https://proofpointcommunities.force.com

TRAP - Abuse Mailbox Enhancements

End-user Feedback

- Email notifications can be configured to be sent to the reporter (for an Abuse Mailbox incident) when a Threat Response administrator has determined the reported email is malicious and has quarantined the email. This is a way to encourage and positively acknowledge the reporter's situational awareness in reporting a phishing email and improving the security posture of the organization.

Improved incident views for better prioritization of Abuse incidents

- The Incident List Filter has added controls for filtering incidents based on their enrichments to known threats:
    - Host Reputation source:
        - Emerging Threats
        - Proofpoint (URIBL)
        - Webroot
    - Campaign Name
    - Campaign ID

TRAP actions and Abuse Mailbox incident correlation

- A new option to "Close email-related incidents" has been added to the "Move email to quarantine" response action. If enabled, a successful quarantine of an email from an alert will result in any other alerts referencing the same recipient/message ID pairing will be closed automatically. This is useful to help close user-reported incidents from the Abuse Mailbox where Threat Response has already quarantined the message based on a TAP alert.

Enhanced severity settings for Abuse incidents where the source of the reported email is Wombat PhishAlarm Analyzer

- Incidents will be assigned the following severities in Threat Response based on PhishAlarm Analyzer's confidence in the email being a Phish:
    - Unlikely: Informational
    - Suspicious: Minor
    - Likely: Major

Support for Match Conditions to automate response actions

- The following response types are available:
    - Move email to quarantine
        - Quarantine related emails
        - Close incident after successful quarantine
    - Custom Response
    - Set Incident Team
    - Set incident field

Platform Features & Enhancements

Modern Auth for Office 365

- Customers using Office 365 for email quarantine now have the option of specifying Azure AD (“Modern Auth”) for authentication for the API calls into O365 and Exchange

Email Notifications for Stale Incidents

- A new email notification type has been added to allow for automated notifications when an incident hasn’t been updated in a configurable period of time

Incident Classification Filter for Email Notifications

- Customers can now define email notifications that include a filter for Incident Classification. Any classifications defined in Custom Fields can be used in the notification definition

Ability to Configure Email Notifications for Certain Teams Only

- Customers now can exclude the recipients for whom they don't want to trigger notifications using a newly provided "Exclude recipients" field

Download instructions

NOTE: Starting in Threat Response v3.2.0, the minimum specification of the virtual appliance has been updated. Please review the Virtual Machine requirements section for updated minimum specification.

Use Proofpoint CTS credentials to access download images:

Threat Response 4.2.0 – OVA File (Fresh Installs only):

https://dl1.proofpoint.com/download/ThreatResponse/4.2.0/Proofpoint_Threat_Response_Installer-4.2.0.ova

Threat Response 4.1.0 – IMG File (Upgrades only):

https://dl1.proofpoint.com/download/ThreatResponse/4.2.0/Proofpoint_Threat_Response_Update-4.2.0.img