Proofpoint Threat Response v3.4.0
Release Notes

November 2017

Release Summary:

Threat Response 3.4.0 is a significant release that provides additional features and capabilities as well as continues streamlining the platforms performance and efficiency. Please refer to the following for more detailed information:

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://support.proofpoint.com/

Investigation Enhancements

Investigations are groups of Incidents that share something in common and have a common set of investigation workflow activities that need to be performed. This release includes multiple improvements to streamline the complete Investigation lifecycle.

- **New Bulk Action for Investigation Linking**:

  There is a new Bulk Action called “Link Investigation” that can be used anywhere Bulk Actions are available to add the selected Incidents to an Investigation.

- **Bulk Actions are now Available for Search Results**:

  Users can select some, or all, of the Incidents that have been included in the search results and perform any available Bulk Action to the selected Incidents.

- **Custom Fields for Investigations:**

  Any Custom Fields that have been defined will now show up in both Incidents and Investigations. If a Custom Field is changed at the Investigation level users will have the option to have that change cascaded to all linked Incidents. Closing an Investigation will also require that any mandatory Custom Fields be set prior to closing.

- **Close Investigation & Linked Incidents**:

  There is now an option to close all linked Incidents when an Investigation is closed. If any of the linked Incidents have mandatory fields that have not been set the user will get a message that the Investigation can’t be closed until the mandatory fields are set. Closing comments will be included in both the Investigation and all linked Incidents (if the user chose to close linked Incidents).

- **Aggregate Incident Activity History in Investigation**:

  When viewing an Investigation there is now an option to see the Activity History including Comments and Attachments from all linked Incidents.

Incident Management Workflow Improvements

The following improvements to Incident Management workflows have been introduced:

- **TAP Dashboard Link for TAP Alerts:**

  For Proofpoint TAP Alerts the Incident Summary and Alert Details pages now display a link that will take the user directly to the TAP Dashboard page for that threat.

- **SmartSearch Match Conditions:**

  The SmartSearch Alert Source no longer requires including an asterisk “*” in the category section of a Match Condition.

- **Support for Custom Fields in Splunk and JSON Alert Sources:**

  Alerts received from Splunk 2.0 or JSON alert sources that include Custom Fields will set the Incident Custom Fields to the value provided in the Alert, but only if the Custom Field does not currently have a value set. If there is a value already set in the Incident the value provided in the Alert will be ignored.

Threat Response Auto Pull (TRAP) Enhancements

The following improvements have been made to the Threat Response Auto Pull (TRAP) capabilities:

- **Support for Email Quarantining in Google G-Suite:**

  Threat Response Auto Pull (TRAP) now supports quarantining messages that were delivered to a G-Suite mailbox. The following capabilities are available:

  - **Quarantine Original Recipient:**

    Using either Match Conditions or through a manual user action, the original email recipient email can be quarantined.

  - **Undo Quarantine Action:**

    For any messages that were quarantined in a G-Suite mailbox the 'Undo Quarantine' action is available in the Incident Activities screen. This will result in the message being returned to the original recipient's mailbox.

  - **Status Flag:**

    The Read/Unread status flag is used to indicate if the message was read or not

- **Quarantine Action Already Taken:**

  If an automated quarantine attempt has already taken place for a message ID and recipient pair no further automated quarantine action will be attempted after the first quarantine attempt.

- **Email Notifications:**

  An email notification can be configured to be sent when an email quarantine action has been completed. This notification will include details on the action such as start and end times, incident number, message recipient and whether the quarantine action succeeded or failed.

- **Incident API Includes Quarantine Actions:**

  The Incident API responses now include details on email quarantine actions. Information such as start and end times, alert source, messageID, message recipient and whether the quarantine action succeeded or failed.

- **Auto Close:**

  Match Conditions can now be configured to automatically close an Incident if all quarantine attempts were successful.

- **Concurrent Attempts Settings:**

  There is a new configuration section called “Quarantine Settings”. On this page admins can configure the maximum number of concurrent quarantine actions to perform. The default value is “20”.

- **Email Quarantine Report:**

  The Email Quarantine Report will now include the reason for a failed quarantine attempt. This information is shown when clicking on the blue ‘Failed’ status under Quarantine Status.

Additional Enhancements and Improvements

The following improvements are included in this release.

- **Time Zones:**

  Users can now configure their preferred time zone in their user profile settings. Changing this value will convert all displayed timestamps to the specified time zone.

- **Device and Alert Source Configuration Control:**

  Only users that are members of the Admin team can perform Create, Update and Delete actions for Alert Sources and Devices configurations.

- **Support for Negation in Match Conditions for LDAP Attributes:**

  Match Conditions can now be configured with ‘does not equal’ for LDAP attribute matching. In this case the Match Condition will trigger when the user identified in the Alert does not belong to the identified LDAP group.

- **Severity Labels:**

  Administrators can configure an alternate Severity label to be displayed throughout the UI and API responses.

- **IoC Process Collection:**

  The IoC collector now shows the SHA256 hash for the Process that has been identified.

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 3.4.0 – OVA File (Fresh Installs only):

Proofpoint_Threat_Response_Installer-3.4.0.ova

Threat Response 3.4.0 – IMG File (Upgrades only):

Proofpoint_Threat_Reponse_Update-3.4.0.img