Proofpoint Threat Response v3.5.0
Release Notes

March 2018

Release Summary:

Threat Response 3.5.0 provides additional features and capabilities as well as continues streamlining the platform's 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/

- **Support for Carbon Black EDR as IOC collector**

  This release adds support for Carbon Black Endpoint Detection & Response (EDR) Platform for IOC (Indicator Of Compromise) collection as an alternative to the native Proofpoint Threat Response PC Data Collection agent.

  - **Supported Carbon Black Versions**:

    Threat Response supports Carbon Black server versions 5.x and 6.x for peforming IOC collection.

  - **IOC Items collected**

    Using the Carbon Black server APIs, Threat Response collects the following IOC data:

    - File system changes
    - Network activity
    - Processes
    - Registry changes

  - **Infection Analysis**

    Threat Response uses the IOCs collected from Carbon Black to identify any IOCs that match forensics event data resulting in an IOC Confidence score

- **Updated SMB version for native Threat Response IOC collection agent**

  Starting in v3.5, Threat Response now supports SMBv2 as the default protocol for distributing the IOC collection agent from the appliance to endpoints. Optionally, Threat Response can be configured to use SMBv1 if SMBv2 is not available.

  Also starting with v3.5, the Threat Response IOC collection agent uses TLSv1.2 as the default for communicating between the agent and the Threat Response server with the ability to fallback to TLSv1 or TLSv1.1 (as a configurable option).

  These optional fallback mechanisms allow Proofpoint to continue to provide support for those customers using Windows Server 2003, XP, and older devices. Note that Windows XP only supports SMB v1 and TLS v1.0.

Threat Response Auto Pull (TRAP) Enhancements

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

- **Abuse Mailbox Support**

  Threat Response Auto Pull (TRAP) now includes a new feature for managing Abuse Mailboxes. This allows security analysts to use Threat Response to monitor an abuse mailbox to quickly understand the context around user reported potentially malicious emails. Abuse mailboxes on MS Exchange, Office 365 and Gmail are supported.

  - **Support for multiple mailboxes and folders:**

    Each mailbox and folder combination can be configured as an independent “Abuse Mailbox” Source.

  - **Automatic Enrichment:**

    For any messages that are found in an abuse mailbox, PTR will automatically create an incident or link to an existing incident (linked via the message-ID of the original message), and enrich with Proofpoint’s email threat intelligence including information such as campaign, URL and file hash reputation.

  - **Email Quarantine:**

    For any messages that were deemed to be malicious by the security Analyst (as forward-delivered to the abuse mailbox), the user can choose to manually quarantine that message.

- **Email address Quarantine Whitelist :**

  This release includes the ability to whitelist specific mailboxes to exempt them from any email quarantine actions. This is especially needed in the case of forwards to avoid quarantining specific email addresses from quarantining action.

  - Before initiating an email quarantine, TRAP will first check the target email address against the whitelist to make sure that there are no matches prior to processing any quarantine logic.

  - For Whitelisting purposes, DLs (Distribution Lists) and Google Groups are both just treated as email addresses. So if the Whitelisting matching logic

finds the email associated with the DL or group, we will exempt that list from quarantining actions.

- All abuse mailbox entries are automatically (internally) treated as whitelisted mailboxes to ensure that messages forwarded to an abuse mailbox are not automatically quarantined and thus removed from the abuse mailbox.

- **Advanced Gmail TRAP features**

  Support for Gmail via TRAP was introduced in Threat Response v3.4. Beginning with v3.5 release multiple advanced features are included that provide parity with email quarantine for Exchange and O365 environments.

  Newly introduced features for Gmail include the following:

  - **Forward Following**: Allows for recursive following of emails that were forwarded versions of the original email, in order to quarantine all mails in the forwarded chain containing the latent threats

  - **Missing Message-ID**: When the message-ID is missing in the alert search for matching emails using attributes of the original message.

  - **DL Expansion for Google Groups**: Expand any recipients that map to Google Groups to create a list of all actual recipients for email quarantine actions.

- **Support for quarantining from recoverable items**

  Starting in v3.5 email quarantine actions will include looking for messages that have been moved to a user's Dumpster / Recoverable Items folder.

  Note: Threat Response has a limitation at this time quarantining from the Recoverable Items folder on Office 365 if Full Mailbox Access permissions are being used by the service account.

Incident and Investigation Enhancements

Incident Enhancements

- **Explicit Linking Logic for JSON events**
  With this release JSON events can be explicitly linked to an Incident based on a field in the JSON event. Events submitted to Threat Response can now optionally include a field in the JSON event to indicate what field the Alert should be linked by.

Providing this field bypasses normal Incident linking logic and instead links exclusivlely based on the supplied field.

The JSON event can include one of the following fields as the field to link on:

- **"target_ip_address"**
- **"target_hostname**
- **"target_machine_name"**
- **"target_user"**
- **"target_mac_address"**
- **"attacker_ip_address"**
- **"attacker_hostname"**
- **"attacker_machine_name"**
- **"attacker_user"**
- **"attacker_mac_address"**
- **"email_recipient"**
- **"email_sender"**
- **"email_subject"**
- **"message_id"**
- **"threat_filename"**
- **"threat_filehash"**

- **CSV upload Source**

  Threat Response v3.5 introduces a new Even Source that can be used to initiate a quarantine action for the Message-ID and recipient pairs supplied in the uploaded CSV file. Expected format is for the first entry to contain the message-ID and the second entry to include the recipient. This source helps to achieve manual quarantine against all types of mail servers (Exchange, O365 and Gmail)

Platform Enhancements and Improvements

- **Multiple Team Membership:**

  Starting with this release Threat Response Users can now be configured to belong to more than one team. User privileges for users that are members of multiple teams are the union of the permissions available from each of the teams the use is a member of.

- **Additional actions added to audit history log**

  We now log additional actions in the audit history. Following is a list of the additional actions that were added to the audit log
  - Audit records for Investigation Activities (linking/unlinking incidents, adding comments, adding attachments).
  - Audit records for Incident Activities (Severity changed, Team changed, added comment, added attachment, incident field changed, target/attacker host/user changed)
  - Audit records for Incident (Description changed, Assignee changed)
  - Added username of the account that initiated manual PC Data Collection to the audit records.

Additional Enhancements and Improvements

The following improvements are included in this release.

- **Customer provided VirusTotal API Keys:**

  Starting in v.35 Threat Response administrators can optionally supply their own VirusTotal (VT) API key. This allows customers to use their own API key for VT queries.

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 3.5.0 – OVA File (Fresh Installs only):

Proofpoint_Threat_Response_Installer-3.5.0.ova

Threat Response 3.5.0 – IMG File (Upgrades only):

Proofpoint_Threat_Reponse_Update-3.5.0.img