Proofpoint Threat Response v4.0.0 Release Notes

July 2018

Release Summary

Threat Response 4.0 adds significant features and capabilities to the Threat Response and TRAP capabilities, API enhancements, and additional bugfixes

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://proofpointcommunities.force.com

Platform Features & Enhancements

Extensibility to PTR Platform via Python Scripting:

- Custom integrations using Alert ETL ingestion through Python Scripting. This allows for custom Extract-Transform-Load (ETL) operations to be performed by consuming events from arbitrary sources and transforming them into PTR native events for ingestion purposes.
    - Scripted Poller Source: Allows for an ETL script to be set to query a custom source at set intervals to import alert data.
    - Scripted Listener Source: Allows for an ETL script to be triggered by an outside source sending alert data into Threat Response.
    - This feature also adds script management functionality to debug scripts in test mode before promoting them to production

LDAP Authentication Improvements:

- Group Membership Sync: User Access can now be granted based upon their AD/LDAP group membership for non-administrators.

Syslog Enhancements:

- Syslog has been improved to now include Threat Response's Audit log. Previously only system events were available via syslog. This change introduces new incident specific events to syslog as seen below. As before syslog can still be sent via UDP to remote destination

- Incident Activity Type is now included in the structured data section of the syslog
    - state_change
    - comment
    - attachment
    - response
    - auto_response
    - undo_quarantine
    - event_linked
    - collection_started
    - collection_finished
    - incident_field_changed
    - team_changed
    - investigation_link_changed
    - summary_changed
    - target_host_changed
    - attacker_host_changed
    - target_user_changed
    - attacker_user_changed

- event_reviewed
- list_members_added
- list_members_removed

Example text of new incident syslog output:

```
[PTRAuditData username="admin" event="MODIFY" identity="Incident(1327)"][incident_data
incident_id="1327" updated_at="2018-05-30T10:41:08.079Z" old_assignee="Unassigned"
new_assignee="admin" old_status="open" new_status="open"
summary="Deadpool"][custom_fields classification="Impostor" severity="Informational"
attack_vector="Web"] admin MODIFY Incident(1327) notification_sent=no description=
```

Threat Response Auto-Pull (TRAP) Enhancements

Abuse Mailbox Improvements:

- Integration with Wombat: Abuse Mailbox Monitor now supports messages reported by Wombat's PhishAlarm plugin directly into a configured Abuse Mailbox. This integration needs PhishAlarm plugin as well as PhishAlarm Analyzer to be present in addition to Threat Response. Please note that at this point reporting via Exchange (Thick Client Plugin) and O365 (Web Client Plugin) are supported.

Quarantine Summary Dashboard

- A new Quarantine Summary has been added to the Dashboard overview to provide additional quarantine details.
  - Quarantine results (success and failures)
  - Recent Attempts
  - Server Health
  - Top Recipients
  - Quarantines by mail environment (Exchange, Gmail)

Incident and Investigation Enhancements

Incident List Improvements:

- A new Bulk Response item has been added to perform the "Undo Quarantine" action across multiple incidents at once from the Incident List View

- Incident List View now includes a summary of successful and failed quarantine status on the Incident summary.

Proofpoint Threat Response API Enhancements

Threat Response's Incidents API now includes the following updates:

- Custom response JSON's changes:
  - Added custom fields
  - Now able to distinguish from Target/Attacker/CNC IP addresses
- Incident API Changes:
  - Added fields for Email Read, Quarantine Undone, and Quarantine Details.
  - Improved "Incident Retrieval" API query to include "updated_before" and "updated_after" fields for detecting changes in Incidents.

Additional Features & Enhancements

- Tanium query can now be performed by hostname instead of requiring the entire FQDN.
- Quarantine from Exchange Online Archive (EOA)
- Ability to bypass proxy settings when connecting to on-premises Exchange servers
- Increased the size of Incident Investigation description dialogue box
- Clicking "Test" no longer resets the password field when connecting services.

Bugfixes

The following issues have been resolved:

- When clicking on related incidents for a given hostname, results now correctly search based upon that hostname instead of the incident ID
- Resolved an issue that caused timeout errors after 5 minutes when using the match condition field "Suppress Incident Creation"
- User last login time now correctly displays after login. Previously would only show after user logged out and back in again.

- Fixed a bug that caused the incorrect results to be displayed when entering custom day: dates for the Email Quarantine Report
- Fixed a bug that caused Full Access service accounts in Office365 to occasionally fail to quarantine from “recoverable items”
- Fixed a bug that caused the Abuse Mailbox Monitor to incorrectly display target/attacker information when abuse message was submitted as an attachment.
- Improved memory allocation to reduce “Out of Memory” issues that could cause certain backend services to fail.

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 4.0.0 – OVA File (Fresh Installs only):

https://dl1.proofpoint.com/download/ThreatResponse/4.0.0/Proofpoint_Threat_Response_Installer-4.0.0.ova

Threat Response 4.0.0 – IMG File (Upgrades only):

https://dl1.proofpoint.com/download/ThreatResponse/4.0.0/Proofpoint_Threat_Response_Update-4.0.0.img