Proofpoint Threat Response v4.1.0
Release Notes

August 2018

Release Summary

Threat Response 4.1.0 is a minor release that brings support for IBM Domino into the main code line. It also improves upon the platform's bulk action capabilities, and provides additional bugfixes.

Please refer to the following for more detailed information:

1. Platform Features & Enhancements
2. Threat Response Auto-Pull (TRAP) Enhancements
3. Incident and Investigation Enhancements
4. Additional Features and Enhancements
5. Bugfixes
6. 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

Platform Features & Enhancements

IBM Domino Integration

- As of 4.1.0 support for IBM Domino has been integrated into the main code line. Customers running IBM Domino can upgrade to this version and then follow the regular update path in the future.

Threat Response Auto-Pull (TRAP) Enhancements

Quarantine Summary Dashboard

- The “Successful Quarantines by Mail Provider" chart has been modified to show "Successful Quarantines by Mail Server". The mail server’s name, rather than type, will now be displayed.

Incident and Investigation Enhancements

Incident List Improvements:

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

Additional Features & Enhancements

- Added additional fields to the search index:
  - Campaign ID
  - Actor ID
  - Malware ID
  - Exploit Kit ID
- Changed the method used to reboot when Threat Response has been setup as a cluster. Upon clicking “reboot” user will now be redirected to the “Cluster Status” page where they will be able to choose which node(s) to reboot.

Bugfixes

The following issues have been resolved:

- Corrected username discrepancy in syslog entries for LOGIN events
- User-created custom fields can again be added as “Incident Close Requirements”.
- Corrected an issue affecting IBM Notes integration whereby copies of received emails were not getting quarantined.
- Corrected an issue that would sometimes cause all incidents not to display upon scrolling down after sorting incidents in the incident list page

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 4.1.0 – OVA File (Fresh Installs only):

https://dl1.proofpoint.com/download/ThreatResponse/4.1.0/Proofpoint_Threat_Response_Installer-4.1.0.ova

Threat Response 4.1.0 – IMG File (Upgrades only):

https://dl1.proofpoint.com/download/ThreatResponse/4.1.0/Proofpoint_Threat_Response_Update-4.1.0.img