Proofpoint Threat Response v3.3.0
Release Notes

August 2017

Release Summary:

Threat Response 3.3.0 provides performance enhancements as well as significant product improvements and enhancements across the following product areas:

- Workflows and Incident Management
- Integrations
- Reporting
- Platform Performance
- Download Instructions

Recommendations:

As with any software upgrade it is recommended that a full system backup be created 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/

Workflows and Incident Management:

Email Quarantine (TRAP) Workflow Improvements:

The following improvements to Threat Response Auto Pull (TRAP) workflow has been introduced:

- **Retry Attempts:** Increased quarantine retry attempts.
- **Retry Time Delay:** Implemented a new back-off algorithm to increase the time between retry attempts.

Incident Management Workflow Improvements:

The following improvements to Incident Management workflows have been introduced:

- **"Unassigned" Incident Filter:** A quick filter was added to the Incident List page to enable viewing of "Unassigned" incidents.
- **Splunk/JSON Alert Custom Field Mapping:** Alert data received via the Splunk 2.0 or a JSON alert source that contain custom fields that match custom incident fields configured in systems settings will be matched and displayed at the incident level. Values are only updated if the custom field value is empty.

Integration Additions and Enhancements:

Palo Alto Network Systems Improvements and Expansions:

The following improvements and expansions to the Palo Alto Networks Systems integrations have been introduced:

- **Panorama Support:** Support for Panorama has been adopted through the current version 8.0.2. This includes support as both an alert source and device member.
- **External Dynamic Lists Support – Host/IP Lists**: The dynamic list URL for host/IP lists hosted by Threat Response has been updated to support the new requirements for the external dynamic lists.
- **External Dynamic List Support – URL Lists:** Threat Response URL lists that have been published now include a URL under "Show published URL…" that is able to be leveraged by external dynamic lists.
- **AutoFocus and MineMeld TAXII Integration:** AutoFocus can provide intelligence data to Threat Response through MineMeld. MineMeld is used to create a TAXII output node that Threat Response can subscribe to.

Splunk Integration Expansion:
Following updates were made to Threat Response integration ecosystem:

- **Customer JSON Response Enhancement:** The custom JSON response can now be configured to authenticate to Spunk's HTTP Event Collector (HEC). When used within a match condition this response will include an overview of the alert and related incident data.

Reporting Enhancements:

The following are some of the reporting enhancements have been introduced:

- **Export to CSV:** All reports listed under 'Reports' are now able to be exported in comma-separated values (CSV) format.

Platform Performance Enhancements:

Page load times have been improved in the following areas:

- **Reports:** Multiple reports have been improved to reduce the page load time.
- **Incident Alerts:** The Alerts view in incidents was adjusted to provide faster load times.
- **Incident Identity:** In incidents where a user might be associated with a large number of incidents the load times have been improved.
- **Incident Overview:** The Incident Overview page was enhanced to improve the loading time.
- **Incident Hosts:** The Hosts page was modified to improve load times.
- **Threat Intel:** Some Threat Intel pages have been enhanced to improve load times.

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 3.3.0 – OVA File (Fresh Installs only):

Proofpoint_Threat_Response_Installer-3.3.0.ova

Threat Response 3.3.0 – IMG File (Upgrades only):

Proofpoint_Threat_Reponse_Update-3.3.0.img