Proofpoint Threat Response 4.3.0

Release Notes

November 2018

Overview

Proofpoint Threat Response (PTR) 4.3.0 specifically details *enhancements*. A comprehensive understanding of these *improvements* can be gained here via the

- Summary of Enhancements/Improvements

Instructions for downloading are also provided.

Important Note

We strongly advise that a full system backup be created prior to starting the upgrade. Backups can be initiated via the **Appliance Management Console**. Note that your backup, as well as an export of the **Master Secret**, should be downloaded and stored in a secure location. In the event that any issues are encountered during or after the upgrade, please open a support ticket:

https://proofpointcommunities.force.com/

Summary of Enhancements/Improvements

Please note the following:

Proofpoint Protection Server (PPS) Integration Relating to the Abuse Mailbox

Improvement: PPS Email Header and Setting the Abuse Alert Severity

- Severity of an alert is now directly derived from PPS.

Feature: Setting the Abuse Disposition

- Whenever an abuse alert creates or links to an "incident," the message is quarantined and the *abuse disposition* changes to "malicious."

Feature: Allowing Auto-Close Incident Upon Successful Quarantine for the Abuse Mailbox

- The *auto-close* "incident" capability has been extended to include the *abuse* "mailbox" case.

Improvement: Allowing Quarantine Response Based on Abuse Disposition

- The *auto-quarantine* "response" is triggered if an *abuse* "message" is deemed malicious by its *abuse disposition*.

Improvement: The Close Incident Response Condition

- The "response" condition closes an "incident" using a match condition.

Instructions for Downloading

Note that the minimum specification for the virtual appliance has been updated. Moreover, VMware no longer supports ESXi 5.5. We strongly recommend using VMware ESXi 6.0 or a newer version, such as 6.5. Going forward, PTR/TRAP releases will require a minimum of VMware ESXi 6.0.

https://kb.vmware.com/s/article/51491/

Please be sure to use Proofpoint CTS credentials to access downloaded images.

PTR 4.3.0 OVA File (Fresh Installs Only)

https://dl1.proofpoint.com/download/ThreatResponse/4.3.0/Proofpoint_Threat_Response_Installer-4.3.0.ova

PTR 4.3.0 IMG File (Upgrades Only)

https://dl1.proofpoint.com/download/ThreatResponse/4.3.0/Proofpoint_Threat_Response_Update-4.3.0.img