Proofpoint Threat Response 4.4.0

Release Notes

January 2019

Overview

Proofpoint Threat Response (PTR) 4.4.0 specifically addresses customer-reported issues and general bug fixes, including security vulnerabilities and performance 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:

Improvement: Abuse Mailbox Alerts Linking

- “Abuse Mailbox” alerts now link automatically when at least two of the following fields match: **Sender**, **Subject**, and **URLs** from the message body.

Bug Fix: Multiple PRI Headers Are Displayed in Remote Rails Syslogs

- The issue concerning multiple message-header fields with the same field name, as displayed in remote rails syslog messages, has been corrected.

Bug Fix: Auto-Quarantine Response Is Attempted Even When Invalid CSV File Is Imported

- While PTR allows a random CSV file to be uploaded and processed to create alerts, it no longer allows a quarantine to be attempted when there is a “match condition” present and when neither *Message-ID* nor “recipient” *Email-ID* exist.

Bug Fix: LDAP Attribute telephoneNumber Is Not Displayed on the User Interface

- Previously, the LDAP attribute *telephoneNumber* was fetched from LDAP but was not shown on the UI.

  All the attributes for a user in the **Active Directory** are now displayed along with *telephoneNumber*.

Bug Fix: Containers and the “Exited/Stopped” State

- Containers with a state of “Exited/Stopped” are cleaned up via the */var* partition.

Bug Fix: ETL: Add UI and Fix Up Backend Cleaner to Include Failed Script Runs

- A UI option has been added to configure the number of failed runs to retain per event source. A daily “cleanup” task now runs and clears out the input and output of the oldest script runs up to the configured limit. In summary, failed script runs, as well as any successful runs, are cleaned up daily.

Bug Fix: Unable to Quarantine a DL Using Modern Authentication on Office 365

- We resolved an issue where quarantining a *DL* using **Modern Authentication** on Office 365 results in failure. Note that if **Modern Authentication** is used, the account which belongs to a “quarantine mailbox” must have sufficient permissions to *expand DL*.

Bug Fix: LDAP Team Sync Fails if One of the Sync-Enabled Teams Has Invalid LDAP Details

- We resolved an issue where an *LDAP team sync* failed when the list included invalid *LDAP groups*.

Instructions for Downloading

Note that VMware no longer supports ESXi 5.5. It is strongly recommended that you should use 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 4.4.0 OVA File (Fresh Installs Only)

https://dl1.proofpoint.com/download/ThreatResponse/4.4.0/Proofpoint_Threat_Response_Installer-4.4.0.ova

PTR 4.4.0 IMG File (Upgrades Only)

https://dl1.proofpoint.com/download/ThreatResponse/4.4.0/Proofpoint_Threat_Response_Update-4.4.0.img