Persistent

CyRev

Release Notes

Software Version: 1.1.3

Legal Notices

Warranty

The only warranties for products and services are set forth in the express license or service agreements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty of any kind, implied, statutory, or in any communication between them, including without limitation, the implied warranties of merchantability, non-infringement, title, and fitness for a particular purpose. Accelerite shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from Accelerite or its licensors required for possession, use or copying. No part of this manual may be reproduced in any form or by any means (including electronic storage and retrieval or translation into a foreign language) without prior agreement and written consent from Accelerite.

Copyright Notices

© Copyright 2023 Persistent Systems Ltd. All rights reserved.

Trademark Notices

Accelerite and Persistent are trademarks or trade name or service mark or logo of Accelerite/Persistent. All other brands or products are trademarks, trade name, service mark, logo or registered trademarks of their respective holders/owners thereof.

Disclaimer

The CyRev products are available and support only the English language.

Table of Contents

Introduction

This document outlines the details of a patch update for CyRev. It includes information on the specific issues addressed, any new features, and known issue for the CyRev product.

Application Version

1.1.3

What's New

Here are changes that are added to improve user experience:

\ Added support for the latest GCBDR version 11.0.5.x.

\ Automated the Scanning flow from UI: The scanning process has been automated through the development of new buttons and pages according to the product design. CyRev offers two types of scanning that are image scan and application scan.

- Image Scan: You can scan the images by following the below steps. A "Schedule New Scan" button has been added on the detection page, which leads to the repositories page.
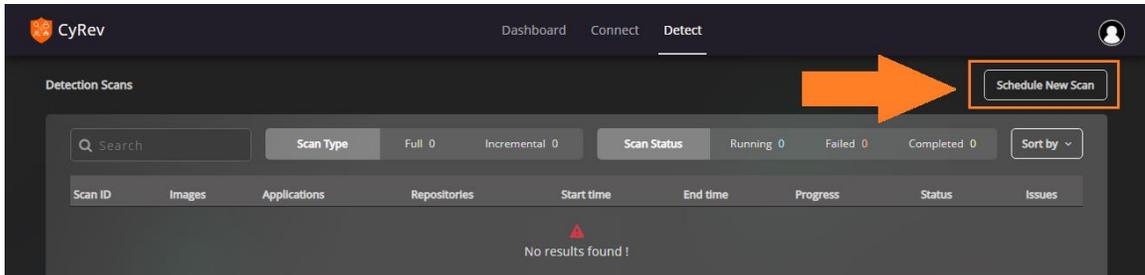
From there, you can select a repository and view the list of applications stored within it.
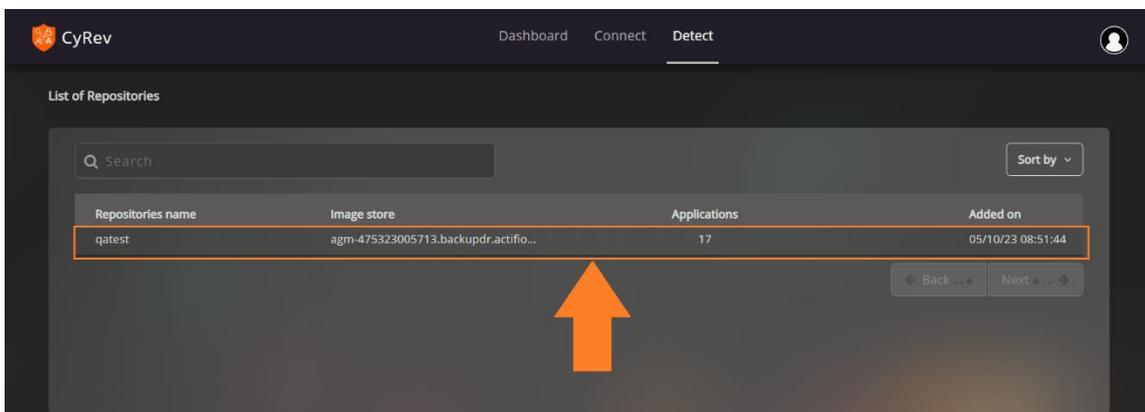
Clicking on an application will allow you to access a list of available images for that application.
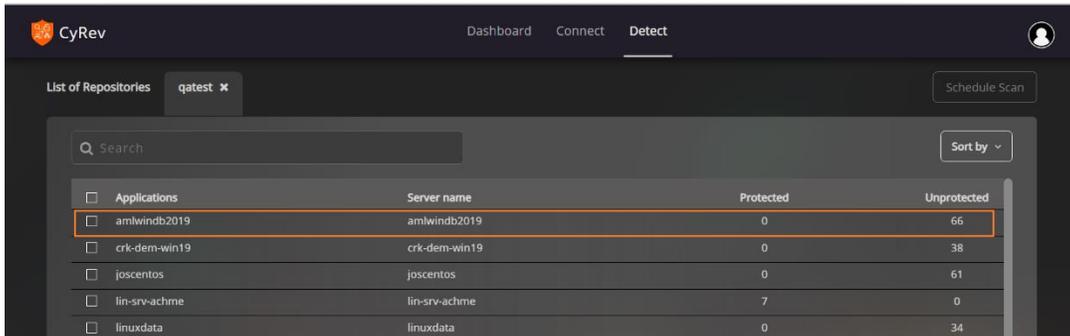
You can select the specific images you wish to scan by clicking on them and then selecting "Schedule Scan".
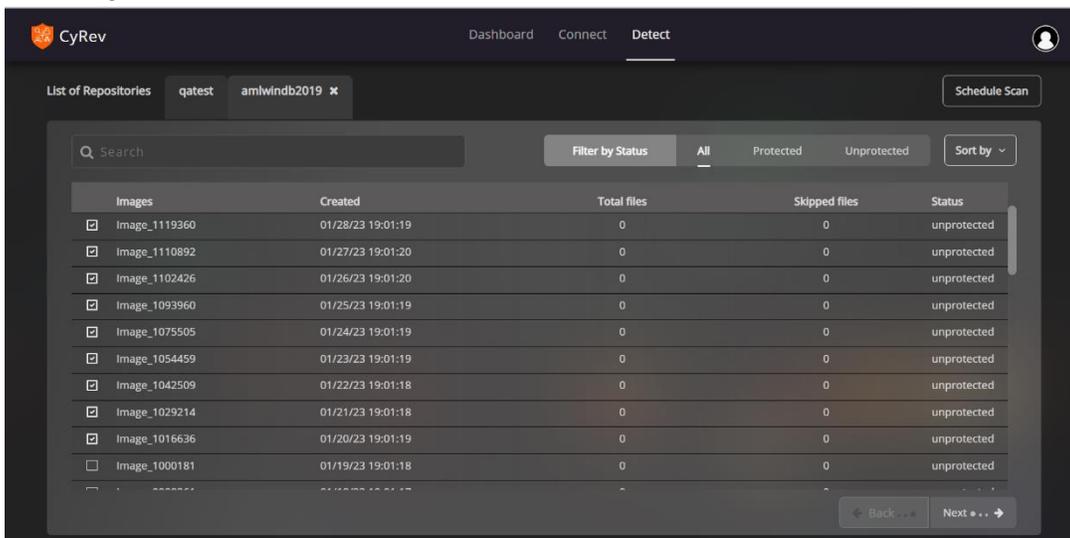
This will take you to the "Run Scan" page where you can see a summary of the selected images.
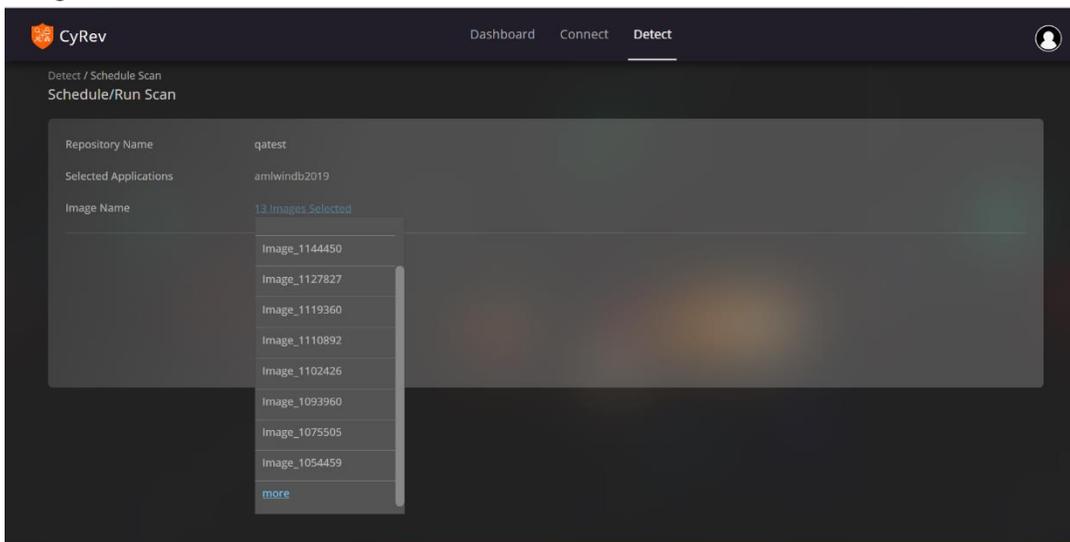
To initiate the scanning process, simply click on "Start" to submit your request.
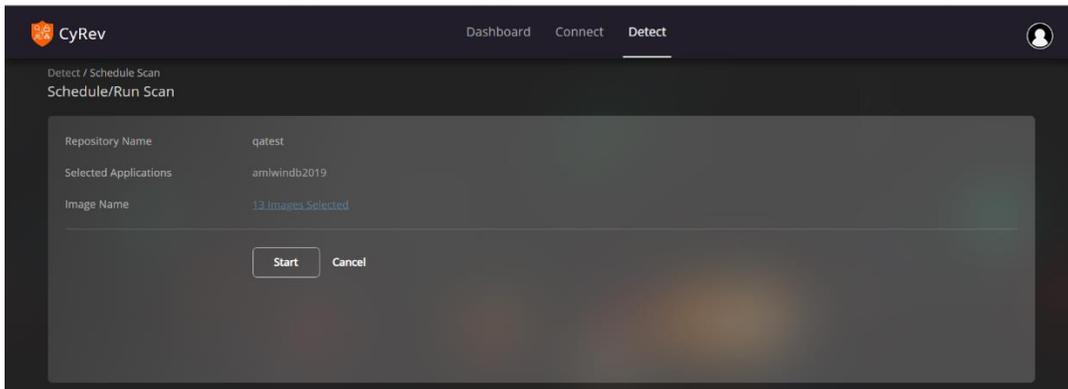
- Application Scan : You can scan applications by following the below steps. A "Schedule New Scan" button has been added on the detection page, which leads to the repositories page.
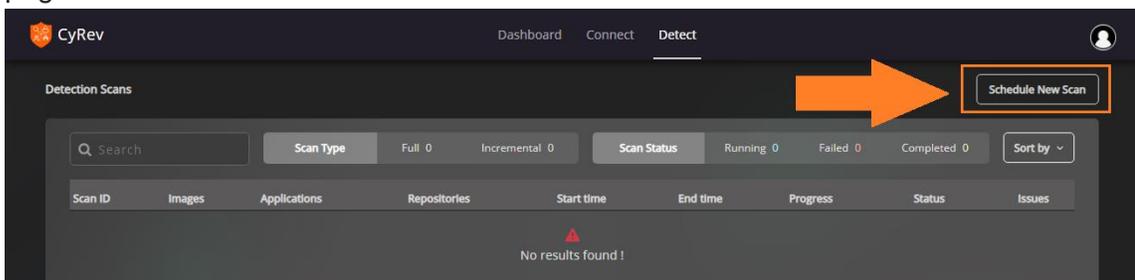
From there, you can select a repository and view the list of applications stored within it.
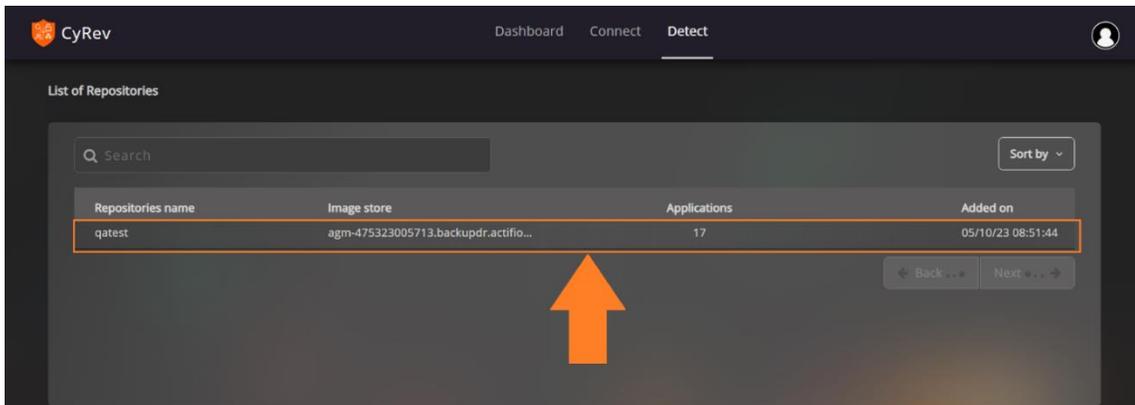
You can select the specific applications or images you wish to scan by clicking on them and then selecting "Schedule Scan".
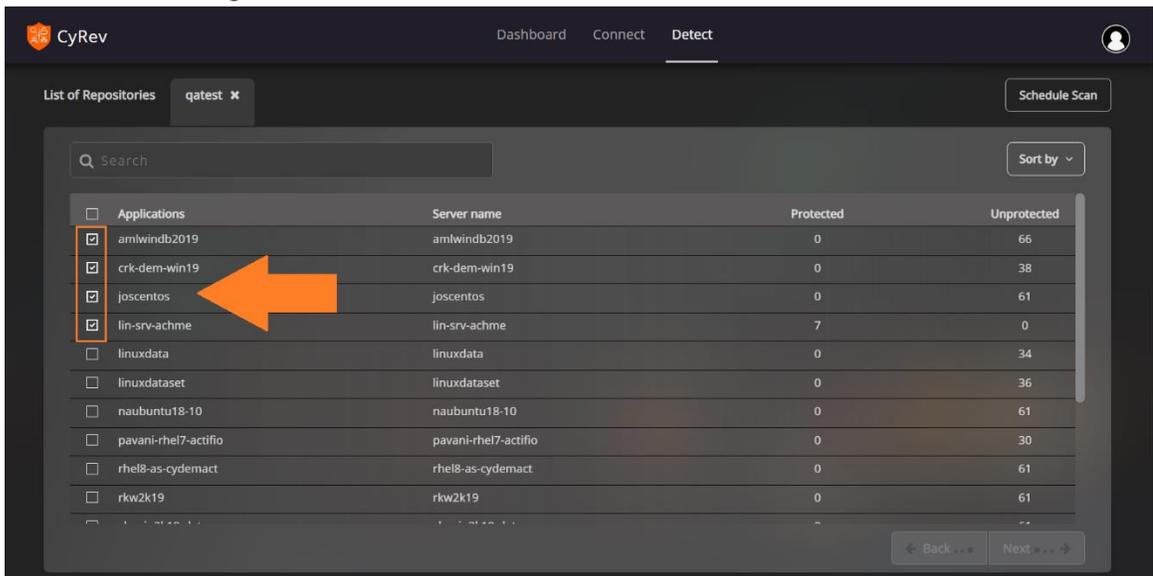
This will take you to the "Run Scan" page where you can see a summary of the selected applications.
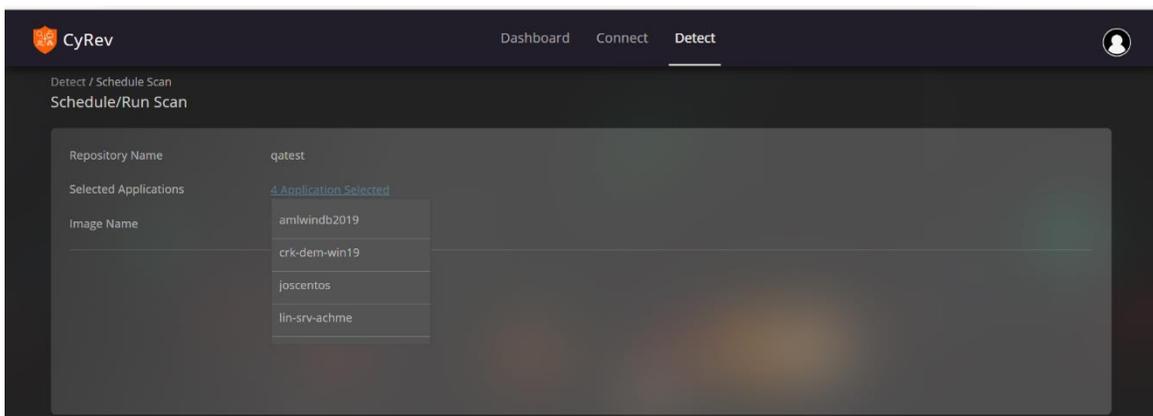
To initiate the scanning process, simply click on "Start" to submit your request.
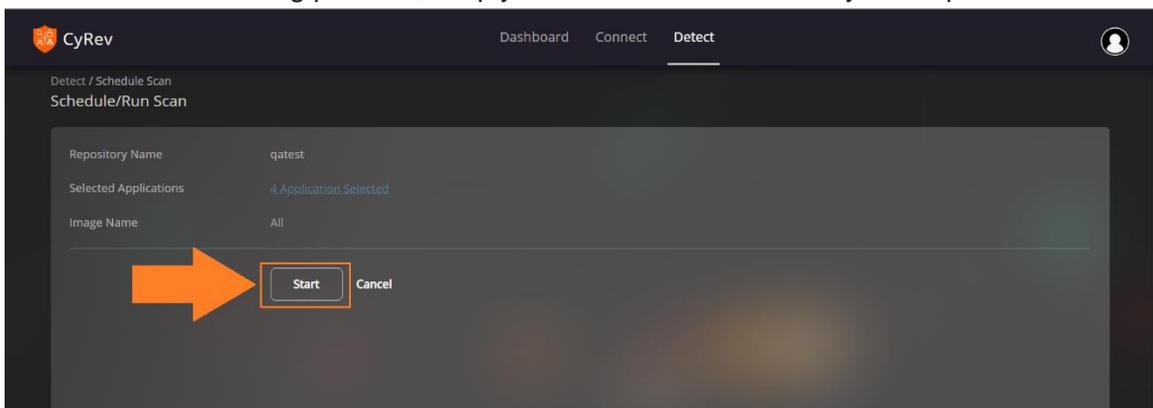
\   Remediate Page: The remediate page tables are revised to add more information. The changes are:

- Image Table: Image table has improved for following features:

  \   New column is added to the image table named as File and which is sub-divided into 2 section names as Total and Skipped.

  \   Existing Encrypted File column name changed to High Entropy.

  \   The Status column name changed to Recovery Candidate image.

  \   Added File Type button to filter file type across all images. Also, user can use search feature provided to search extension or file type.

  \   Existing columns are rearranged to accommodate the information.

- File Table: Files table is improved for the following features:

  \   Entropy column is rearranged, divided into two parts in which 'Current' and Previous entropy. This will assist user to analyze change in entropy for the file.

  \   Added the Hash column to the table to improve search feature for the files.

  \   Pagination: Added the pagination animation to the Back and Next button.

\   Dashboard Page: The dashboard page updated for following changes:

- Revised 'Registered Repository' label to 'Repository'.

- Made few changes to UI panel colors to improve clarity, color, fonts, and visuals.

- Pie Chart improved to add the highlight as per design.

- Improved Applications with threats (Top 10) graph for visuals.

- In Applications with threats table the Alert column label changed from Medium to Med. The space between the column has changed to accommodate more information. Change column name from Cyber risk to Risk and Alert level to Alert. The Date format is updated in the table in MMDDYY format.

- The Risk Trend Graph has been enhanced to provide a more comprehensive representation of the cyber risk fluctuations. The graph now displays the changes in risk on a per-minute basis. Also, the size of the dots reduced to streamline the graph. You can zoom in the graph by selecting the area as shown in below screenshot.
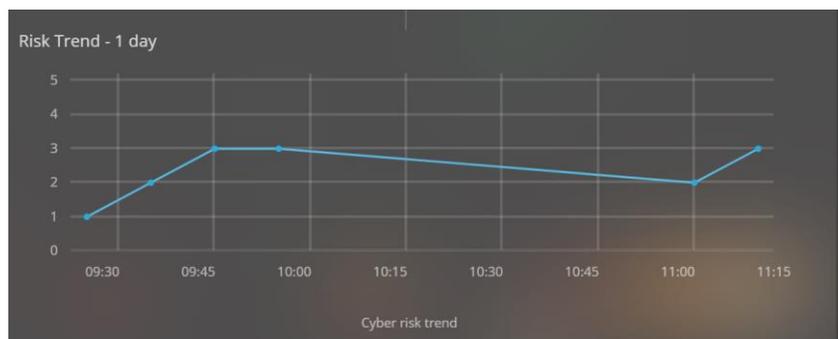
You can restore view by clicking Zoom Out button.
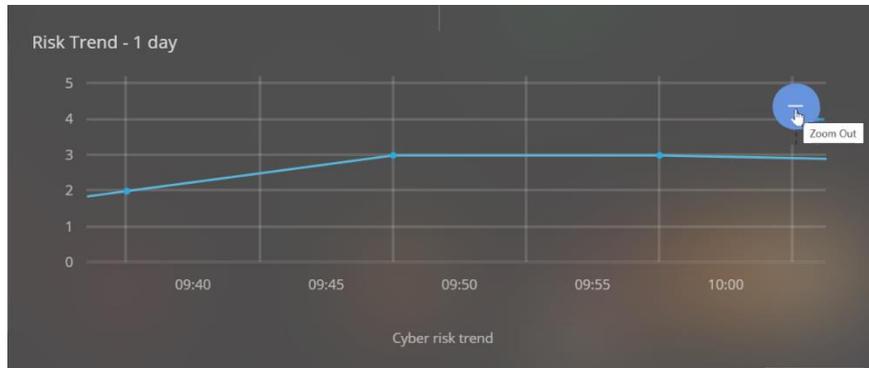
\ Connect Page: Connect page is updated for following changes:

- Number of application column name changed to Applications.

- Number of images protected column name changed to Protected.

- Number of images unprotected column name changed to Unprotected.

- Created date column name changed to Date connected.

Defect Fixed

Here is the list of issues that are observed and fixed in CyRev 1.1.3:

Scan Failure due to Image mounting issue	
Defect ID	PICR-2576
Description	Application scanning fails application with "ERROR: Error Message: [Cannot bind argument to parameter 'MountedImageName' because it is an empty string.]"
Solution	The issue is fixed with latest build 1-1-3-26072023-12-05.
Modules Impacted	Analysis and Detection

Known Defects

This table lists the known issues for the 1.1.2 release:

In Application Test and Production REFS drive support issue	
Defect ID	PICR-2557
Description	In test and production- Windows Server with Drive formatted as REFS is not accessible and is asking to format.
Explanation	Windows drives formatted as ReFS are currently not supported.
Walkaround	None
Modules Impacted	Test And Production

In Application Test and Production REFS drive support issue	
Defect ID	PICR-2648
Description	Remediation fails in GCP Projects with Shielded VM organizational constraint enforced.
Explanation	Google export image command is currently not supported in a GCP project with the Shielded VM Org organizational constraint enforced, which prevents remediation operations from completing. It is recommended that the Shielded VM constraint be disabled during remediation until this issue is addressed in GCP.
Walkaround	None
Modules Impacted	Remediation

Google Console issue for wrong indication for RDP and SSH	
Defect ID	PICR-513
Description	The connection type on the Google console is displayed as SSH instead of RDP for windows deployed VM and this is the way GCBDR create the VM.
Explanation	None
Walkaround	Use the IP address to RDP to the VM and use the username and password of the source VM.

Modules Impacted	Test and Production

Unable to cancel the remediation plan selected	
Defect ID	PICR-2782
Description	Unable to undo or cancel remediation after I confirm the files/image for remediation and before running the remediation scheduler
Explanation	None
Walkaround	None
Modules Impacted	Remediate

Remediation of few applications are in running state	
Defect ID	PICR-4502
Description	The remediation running status is not updating on UI after canceling the remediation operation
Explanation	After canceling the remediation schedular service the status for the ongoing remediation is not updating on the UI.
Walkaround	None
Modules Impacted	Remediate

For all Windows scanning is getting failed with CyRev Scanner Exception error	
Defect ID	PICR-4524
Description	The Scanning failed with CyRev Scanner Exception error.
Explanation	As per the logs the issue is due image unmount issue from the GCBDR.
Walkaround	Manually unmount the images that has been mounted on the scanner host from GCBDR console and retry the scanning.
Modules Impacted	Scanner

Linux scanning is not happened properly, and files are missing in the remediate window.

Defect ID	PICR-4503
Description	Linux scanning is not happened properly, and files are missing in the remediate window. For the linux applications, only 8 to 13 files are scanned
Explanation	None
Walkaround	None
Modules Impacted	Scanner

Few windows and Linux applications got failed due to mount exception.	
Defect ID	PICR-4485
Description	windows and Linux applications got failed due to mount exception.
Explanation	bug was originally for empty error message and null pointer exception. Empty error message has been fixed. Following exceptions has been thrown for this issue: 1. Mount Api: [@\{errormessage=Failed to get volume information about image ID 78912}.errormessage] 2. Unmount Api: @{errormessage=failed getRequest: 10.160.0.5 caused by connect timed out}.errormessage]
Walkaround	Check the GCBDR console for the error message.
Modules Impacted	Scanner

Running scan jobs are coming in between after applying end time filter.	
Defect ID	PICR-4553
Description	Running scan jobs are coming in between after applying end time filter.
Explanation	Running scan jobs after applying end time filter should come either the top or at the end because it has no end time.
Walkaround	None
Modules Impacted	Analysis and detection

Retry is not happening for the images where ml processing has been failed	
Defect ID	PICR-4460
Description	Retry is not happening for the failed images which are failed at ml processing phase.
Explanation	None
Walkaround	None
Modules Impacted	Analysis and detection

Remediation failing due to GCP API error.	
Defect ID	PICR-2643
Description	The remediation image creation fails with error message: 1260: Failed to create volume from snapshot. 155: VM task failed. Error: Cloud task failed.
Explanation	Mount image to existing gce instance API is failing with error messages. Raised a support case (#00289604) with google to address this issue.
Walkaround	None
Modules Impacted	Remediation

Contacting Support

Persistent Systems Software support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by being able to:

\   Search for knowledge documents of interest

\   Submit and track support cases and enhancement requests

\   Submit enhancement requests online

\   Download software patches

\   Look up Persistent support contacts

\   Enter into discussions with other software customers

\   Research and register for software training

To access the Self-serve knowledge base, visit the Persistent System Support home page at

https://support.persistent.com/hc/en-us

Most of the support areas require that you register on the Persistent Systems Support Portal. Many also require a support contract.

To register an account at the Persistent Systems Support Portal, visit

https://support.persistent.com/hc/en-us

To know more about registration process at Persistent Systems support portal, visit https://support.persistent.com/hc/en-us/articles/202042570-New-user-registration-process

Persistent