IBM Security

IBM Resilient SOAR Platform

Release Notes

V34

Date: August 2019

Contents

Chapter 1. What's new in V34

IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform V34 enables organizations to orchestrate and automate the people, processes, and technology that are associated with incident response. Purpose-built for either cloud or on-premises environments based on your business needs, these solutions streamline incident response and privacy response management to provide an automatic, fast, and flexible way for organizations to react to events and incidents.

The V34.0 release of the Resilient SOAR Platform introduces the following new features and enhancements. All changes and bug fixes from the previous releases are included.

The V34 product documents are available within the Resilient platform. Open the Help/Contact menu to access. You can also view the product guides and additional information in the IBM Knowledge Center.

Features and enhancements

Feature	Description
Resilient for MSSPs add-on	• Implemented the Users tab. Administrators can invite users to one or more organizations simultaneously, edit user settings, and reassign incidents. • Updated the text in the invitation email sent to users to address when a use is invited to multiple organizations. Also added a link to the documentation within the email message. • Improved performance of the configuration push. For more information, see the Resilient for MSSPs Configuration Guide.
Analytics Dashboard	Added a Sort By feature that determines the order in which fields are presented when creating custom graphs. This applies to all graph types except Table. For more information, see the User Guide.
Audit log	• Added creating, deleting and editing rules to the audit log. • Updated the documentation to describe how to view audit messages from a Splunk platform. • Changed the use of a colon (':') to an equal sign ("=") in audit messages to keep the format consistent.
Tasks page	Updated the Tasks page to be a full page, and included breadcrumbs for ease of navigation.
Security Updates	The security update for V34 addresses various security issues. For on-premises customers, consult your *Resilient Installation Guide* for the location of these updates. On-Cloud customers are updated automatically.
REST API	For API users only. The REST endpoint GET /rest/orgs/org_id/users has been deprecated and should be replaced with POST /rest/orgs/org_id/users/query_paged or POST /rest/orgs/org_id/principals/search. The existing endpoint will be available for two more major releases but may be slow for large numbers of users so it should be replaced in any custom code as soon as practical. The POST /rest/orgs/org_id/users/query_paged endpoint requires the administration/list users privileges.
Documentation	The Resilient Integration Server Guide was added to IBM Resilient Knowledge Center.

Privacy updates

The following table lists the regulators that were updated in the Privacy Solution.

In conjunction with the continued effort to maintain the Privacy Solution Regulators, the Privacy Team has revamped and refreshed the Data Breach Best Practices Regulator tasks. By updating the Data Breach Best Practices Regulator tasks, we continue to provide you with a comprehensive list of tasks that will help with implementing your best practices.

We always appreciate feedback on current legislation and guidance whether it appears in our product or not. Contact your Customer Relationship Manager if you have any questions about these updates or suggestions for future updates. You can also use the IBM Resilient Community to see how your peers are using IBM Resilient to simplify the complex world of information security.

Feature	**Description**
Australia	Updated the Resource Library.
Europe	Updated the online forms, guidance links, and contact information of the following European Union Member States: *Austria, Jersey, and Poland.*
Mexico	• Updated the Resource Library. • Removed the ‘Harm/Misuse Trigger’ from affecting the “Analyze the Incident (Mexico)” task. • Added ‘Verbal’ to the data format types. • Revised tasks “Analyze the Incident (Mexico)” and “Notify Affected Individuals (Mexico).”
US: Arkansas	Removed outdated amendment language.
US: FTC (Health)	Revised the Resource Library to include updated fines.
US: Minnesota	Revised the instructions for the “Notify MN Consumers Individually” task.
US: New Jersey	Updated the New Jersey Regulator to incorporate the new amendment changes effective 9/1/2019: • Updated the Resource Library. • Revised the “Notify NJ Consumers Individually” task. • Added the new personal data type combinations.
US: Ohio	Updated the Resource Library, and revised the instructions for the “Notify OH Consumers Individually” task.
US: Ohio (Insurance)	Removed the rule triggering for encryption for this Regulator.
US: Virginia	Removed outdated amendment language.

Chapter 2. Issues

The following tables list the issues corrected for this release, and known issues.

Corrected issues

Tracking Code	Issue
RES-11789	"No active JTA transaction on joinTransaction call" error thrown by Co3Scheduler causes the scheduler to stop working.
RES-12818	Audit messages stopped appearing on Splunk Cloud instance.
RES-12866	Analytics widget, Average Time, Time Unit switches back to minutes when modified or moved.
RES-14383	Changed the use of a colon (':') to an equal sign ("=") in audit messages to keep the format consistent.
RES-14390	Rich text field in Microsoft Edge V42 shows the cursor when focus is not actually working. This problem is not seen with Edge V44 and later.
RES-14702	Cannot create a linked LDAP group if it contains a pound (#) character.
RES-14956	The State field must be a US or Canadian state when using resutil editorg.
RES-15155	An external server error occurs during an export configuration when the system override tasks cannot find the Phase.
RES-15174	Spinners in the Artifact table do not disappear.
RES-15209	Error when creating an incident using the external/new_by_url endpoint
RES-15241	Bulk close modal does not display the values of the Incident Type field
RES-15248	Deleted User(s) appearing in group member listing on Incident View
RES-15265	DNS name regex is too restrictive
RES-15430	The notes comments are not ordered by create time, comments that has mention in it are displayed at the top
RES-15436	Microsoft Edge Paste into Resilient does not work.
RES-15640	Changing Priority of Configuration Push Command. Configuration push happens in the background. The fix here was to ensure this task has higher priority than other background tasks to ensure it completes in a timely fashion.

Known issues

Tracking Code	Issue
RES-15827	Immediately after an upgrade, a user logging in may see an error, Unable to perform the search operation. This can happen since it takes a few minutes for all system services to restart. IBM Resilient recommends that you wait a few minutes to log in after an upgrade, or wait a few minutes to log in again after seeing this error.

Tracking Code	Issue
RES-15595	With the Resilient for MSSPs add-on, an export operation fails if there was previously an import operation from a different configuration organization. To avoid this issue, consider the following: • When migrating settings from a configuration organization on one Resilient platform to another, make sure the destination organization has at least all the same child organizations as the source. • Make sure the configuration user is a member of all the organizations in the hierarchy.