IBM Resilient

Resilient SOAR Platform

Release Notes V33.0

Release Date: June 2019

IBM Resilient Security Orchestration, Automation, and Response (SOAR) Platform V33.0 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.

FEATURES AND ENHANCEMENTS

The V33.0 release of the Resilient SOAR Platform introduces a number of new features and enhancements. All changes and bug fixes from the previous releases are included.

The following new features and enhancements are provided in Resilient V33.0:

- **Resilient for MSSPs add-on:** The Resilient for Managed Security Service Providers (MSSP) add-on is an optional deployment feature that allows you to create multiple Resilient child organizations and manage them from a single configuration organization. Each child organization can be assigned to a different group, division, or company to meet their incident response requirements. A single global dashboard organization allows security analysts to analyze incident data from the child organizations. Users within a child organization cannot view the other organizations. Users in the global dashboard organization can view and manage incidents from the organizations to which they have permissions.

  The Resilient for MSSPs add-on requires a separate license.
- **API Key accounts**: API key accounts are more secure accounts designed to enable external scripts or integrations to authenticate to the Resilient platform through the REST API, with the minimum required permissions. A system-generated token is used to authenticate. API key accounts are not linked to LDAP and cannot access the Resilient user interface, own incidents or be members of an incident or group. If upgrading, you must set the API Keys permission for one or more roles before you can access this feature.

- **Analytics Dashboard**: Improved the user experience and added a number of capabilities, including:
  - Unique Count option on the Custom Incident Widget.
  - Search box in the Custom Incident Widget configuration for users to find a field.
  - Save As option when editing custom widgets.
  - Ability to export charts to different formats.
  - Time fields to calculate an average in custom charts.
  - Chart that displays the average time to close for an incident.
- **Audit log**: Updated the audit log as follows:
  - Extended the audit log to include the creation, deletion and update of API keys, workflows and message destinations.
  - Updated the **Modified By** value to specify who performed the current action, not who made the last change.
- **Country/Region value**: Added the ability to change the default value. For existing installations, the default value for the Country/Region field is set to United States. For new installations, the default Country/Region value is not set. You can change the default Country/Region value in an existing installation or new installation by editing the **Country/Region** field in the Layouts tab.
- **Import/Export**: Updated the export feature to include groups, email connection settings, notifications, and timeline.
- **Performance and user experience improvements**:
  - Improved the performance and user experience for those scenarios where there are thousands of users and groups.
  - Added the ability to enable or disable rules from the Rules tab.
  - Added a link to the IBM DeveloperWorks website on the Help/Contact page to assist integration developers in finding the Resilient developer documentation and communities.
- **Security Updates**: The security update for V33 addresses various security issues. For on-premises customers, consult the *Resilient Installation Guide* for the location of these updates. On-Cloud customers are updated automatically.

  With the new security updates, the Red Hat Enterprise Linux (RHEL) included in the Resilient Open Virtualization format (.ova file) is effectively version 7.6.
- **Optional Packages**: The OpenVPN package has been added to the optional packages installer.

Privacy Updates

- New Feature: **Date Determined**

  V33 adds a new field in the layout of the Privacy Solution called **Date Determined**, which will show up by default in the Breach tab of the Privacy Solution. The Date Determined field can be used to calculate the due dates of regulatory tasks in the Privacy Solution.

  In previous versions of the product, the due dates of custom tasks are calculated based upon a single field, **Date Discovered**. Users can now choose whether the due date of a custom task is to be calculated from the **Date Discovered** (the date the incident was discovered by your organization), **Date Determined** (the date your organization determined whether or not the incident involved a breach of personal information), or **Date Task Initiated** (the date the task was activated).

  Please note, if you leave the Date Determined field blank when creating an incident, it automatically defaults to the value you provided in the Date Discovered field.

As an existing customer, your layouts remain unchanged during installation to retain any existing customizations. If you choose to delete the **Date Determined** field from the Breach tab, but later decide to re-add it, you must add it manually by completing the following steps.

1. Click ***OrgName* > Customization Settings**.
2. Open the **Layouts > Incident Tabs > Breach** tab.
3. Under **Fields**, search for **Date Determined**.
4. Click and drag the **Date Determined** field, and insert it between **Was personal information or personal data involved?** and **Is harm/risk/misuse foreseeable?**.
5. Click **Save** to apply your updates.

Note: Your current layouts might not look exactly the same as described below depending on which version of the Resilient platform you started with and what customizations you have made.

- The following regulators were updated in the Privacy Solution:
  - **Alabama**: Updated the Resource Library with a new source link.
  - **Arkansas**: Updated the Resource Library to include the language of the Amendment (Effective July 24, 2019). Modified the logic to apply the encryption safe harbor to prevent Arkansas tasks if you respond Yes to the Data Encrypted field. Expanded the personal data-type triggers to include: “Biometric data”; or “Fingerprint”. Arkansas tasks are now generated by selecting: First Name/First Initial and Last Name, in combination with Biometric Data or Fingerprint. Created new tasks: “Notify AR Attorney General” and “Document the Determination for (AR) Residents”.
  - **Illinois**: Updated the Resource Library. Revised the instructions of “Notify IL Consumers Individually” task and “Notify IL AG (HIPPA)” task.
  - **Kansas**: Updated the Resource Library with a new source link.
  - **New York**: Updated task instructions of “Notify NY Consumers Individually” to replace reference to “email” notification with “electronic” notification. Inserted a link to the Online Data Breach Reporting Form into the task instructions of “Notify NY AG,” “Notify NY State Division of Consumer Protection”, and “Notify NY State Police”. Set the timeframe for the “Notify Credit Bureaus (NY)” task to “Most expedient”.
  - **New York (Department of Financial Services)**: Updated the Resource Library. Revised the instructions of the “Determination and Notification to Superintendent (NY Dept Financial Services)” task to include a link to the Superintendent’s Cybersecurity Resource Center.
  - **Rhode Island**: Updated the formatting of the Resource Library. Revised the instructions of the “Notify RI AG” task.
  - **Utah:** Updated the Resource Library to include the language of the Amendment. Revised the instructions of the “Notify UT Consumers” task.
  - **Virginia**: Updated the Resource Library with the language of the Amendment (Effective July 1, 2019). Expanded the personal-data type triggers to include: “Passport Number” and “Military ID Number.” Virginia tasks are now generated by selecting: First Name/First Initial and Last Name, in combination with Passport Number or Military ID Number.
  - **Canadian Provinces**: As part of a continuous monitoring and review process, we updated the content of the following Canadian Provinces: Alberta, New Brunswick, Newfoundland, New Labrador, and Ontario (Health).
  - **Europe**: As part of a continuous monitoring and review process, we updated the online forms, guidance links, and contact information of the following European Union member states: Austria and Germany.
  - **Mauritius**: Added this new regulator under the Africa Region in the Privacy Solution.

- **Singapore**: Updated the Resource Library to incorporate the Personal Data Protection Commission's Guide 2.0 to Managing Data Breaches. Modified the harm trigger to only prevent the "Notify Affected Individuals (Singapore)" task from activating if you respond "No" to the "Is harm/risk/misuse foreseeable?" field. Added verbal as a Data Format trigger. Updated the instructions of the "Notify Personal Data Protection Commission (Singapore)" and "Notify Affected Individuals (Singapore)" tasks. Modified the due date of "Notify Personal Data Protection Commission (Singapore)" to 72 hours, and "Notify Affected Individuals (Singapore)" to "As soon as practicable". Created a new task: "Document the Breach (Singapore)" which has a set time frame of "As soon as practicable".
- **Uganda**: Added this new regulator under the Africa Region in the Privacy Solution.

NOTE: 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.

CORRECTED ISSUES

Tracking Code	Issue
RES-9054	If the email address of a new user does not contain a "typical" top level domain, the user account cannot be created.
RES-9176	Notes are marked "unassigned" when users are deleted from the Active Directory.
RES-9333	Java dump files should be written to /usr/share/co3/logs.
RES-11306	Problem with indents when using the Rich Text Editor, such as in the wiki. The second level indent disappears when creating a third level indent.
RES-12394	Changes to an LDAP user's status fails when LDAP is down or the user is changed in LDAP.
RES-12771	Custom Text fields can be interpreted as dates by Elasticsearch.
RES-13057	Quartz scheduler worker threads stuck while sending email notifications.
RES-13060	Artifact tab causes JavaScript error in the web browser's console.
RES-13234	V31 upgrade fails when a linked AD group does not exist or cannot be found.
RES-13253	Add error messages to ensure users exist during upgrade and installation.
RES-13311	All outbound connections should have a timeout.
RES-13312	Custom threat service should be disabled if it is unreachable.
RES-13378	Disaster Recovery: IP address versus fully qualified host name is confusing for customers creating slow configuration times.
RES-13445	Long task or incident name extends beyond borders.
RES-13473	Cannot assign null terminated string to data table text field.
RES-13475	"No Organizations" message is not translated to comply with the client's locale.

Tracking Code	Issue
RES-13511	Some filter types are displayed in English on the Incidents page in a Japanese locale organization.
RES-13722	Whitespace at the end of an email address causes LDAP authentication to fail.
RES-13757	Mouse cursor is lost when editing a rich text field and subsequent text is written backwards.
RES-13773	Include query string when logging Elasticsearch query failures.
RES-13829	There are excessive LDAP group calculations when the LDAP group does not exist.
RES-13855	Background job fails when an incident is created by an email message and another rule tries to change an incident member or workspace.
RES-13920	When an “email message is created” rule updates the incident field “last_update_date”, other rules with the condition "is changed" for the “last_update_date” field do not see the change and are not triggered.
RES-14039	Substitution values do not work in notifications.

KNOWN ISSUES

Tracking Code	Issue
RES-15007	As part of the changes to support large numbers of users, users and groups are now indexed so that they are searchable. This indexing takes place as part of the first server startup after upgrade. For installations with large numbers of users or groups or both, this indexing might add 2 to 3 minutes to the initial server startup time. This indexing is a one-time event after upgrading to version 33.
RES-13340	A change to the Roles tab that affects the permissions of the current user, does not update that user's permissions in the user interface until the user logs out and logs back in. To work around this issue, the user needs to refresh the page in the browser.
RES-13146	Safari browser users are unable to embed screen shots into rich text. This issue is being tracked with the third-party vendor.
RES-12861	The incident field, Assessed Liability, has been deprecated; however, it still appears when creating a new widget in these areas: Fields in Customization Settings, Custom Incident Widgets, and Incident list view's columns.