IBM Resilient

Incident Response Platform API

API Release Notes v31

Release Date: October 2018

IBM Resilient Incident Response Platform on Cloud and IBM Resilient Incident Response Platform V31 (on-premises licensed version) 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 Resilient Incident Response Platform solutions streamline incident response and privacy response management to provide an automatic, fast, and flexible way for organizations to react to events and incidents.

These release notes describe the changes to the REST endpoints and Data Transfer Objects (DTOs) in the Resilient platform V31 API.

FEATURES AND ENHANCEMENTS

The Resilient Platform V31 includes the following new features and enhancements:

- **Localization**: The Resilient user interface and cybersecurity playbooks have been globalized and translated into the various languages. Resilient users can change the language by setting the Web browser to their preferred language. On-premises customers can set the default language for a new organization.
- **Disaster recovery**: For on-premises customers, disaster recovery deployment options to enable rapid failover in the event of a major infrastructure outage. The Disaster Recovery system is licensed separately.
- **Scripts**: Various enhancements, such as a script query builder object that enables users to build queries in scripts, and scripts triggered by Menu Item rules (including scripts in workflows) that can access Activity Fields as a dictionary 'rule.properties'.
- **Dashboard and Reporting**: Various enhancements, such as a global dashboard-wide filter to restrict the list of incidents available / displayed in each of the displayed dashboard widgets, and added reporting on average throughput metrics for events and incidents, aiding the measurement of security practitioners' effectiveness.
- **Other changes**:
  - Support for handling large numbers of users and group in the user and groups administration pages.
  - Re-organized the Resilient menu bar for improved usability.
  - Support for sending audit data to Splunk Cloud.

More details are included in the general release notes, the System Administrator Guide, the Playbook Designer Guide, and the User Guide.

The following sections describe changes to REST endpoints, DTOs and Types.

New REST Endpoints

The following REST endpoints have been added:

- **ReportREST**
    - Provides access to reporting capabilities.

Modified REST Endpoints

The following REST endpoints have been modified:

- **ActionREST**
    - The **{org_id}/actions : GET** method has an additional parameter: layout_view_element_type that lists the actions.
- **AdminInvitationREST**
    - The **{org_id}/query_paged : POST** method has been added to return invitation details via a query.
- **GroupREST**
    - The **{org_id}/query_paged : POST** method has been added to return group details via a query.
- **OrgUserREST**
    - The **{org_id}/query_paged : POST** method has been added to return user details via a query
- **TaskREST**
    - The **{task_id}/instructions : GET** method has been deprecated and will be removed in a future release. Please use the **{task_id}/instructions_ex : GET** method instead.
    - The **{task_id}/instructions_ex : GET** method has been added to return information about the task instructions.

Deleted REST Endpoints

The following REST endpoints have been deleted:

- **EmailREST**
    - This endpoint was deprecated in v29.

New DTOs

The following DTOs have been created:

- **GDPRRiskDTO**: Defines information that is required for incidents related to GDPR.
- **IncidentHistoryReportRequestDTO**: Defines configuration options for exported incident history records data.

- **WorkflowInstanceInfoDTO**: Contains information about a workflow instance that this execution originated from.

Modified DTOs

The following DTOs have been modified:

- **ActionDataDTO**
    - The **workflow** and **user** fields are deprecated and will be removed in future release. The workflow information is available in a new **workflow_instance** field.
- **CommentDTO**
    - The **user_fname, user_lname, and modify_user** fields have been deprecated, and will be removed in a future release.
- **ConfigurationExportDTO**:
    - The **locale** field has been added to indicate the locale setting for the exported configuration.
- **ConstDTO**:
    - The **gdpr_risk_types** field has been added to enumerate the possible GDPR risk types.
    - The **max_artifact_mb** field has been added to indicate the maximum allowed size for artifacts (in MB).
- **DataTableRowDataDTO**:
    - The **version** field was added to indicate the version of the data table row.
- **FieldDefDTO:**
    - The **deprecated** field was added to indicate whether the field definition is deprecated.
- **FullIncidentDataDTO**
    - The **exposure** field has been deprecated and will be removed in a future release. Please us the **hard_liability** field instead. This field is inherited from IncidentDTO.
    - The **hard_liability** field was added to calculate exposure up to and beyond the limit provided by the deprecated **exposure** field. This field is inherited from IncidentDTO.
    - The **gdpr** field was added to provide GDPR risk information. This field is inherited from IncidentDTO.
- **FunctionDataDTO**
    - The **workflow** field has been deprecated. Use workflow_instance instead.
    - The **workflow_instance** field has been added to provide information about the workflow instance from which this function execution originated.

- **GroupDTO**:
    - The **role_handles** field has been deprecated, please use the instance_roles field instead.
    - The **last_modified_by** field has been added to provide the user who last modified the group.
    - The **last_modified_time** field has been added to provide the time at which the group was last modified.
- **IncidentDTO**:
    - The **exposure** field has been deprecated and will be removed in a future release. Please us the **hard_liability** field instead.
    - The **hard_liability** field was added to calculate exposure up to and beyond the limit provided by the deprecated **exposure** field.
    - The **gdpr** field was added to provide GDPR risk information.
- **IncidentPIIDTO**:
    - The **exposure** field has been deprecated and will be removed in a future release. Please use the **incident.hard_liability** field instead.
    - The **gdpr_harm_risk,** and **gdpr_lawful_data_processing_categories** fields was deprecated in v30.2. Please refer to the GDPRRiskDTO for use in incidents related to GDPR.
    - The **alberta_health_risk_assessment** field has been added to show the health risk information for the Alberta, Canada regulations.
- **JustUserDTO**:
    - The **last_modified** field has been added to provide information on the time at which the user/group was last modified.
    - The **password_changed** field has been added to provide information on whether the user's password has been changed.
    - The **display_name** field has been added to provide information on the display name of the user.
    - The **create_date** field has been added to provide information on the date the user was created.
- **NewsfeedEntryDTO**
    - The **user** field has been deprecated. Use **principal** instead.
- **PivotQueryDTO**:
    - The **include_interpolated_fields** field has been added to indicate whether interpolated fields should be included in the query.
- **RoleDTO**
    - The **last_modified_by** field has been added to provide information on the principal that last modified the role.

    - The **last_modified_time** field has been added to provide information on the time that the role was last modified.

- **TaskDTO**
    - The **instr_text** field has been deprecated. Please use the **instructions** field instead.

- **UserDTO**:
    - The **roles** and **role_handles** fields have been deprecated. Please use **instance_roles** instead.
    - The **last_modified** field has been added to provide information on the time at which the user/group was last modified. This field is inherited from JustUserDTO.
    - The **password_changed** field has been added to provide information on whether the user's password has been changed. This field is inherited from JustUserDTO.
    - The **display_name** field has been added to provide information on the display name of the user. This field is inherited from JustUserDTO.
    - The **create_date** field has been added to provide information on the date the user was created. This field is inherited from JustUserDTO.

- **UserOrgDTO:**
    - The **deactivated** field has been added to indicate whether the user is deactivated.
    - The **roles** and **role_handles** fields have been deprecated. Please use **instance_roles** instead.

- **UserSessionDTO:**
    - The **user_displayname** field has been added to provide information on the display name of the user.

- **WikiPageDTO:**
    - The **mentioned_users** field was removed. This was deprecated in v29.
    - The **mentioned_widgets** field has been added and it refers to the widgets that are used by a page.

Deprecated DTOs

The following DTOs are deprecated in this release:

- **ActionAcknowledgementDTO**: Use AcknowledgementDTOinstead.
- **ActionDataWorkflowInfoDTO**: The workflow data is now accessible in the workflow field in the (WorkflowInstanceInfoDTO).
- **PermsDTO**: Use the roles field in the class that references this class.
- **SessionOrgInfoPermsDTO**: Use the roles field in the class that references this class.

Deleted DTOs

The following deprecated DTOs have been deleted in this release:

- **EmailMessageDTO**: Removed as a part of the removal of SearchREST. Deprecated in v29.
- **InboutndMailboxDTO**: Removed as a part of the removal of SearchREST. Deprecated in v29.
- **RichTextWidgetContainerDTO**: Use CommentDTO instead. Deprecated in v27.2.

Modified Types

The following types have been modified:

- **FunctionType**:
    - The **AVERAGE_TIME_DIFFERENCE** field was added to provide information on the averaged time difference over the set of time difference between two date fields.
- **PivotFieldType:**
    - The **AVERAGE_TIME_DIFFERENCE** field was added to provide information on the averaged time difference over the set of time difference between two date fields.
- **ScriptMetadataType**:
    - The **SCRIPT_CONDITIONS** field was added to provide information on the conditions of the script.

Deleted Types

The following types have been modified:

- **EmailProtocolType**
- **EncryptionMethodType**