



# Resilient Incident Response Platform API

## Release Notes v25

Release Date: March 2016

Based on a knowledgebase of incident response best practices, industry standard frameworks, and regulatory requirements, the Resilient Incident Response Platform helps make incident response efficient and compliant.

## Features and Enhancements

The following endpoint has been created in version 25:

- **DataTableDataREST**: The endpoint to use to interact with data in a Data Table. For more information on the usage of Data Tables, please see the *Resilient Incident Response Platform Master Administrator's Guide*. This endpoint exposes methods to create, read, update and delete data stored on a Data Table.

The following data types and Data Transfer Objects (DTOs) have been created:

- **dataTableCellDataDTO**: This DTO represents the data of a Data Table cell and exposes the ID, name and value of the cell.
- **dataTableDataDTO**: This DTO represents all of the data of a Data Table and exposes the incident ID to which the Data Table belongs and the ID and rows of the Data Table.
- **dataTableRowDataDTO**: This DTO represents the data related to a row in a Data Table and exposes the ID, cells and actions of a Data Table row.
- **layoutType**: Layout Type enumeration. This type enumerates the available types of layout.
- **threatSourceLicenseDTO**: This DTO represents a threat source license and exposes the private\_key, expiration, public\_key and key of a threat source license.

The following data type was removed:

- threatServiceArtifactTypes

The following items were deprecated in v25:

Types:

- dataSourceDTO
- exposureVendorDTO
- exposureDepartmentDTO
- orgDataSourceDTO

Endpoints:

- POST /rest/orgs/:orgId/exposure\_vendors
- GET/PUT/DELETE /rest/orgs/:orgId/exposure\_vendors/:id
- POST /rest/orgs/:orgId/data\_sources
- GET/PUT/DELETE /rest/orgs/:orgId/data\_sources/:id
- POST /rest/orgs/:orgId/exposure\_departments
- GET/PUT/DELETE /rest/orgs/:orgId/exposure\_departments/:id

Properties:

- data\_source\_ids
- exposure\_vendor\_id
- exposure\_dept\_id
- fullOrgDTO

The associated functionality has been moved into the type/field endpoints. Here are the sequence of steps to add a new value to the data\_source\_ids field:

1. Get the fieldDefDTO for the data\_source\_ids field using a "GET /rest/orgs/:orgId/types/incident/fields/data\_source\_ids".
2. Add your new fieldDefValueDTO to the returned FieldDefDTO object's "values" array.
3. PUT the updated fieldDefDTO object using "PUT /rest/orgs/:orgId/types/incident/fields/data\_source\_ids".

The process is similar for the exposure\_vendor\_id and exposure\_dept\_id fields.

This brings the management of select list values for the data\_source\_ids, exposure\_vendor\_id and exposure\_dept\_id fields in line with other fields (e.g., severity\_code, resolution\_id and all custom select/multi-select fields).

## API Compatibility

The following consideration should be made when migrating applications using version 24 of the Resilient API to using version 25:

- When creating custom actions using the API, the object\_type field had to be specified as an integer even when using NAMES. In version 25 the object\_type field must be specified as the API name of the object type (incident, task, etc.) when using NAMES.