Resilient Incident Response Platform API

Release Notes v26

Release Date: June 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 REST endpoints have been modified:

- **IncidentArtifactREST**
  - The **copy** resource has been added to permit the copying of an Artifact.
- **incidentREST**
  - The **query_paged** resource was added to permit the paged retrieval of incidents.
  - The **related** resource has been deprecated in v26.
  - The **related_ex** resource was added to obtain a list of related incidents.
- **orgREST**
  - The **data_sources** resource has been removed.
  - The **exposure_departments** resource has been removed.
  - The **exposure_vendors** endpoint has been removed.

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

- **columnDTO**: This DTO represents a Data Table column and exposes the name and sort order of the column.
- **filterContentDTO**: This DTO represents the contents of a filter set and exposes the conditions and columns in the filter.
- **layoutPermsDTO**: This DTO represents the permissions on a layout and exposes whether the caller can delete or edit the layout, and/or edit the permissions of the layout.
- **pagedResultsDTO**: This DTO was added to facilitate the paging of data and exposes the total number of records, the actual data and the total number of records as filtered by the current query.
- **queryPagedDTO**: This DTO was also added to facilitate the paging of data. It exposes the start record, number of records in the response and the total number of records for the current query.
- **relatedIncidentsDTO**: This DTO represents a list of related incidents and exposes the records of related incidents.
- **sessionOrgInfoPermsDTO**: This DTO represents the permissions that a user has, and currently exposes only whether a user can create a shared layout.

The following Data Transfer Objects (DTOs) have been modified:

- **actionSimpleFieldDefDTO** and **actionSimpleTypeDTO**: These DTOs were modified to also return the internal ID of the field.

The following DTOs were deprecated in a past release and have been removed:

- **dataSourceDTO**
- **exposureDepartmentDTO**
- **exposureVendorDTO**
- **ns0_orgDataSourceDTO**

Resilient API Examples

The following REST API example was added:

- **java/examples/maven**: a REST API example that uses Maven.

The following fixes and updates were made to the **resilient_circuits** module in the Resilient API Python Modules:

- New ability to use a configuration file setting 'cafile=false' to disable SSL verification.
- New application mode that can restart components when the configuration file changes.
- Fixes a problem where a network outage might cause the Action Module connection to drop.
- Fixes a problem that prevents Ctrl+C from interrupting a Resilient Circuits application.

The following problem was corrected in the co3 Python module:

- The module raises an exception instead of failing silently, when users cannot access their organization due to IP address restrictions.