Resilient Incident Response Platform

CUSTOM THREAT SERVICE GUIDE v24

Published: October 2015

https://www.resilientsystems.com

Table of Contents

1. Introduction

As part of the incident response, artifacts (or evidence) may be added to an incident for tracking and analysis. The Resilient platform may scan the submitted artifacts using several predefined threat sources such as VirusTotal and iSight to provide additional information regarding the artifacts.

The Custom Threat Service allows you to provide your own artifact scanning from your own threat sources, or provide additional scanning beyond what the Resilient platform provides.

The Resilient platform supports custom threat services through a REST interface as defined within this document. To provide your own artifact scanning, you need to implement a threat service as outlined in this document.

This document assumes your familiarity with JSON, REST architecture, and the programming language of your threat source.

This guide defines the terms *threat service* and *Data Transfer Object* as follows:

- **Threat service:** The service that you build using this guide. The Resilient platform sends new incident artifacts to your threat service for scanning.
- **Data Transfer Object (DTO):** Data Transfer Objects represent the JSON objects that transfer the data between the Resilient platform and the threat service. In this document, all JSON objects have the DTO suffix to indicate its purpose and usage.

For an example of a custom threat service, see ***to be supplied*** file.

2. Authentication and Rescans

The threat service can optionally support basic authentication to restrict access. If the credentials are provided when creating the threat service in the Resilient platform, the platform sends the credentials with each request using basic authentication scheme as defined in RFC 2617 section 2.

The Resilient platform rescans active incidents' artifacts periodically, and resubmits the artifacts using the Scan Artifact endpoint.

3. REST Endpoints

The threat service shall implement the following two REST endpoints. The tilde (~) represents the root of the endpoint (e.g., https://internal.companyxyz.com/it/threatservice).

It is recommended that the REST endpoints use SSL to ensure privacy. The Resilient platform can accept an HTTP or HTTPS URL as the root.

3.1. Scan Artifact Endpoint

Endpoint: ~/

Method: POST

Request content type: `application/json`

Request body: ThreatService`ArtifactDTO`

Response content type: `application/json`

Response body: `ResponseDTO`

The Scan Artifact endpoint is the primary method for the Resilient platform to send artifacts to the threat service. When an artifact is added, the Resilient platform connects to this endpoint with a multi-part POST, which has an **artifact** entity and an optional **file** entity.

The artifact entity has a content type of **application/json**. The value is a ThreatServiceArtifactDTO JSON object that describes the artifact. If the artifact is a file and the threat service has requested it (see Query Capabilities Endpoint), the POST would also contain a second entity named file with the type **application/octet-stream**. The value is the raw file content.

The threat service shall perform threat intelligence operations on the artifact and then return a response as specified in the Responses section of this document.

It is important that the threat service minimize the response time for each request. If a response cannot be fulfilled in no more than a few seconds, the threat service should respond with a 303 HTTP status code so that the Resilient platform tries again later. The threat service must assign an ID in the ResponseDTO object, which is used by the platform when invoking the Retrieve Artifact Result endpoint to retrieve the results for the specified artifact.

3.2. Retrieve Artifact Result Endpoint

Endpoint: ~/<id>

Method: GET

Response content type: application/json

Response: ResponseDTO

When the threat intelligence operation cannot be completed for a given artifact, the Resilient platform connects to this endpoint to retrieve the pending result for the artifact identified by **id**. The id is provided by the threat service in the Scan Artifact request.

In response to the request, if the result for the specified artifact is available, then it is returned in the ResponseDTO object. If the Resilient platform needs to wait and retry, the threat service must respond with another 303 HTTP status code, with the ResponseDTO object's id property populated.

3.3. Query Capabilities Endpoint (Optional)

Endpoint: ~/

Method: OPTIONS

Response content type: application/json

Response: ThreatServiceOptionsDTO

The Resilient platform queries this endpoint to obtain the threat service's capabilities. This endpoint is optional. If unimplemented, the Resilient platform assumes the threat service supports only the default behavior, which currently means the threat service does not support file uploads.

If the threat service can process artifact files, this endpoint must be implemented and the ThreatServiceOptionsDTO **upload_file** property must be true.

4. Responses

The status codes are conveyed using HTTP status code in the response header. The Resilient platform responds to the status code ranges as follows:

- 200 - 299: Request is successfully completed.
- 300 - 399: Request is partially completed. The Resilient platform makes at least one additional request to retrieve results.
- 400 - 499: Invalid requests. The Resilient platform does not query the artifact again.
- 500 - 599: Server error. The Resilient platform attempts to send the artifact periodically.

4.1. 200 - 299: OK

The operation has completed successfully and fully, with the threat service returning the full result set for the request. After receiving the 2xx status code, the Resilient platform does not query for this artifact until the next rescan.

- **Hit:** If the threat service finds one or more matches for the artifact, then the threat service shall return a ResponseDTO object, with information about each hit stored in the hits property.
- **No Hit**: If the artifact has no hits, then the threat service shall return an empty ResponseDTO object.

If the result set is incomplete (i.e., not all data is available), then the threat service must return 3xx instead of 2xx.

4.2. 300 - 399: Retry

If all or some of the data is unavailable to determine the status of the artifact, the threat service shall return an HTTP status code of 3xx. The id property in the ResponseDTO object must be specified. The Resilient platform accesses the Retrieve Artifact Result endpoint in conjunction with the id to obtain the results after the lesser of retry_secs or 5 seconds.

Optionally, the threat service can populate the **hits** property with available data so that the user can see the partial result immediately.

4.3. 400 - 499: Client error

These status codes indicate error(s) in the request. The Resilient platform does not retry sending of the artifact again.

If the supplied authorization is missing or incorrect, the threat service shall return the 401 status code. The Resilient platform disables the threat service and stops submitting artifacts to the threat service until it has the correct authorization.

4.4. 500 - 599: Server Error

If the threat service encounters an unhandled error, it shall return an HTTP status code of 5xx. The Resilient platform retries the request periodically.

5. Data Structures

The following sections describe the various Data transfer Objects and artifacts.

5.1. DTOs

ThreatServiceArtifactDTO

Property	Type	Description
type	string	Artifact type. See the Artifact Types section of this document for a list and description of supported artifact types.
value	number | string | object	Artifact value

ResponseDTO

Property	Type	Description
id	string	Unique identifier for the artifact. The id is used in subsequent requests to retrieve information about the artifact.
retry_secs	number (optional)	If the results are not immediately available, retry_secs specifies the number of seconds the platform should wait before contacting the threat service for the results. The default value is 5 seconds for the initial request, 60 seconds for all subsequent requests for the same id.
hits	ArtifactHitDTO array (optional)	An array of ArtifactHitDTO objects each representing a hit.

ArtifactHitDTO

Property	Type	Description
props	ArtifactPropertyDTO array	An array of ArtifactPropertyDTO objects describing the hit. The properties are displayed in the artifact info dialog.

ArtifactPropertyDTO

Property	Type	Description
type	string	Property type. One of the following: • string • number • uri • ip • latlng The property type determines how the value is formatted. If the type is uri, the Resilient platform automatically generates a hyperlink for the property. If the uri should not be clicked, then set the type to **string** to prevent unintended clicks.
name	string	Display name of the value. Must be unique within the ArtifactHitDTO object.

value	string | number | object	Property value. If the type is latlng, the value (in degrees) should be in the format:
		`{`
		`lat: number,`
		`lng: number`
		`}`

NameValueDTO

Property	Type	Description
name	string	Property name
value	string	Property value

RegistryDTO

Property	Type	Description
key	string	Registry key (or path) to the entry
entry_name	string (optional)	Registry entry's name
entry_value	string (optional)	Registry entry's value

ThreatServiceOptionsDTO

Property	Type	Description
upload_file	boolean	Specifies whether the threat service can process uploaded artifact files. If true, the Resilient platform uploads the artifact files to the threat service. Otherwise, only the file metadata is sent.

5.2. Artifact Types

File artifact types

Name	Type	Description
file.content	raw	Contents of the file
file.name	string	File name
file.path	string	File path without the name

Email artifact types

Name	Type	Description
email	string	RFC 822 email message file
email.header	NameValueDTO	Header in the email in the form of a name/value pair as represented by the NameValueDTO type
email.header .sender_address	string	Email sender's email address
email.header.sender_name	string	Email sender's display name
email.header.to	string array	Array of recipient email addresses
email.body	string	Body of the email

Hash artifact types

Name	Type	Description
hash.md5	string	MD5
hash.sha1	string	SHA-1
hash.fuzzy	string	Malware fuzzy hash

Certificate artifact types

Name	Type	Description
cert.x509	string	X.509 certificate

Network artifact types

Name	Type	Description
net.name	string	DNS host name. Note that the name might not be fully qualified.
net.ip	string	IP v4 or v6 address
net.port	number	Network port

Name	Type	Description
net.uri	string	Universal resource identifier
net.http.request.header	NameValueDTO	HTTP request header, which contains the header name and value
net.http.response.header	NameValueDTO	HTTP response header, which contains the header name and value

Process artifact types

Name	Type	Description
process.name	string	Name of the executable

System artifact types

Name	Type	Description
system.name	string	Name of the computer system
system.mutex	string	Mutex within the computer system
system.registry	RegistryDTO	Registry value
system.service.name	string	Name of the system service
system.user.name	string	User account name
system.user.password	string	User account password