Cloud Security Alliance Europe

Star Registry Integration API

rev. 5

August 2019

Contents

1. Revision history

- October 2016: Initial version.
- August 2017: Minor cleanup.
- September 2017 (r2): Changed to an id-centric approach and added collections. Naming adjustments on the APIs described in 3.2, 3.3 and 3.4. These changes notably include:
    - The number of API calls was changed from 3 to 6: for each type of resource we added a call to get a “collection” of resources.
    - All single resources now have an **id** property.
    - Short property names where replaced by more descriptive names (e.g. **qid** was replaced by **question_id**).
    - Added some properties to allow better transition from existing legacy entries in the CSA STAR registry (e.g. **registry_entries[].asset_url**).
- October 2017 (r3): Naming adjustments to the API described in 3.6:
    - Added the missing **id** property in 3.6.
    - Renamed the list **answers[]** to **responses[]** in 3.6.
    - Renamed the property **service_name** to **name** in 3.6 to be consistent with 3.7.
    - Clarified the possible values of **responses[].answer** in 3.6.
- April 2018 (r4):
    - Added token-based authentication in Section 4,
    - Amended section 3.2, adding the following fields: “supporting_assets" and “external_url”.
    - Added a clarification on the roles of the different types of URLs accessible.
- August 2019 (r5):
    - Added method for retrieving data on the organizations within the registry.
    - Amended section 3.0 to add in the latest method.
    - Inserted the Organization profile and Organization profile collection as sections 3.4. and 3.5. Each section after this was pushed back by two to account for this change.
    - Changed all references to section 3 to match the new table of contents (old references to 3.4 became 3.6 etc.)
    - Amended examples for cloud services to account for organization_id and added additional examples for organizations.

2. Introduction

The Star Registry is a publicly available repository on Cloud Security Alliance's website, which contains assurance information voluntarily submitted by over 200 cloud providers. The Star Registry entries can be found at:

https://cloudsecurityalliance.org/star/#_registry

Currently each entry in the registry describes whether a service provider has:

- Submitted a self-assessment along with a link to the content of that self-assessment,
- Received a Star Certification,
- Received a Star Attestation,
- Received a C-Star Certification,
- Holds continuous certification.

Star Certification, C-Star and Star Attestation are all independent third party audit schemes, while the Self-assessment is based on a questionnaire called the CAIQ[1] (Consensus Assessments Initiative Questionnaire). The CAIQ is itself based on the CCM (Cloud Control Matrix), a GRC control framework specifically designed for the cloud, based on industry best practices. Most providers currently provide self-assessments as through a standardized EXCEL spreadsheet.

The Cloud Security Alliance (CSA) has recently launched a new SaaS application called STARwatch that aims to facilitate assessments of cloud services through an online version of the CAIQ. CSA is also launching an effort to better exploit all the assurance data currently contained in the Star Registry.

As part of this effort, this document proposes an API specification that will enable machine-readable access to the data currently stored in unstructured format in the Star Registry.

3. APIs

CSA has developed an API with 7 methods:

1) A method to query the type of assessments that have been performed for a specific cloud service, as described in the STAR Registry. This information should be sufficient to automatically annotate a service provider with security information.

2) A method to get a collection of pointers to all cloud services that exist in the STAR registry. Each pointer references a resource defined in point 1.

[1] https://cloudsecurityalliance.org/cai

3) A method to get a collection of pointers to all organizations that exist in the STAR registry. Each pointer references a resource defined in point 2.

4) A method to query the structure and content of a particular version of the CAIQ as defined by CSA, including the description of all domains, controls and questions.

5) A method to get a collection of pointers to all versions of the CAIQ, which are referenced in the STAR registry. Each pointer references a resource defined in point 4.

6) A method to query the responses provided by a specific provider in the context of a CAIQ self-assessment. Each response is either “yes”, “no” or “na” (not applicable) and is accompanied with an optional textual comment.

7) A method to get a collection of pointers to all CAIQ questionnaire self-assessments. Each pointer references a resource defined in point 6.

Methods (4) and (6) can be combined to reconstruct a full self-assessment that includes both CAIQ questions and their answers.

3.1.Conventions used in the API description

The provided API is based on the REST paradigm and uses JSON. The HTTP content type of all responses will be set to *application/json*.

Each API request URL description is formed with an HTTP method (here GET in all 3 cases) followed by a relative path to an API base URL. As such, if the API base URL is *https://star.watch/* and if the specified relative path is */api/v1/registry/cloud_services/42*, the full query would be sent to the URL *https://star.registry/api/v1/registry/cloud_services/42*.

Parameters in request URLs will be denoted by a symbol preceded by ‘:’ (e.g. “:serviceid”), following a convention that is frequently used in the description of REST APIs.

The following additional conventions are used in the API description.

- *Data types*: In addition to traditional JSON data types, we also refer to the following types derived from a JSON string:
    - “url”: a string representing a URL (as defined in [RFC 1738]).
    - “UTC_timestamp”: a string representing a UTC timestamp as defined in ISO 8601, including the year, month, day, hour, minute and second, and ending with the ‘Z’ marker representing UTC time (e.g. 2016-09-29T13:11:43Z).
- *Creation and update*: each JSON response to a query contains a creation date (“created_at”) and a modification data (“updated_at”), unless the query applies to a collection of resources.
- *The “self” property*: each JSON response to a query contains a property called “self”, which is a full URL that points back to the queried resource, essentially repeating the requested API query URL with all parameters defined (including the base URL).

- *Array descriptors*: when an array appears in a schema description, we only represent an example of the first element in the array, followed by an ellipsis ("…"). This means that the element may appear 0 or more times.

The properties of JSON objects described in this specification are listed in a non-binding order (e.g. the specification, may list the "self" property before the "id", but an implementation may use the opposite order in a JSON resource.)

3.2.Cloud service assurance profile

Description

This GET method provides a way to query the assurance level associated with a cloud service, as stored in the CSA STAR registry.

The id of the service is specified in the query URL, and the response provides a list of all known assessments from the CSA STAR Registry for that particular service.

Currently there are mainly two types of assessments:

1) A self-assessment based on the CSA CAIQ (or the CSA CCM).

2) An independent third party assessment such as the CSA STAR Certification (derived from ISO/IEC 27001), STAR Attestation or C-STAR.

The JSON schema allows adding any future type of assessment (e.g. STAR Continuous).

Each item in the "registry_entries[]" array offers several types of optional URLs where further information can be found:

* "url" points to a machine-readable assessment as described for example in 3.6. The presence of this field indicates that the cloud service provider provided CSA with a correctly formatted assessment. When this field is absent, it indicates that no-machine readable assessment is available.

* "asset_url" provides data in non-machine readable format, typically as a ZIP file containing an XLS file or a PDF file, along with a cryptographic proof or receipt issued by CSA. Data in this file may be supplemented with additional data in the "supporting_assets" property.

* "external_url" provides pointer to an assessment that is not hosted by CSA. This case is rare and is maintained for legacy purposes.

* "specification_url" is a URI that specifies the standard or best practice used in the assessment (e.g. CAIQ version 3.0.1).

Request URL

```
GET /api/v1/registry/cloud_services/:serviceId
```

Parameters:

- **serviceId**: a numerical string uniquely identifying the service for which information is requested.

Request body

none.

Response body

```
{
    "self": <url>,
    "created_at": <UTC_timestamp>,
    "updated_at": <UTC_timestamp>,
    "id": <number>,
    "name": <string>,
    "description": <string>,
    “organization_id”: <number>,
    "registry_entries": [
        {
            "id": <number>,
            "type": <string>,
            "specification_name": <string>,
            "specification_url": <url>,
            "asset_url": <url> (optional),
            "external_url": <url> (optional)
            "supporting_assets": [
                {
                    "url": <url>,
                    "description": <string>
                },
                ...
            ] (optional),
            "url": <url> (optional)
        },
        ...
    ]
}
```

Property	Description
self	See 3.1.
created_at	See 3.1. (e.g. "*2016-09-27T14:07:18Z*")
updated_at	See 3.1.
id	This will have the same value as the **:serviceId** parameter in the request URL.
name	The textual name of the service (e.g. “Azure”)
description	Textual description of the service as provided by the service provider.
organization_id	A unique identifier of the organization for the cloud service.
registry_entries[]	List of registry entries for the service provider
registry_entries[].id	A unique identifier of the registry entry.

registry_entries[].type	The type of assessment as displayed in the STAR registry: • "*SelfAssessment*" for a CAIQ assessment, • "*Certification*" for a STAR Certification, • "*Attestation*" for a STAR attestation.
registry_entries[].specification_name	The name of the reference standard or best practices used in the assessment. (e.g. "*Consensus Assessment Questionnaire v3.0.1*")
registry_entries[].specification_url	A unique URL identifying the reference standard or best practices used in the assessment. Two distinct versions of the CAIQ will use a different URL.
registry_entries[].asset_url (Optional)	A URL pointing to a non-machine readable version of the assessment, if it exists. This is typically a file (XLS, ZIP, PDF, …). For CAIQ assessments, this URL is designed to support "legacy" assessments that have not yet been translated to a machine readable-version. This property may be absent in the case where no asset is defined.
registry_entries[].external_url (optional)	A URL pointing to an externally hosted assessment or webpage describing the assessment. This field is maintained for legacy purposes in some rare cases and should not be considered as reliable source of data.
registry_entries[].supporting_assets[] **(optional)**	A list of additional documents that complement the data provided in asset_url. This could be for example a scanned PDF of a certificate.
registry_entries[].supporting_assets[].url	A URL pointing to a supporting asset.
registry_entries[].supporting_assets[].description	A textual description of the supporting asset.
registry_entries[].url **(Optional)**	A URL pointing to a location where a machine-readable version of the assessment can be found. In the case of CAIQ, this points to a URL as described in section 3.6 with a machine-readable version of the answers provided by the service provider. This property may be absent in no machine readable version of the assessment is available.

Error codes

404: The service was not found in the registry.

3.3.Cloud service assurance profile collection

Description

This GET method provides a way to get a collection of pointers to all cloud services referenced in the CSA STAR registry.

Request URL

```
GET /api/v1/registry/cloud_services
```

Parameters:

none.

Request body

none.

Response body

```
{
    "self": <url>,
    "cloud_services": [
        {
            "id": <string>,
            "name": <string>,
            "url": <url>,
            "created_at": <UTC_timestamp>,
            "updated_at": <UTC_timestamp>
        },
        ...
    ]
}
```

Property	Description
self	See 3.1.
cloud_services[]	List of cloud services
cloud_services[].id	The unique numerical identifier of a cloud service in the STAR registry.
cloud_services[].name	The textual name of the service (e.g. “Azure”).
cloud_services[].url	A unique URL pointing to a cloud service description as specified in section 3.2.
cloud_services[].created_at	See 3.1. (e.g. "*2016-09-27T14:07:18Z*")

cloud_services[].updated_at	See 3.1.

Error codes

None.

3.4.Organization profile

This GET method provides a way to query information with regard to an Organization, as stored in the CSA STAR registry.

The id of the organization is specified in the query URL, and the response provides a list of all known cloud services from the CSA STAR Registry for that particular organization.

Request URL

```
GET /api/v1/registry/organizations/:organizationId
```

Parameters:

- **organizationId**: a numerical string uniquely identifying the organization for which information is requested.

Request body

none.

Response body

```
{
    "id": <number>,
    "name": <string>,
    "self": <url>,
    "description": <string>,
    “website”: <string>,
    "created_at": <UTC_timestamp>,
    "updated_at": <UTC_timestamp>,
    “cloud_services": [
        {
            "id": <number>,
            "name": <string>,
            "url": <url>,
            "created_at": <UTC_timestamp>,
            "updated_at": <UTC_timestamp>
        },
        ...
    ]
}
```

Property	Description
self	See 3.1.
created_at	See 3.1. (e.g. "*2016-09-27T14:07:18Z*")
updated_at	See 3.1.
id	This will have the same value as the **:organizationId** parameter in the request URL.
name	The textual name of the organization (e.g. “Microsoft”)
description	Textual description of the organization as provided by the organization.
website	Textual url for the organization website as provided by the organization.
cloud_services[]	Cloud services associated with the organization on the STAR registry.
cloud_services[].id	A unique identifier of the cloud service.
cloud_services[].name	The name of the cloud service.
cloud_services[].url	A unique URL pointing to a cloud service description as specified in section 3.2.
cloud_services[].created_at	See 3.1. (e.g. "*2016-09-27T14:07:18Z*")
cloud_services[].updated_at	See 3.1.

Error codes

404: The service was not found in the registry.

3.5.Organization profile collection

Description

This GET method provides a way to get a collection of pointers to all organizations referenced in the CSA STAR registry.

Request URL

```
GET /api/v1/registry/organizations
```

Parameters:

none.

Request body

none.

Response body

```
{
    "self": <url>,
    "organizations": [
        {
            "id": <string>,
            "name": <string>,
            "url": <url>,
            "created_at": <UTC_timestamp>,
            "updated_at": <UTC_timestamp>
        },
        ...
    ]
}
```

Property	Description
self	See 3.1.
organizations[]	List of organizations
organizations[].id	The unique numerical identifier of an organization in the STAR registry.
organizations[].name	The textual name of the organization (e.g. “Azure”).
organizations[].url	A unique URL pointing to an organization description as specified in section 3.4.
organizations[].created_at	See 3.1. (e.g. "*2016-09-27T14:07:18Z*")
organizations[].updated_at	See 3.1.

Error codes

None.

3.6.CAIQ template description

Description

This GET method provides a way to retrieve a template describing the structure of a CAIQ based self-assessment, as used in StarWatch. By definition, all CAIQ assessments conducted with the same version of the CAIQ use the same template, with the same questions.

By combining this generic template with the answers provided for a specific service (see 3.8.), it is possible to create a full description of a CAIQ assessment, combing both questions and answers.

Request URL

```
GET /api/v1/registry/caiq_templates/:templateId
```

Parameters:

- **templateId**: a numerical string uniquely identifying the CAIQ reference questionnaire requested.

Request body

none.

Response body

```
{
    "self": <url>,
    "created_at": <UTC_timestamp>,
    "updated_at": <UTC_timestamp>,
    "id": <string>
    "template_version": <string>,
    "specification_name": <string>,
    "specification_url": <string>,
    "domains": [
        {
            "domain_id": <string>,
            "title": <string>,
            "controls": [
                {
                    "control_id": <string>,
                    "title": <string>,
                    "description": <string>,
                    "questions": [
                        {
                            "question_id": <string>,
                            "description": <string>,
                        },
                        ...
                    ]
                },
                ...
            ]
        },
        ...
    ]
}
```

Property	Description
self	See 3.1.
created_at	See 3.1. (e.g. "*2016-09-27T14:07:18Z*")
updated_at	See 3.1.
id	This will have the same value as the **:templateId** parameter in the request URL.
template_version	The version of the template used (e.g. "*1.0*"). This is to account for potential future evolutions of the questionnaire format.
specification_name	The name of the reference standard or best practices described in the template. (e.g. "*Consensus Assessment Questionnaire v3.0.1*")

specification_url	A unique URL identifying the reference standard or best practices described in the template.
domains[]	A list of objects, each representing a CAIQ/CCM domain. In version 3.0.1 of the CAIQ there are 16 domains.
domains[].domain_id	Domain identifier as defined in CAIQ/CCM (e.g. "*AIS*"). In CAIQ 3.0.1 this is identified as "did".
domains[].title	Domain description (e.g. "*Application & Interface Security*")
domains[].controls[]	A list of objects, each representing a CAIQ/CCM control group within a domain.
domains[].controls[].control_id	Control group identifier as defined in CAIQ/CCM (e.g. "*AIS-01*"). In CAIQ 3.0.1 this is identified as "cgid".
domains[].controls[].title	Control group title (e.g. "*Application security*").
domains[].controls[].description	Control group description as defined in CAIQ/CCM (e.g. "*Applications and programming interfaces (APIs) shall be designed, developed, [...]*").
domains[].controls[].questions[]	A list of objects, each representing a CAIQ question.
domains[].controls[].questions[].question_id	The CAIQ question identifier (e.g. "*AIS-01.1*"). In CAIQ 3.0.1 this is identified as "cid".
domains[].controls[].questions[].description	CAIQ question description (e.g. "*Do you use industry standards (Build Security in Maturity Model) [...]* ").

Error codes

404: The requested CAIQ does not exist.

3.7.CAIQ template collection

Description

This GET method provides a way to get a collection of pointers to all CAIQ versions referenced in the CSA STAR registry.

Request URL

```
GET /api/v1/registry/caiq_templates
```

Parameters:

none.

Request body

none.

Response body

```
{
    "self": <url>,
    "caiq_templates": [
        {
            "id": <string>,
            "name": <string>,
            "url": <url>,
            "created_at": <UTC_timestamp>,
            "updated_at": <UTC_timestamp>
        },
        ...
    ]
}
```

Property	Description
self	See 3.1.
caiq_templates[]	List of CAIQ questionnaire templates.
caiq_templates [].id	The unique numerical identifier of a CAIQ questionnaire template in the STAR registry. Each version of the CAIQ will have a different id (e.g. CAIQ 3.0.1 will have id=1, CAIQ 3.0.2 will have id=2, …)
caiq_templates[].name	The textual name of the CAIQ template (e.g. “CAIQ 3.0.1”).
caiq_templates[].url	A unique URL pointing to a CAIQ template description as specified in section 3.4.
caiq_templates[].created_at	See 3.1. (e.g. "*2016-09-27T14:07:18Z*")
caiq_templates[].updated_at	See 3.1.

Error codes

None.

3.8.CAIQ assessment

Description

This GET method enables to retrieve the answers provided by service provider to the CAIQ questionnaire, in the context of a self-assessment.

Request URL

```
GET /api/v1/registry/caiq_assessments/:assessmentId
```

Parameters:

- **assessmentId**: : a numerical string uniquely identifying a CAIQ assessment.

Request body

none.

Response body

```
{
    "self": <url>,
    "created_at": <UTC_timestamp>,
    "updated_at": <UTC_timestamp>,
    "id": <string>,
    "template_url": <url>,
    "service_name": <string>,
    "description": <string>,
    "responses": [
        {
            "question_id": <string>,
            "answer": <"yes", "no", or "na">,
            "comment": <string>
        },
        ...
    ]
}
```

Property	Description
self	See 3.1.
created_at	See 3.1. (e.g. "*2016-09-27T14:07:18Z*")
updated_at	See 3.1.
id	This will have the same value as the **:assessmentId** parameter in the request URL.
template_url	This URL points to machine-readable data of the questionnaire or control framework used in the assessment. In the case of CAIQ, this points to a URL as described in section 3.6. (e.g. http://star.watch/api/v1/registry/caiq_templates/42)

name	The name/title of the assessment. This is usually the name of the service (or organization) that is being assessed.
description	Free text that accompanies the assessment (e.g. *"This document provides customers a straightforward process for evaluating Azure's [...]"*).
responses[]	
responses[].question_id	CAIQ question identifier (e.g. "AIS-01.1"), which can be matched with **domains[].controls[].questions[].question_id** defined in the template in 3.6. (note: In the CAIQ 3.0.1 specification this is identified as "cid").
responses[].answer	Answer provided to the CAIQ question, which must be either "Y*es*", "*No*" or "Not Applicable".
responses[].comment	Free text comment provided by the auditor or service provider in relation with the answer.

Error codes

404: The requested service assessment does not exist.

3.9. CAIQ assessment collection

Description

This GET method provides a way to get a collection of pointers to all CAIQ answers referenced in the CSA STAR registry.

Request URL

```
GET /api/v1/registry/caiq_assessments
```

Parameters:

none.

Request body

none.

Response body

```
{
    "self": <url>,
    "caiq_assessments": [
```

```
        {
            "id": <string>,
            "name": <string>,
            "url": <url>
        },
        ...
    ]
}
```

Property	Description
self	See 3.1.
caiq_assessments[]	List of CAIQ questionnaire responses.
caiq_assessments[].id	The unique numerical identifier of a CAIQ assessment in the STAR registry.
caiq_ assessments[].name	The textual name of the assessment (this is typically the name of the service).
caiq_ assessments[].url	A unique URL pointing to a CAIQ assessment description as specified in section 3.8.

Error codes

None.

4. Security

To access the registry APIs at https://star.watch/api/v1/registry, clients will be required to provide an API key, in order to verify that they have the right to access the APIs. This API key shall be provided with the following HTTP header in every request:

Authorization: Bearer <API_KEY>

Where API_KEY is a 20-byte random secret value, encoded in BASE64.

Each organisation accessing the API shall get a distinct API_KEY.

If a client makes a request without specifying an API key, or with an unknown API key, the server will respond with HTTP error code 401 (Unauthorized) and provide the following HTTP header in the response:

WWW-Authenticate: Bearer realm="https://star.watch/api/v1/registry"

Requests for an API key can be made by sending an email to:

starwatch-support@cloudsecurityalliance.org

Once generated, the API key will appear in the STARwatch user account of the person who requested the key. To access the key, simply log into STARwatch and click on “account” in the top right of the screen. Note that creating a STARwatch account is free of charge.

In case a user requests a new API key, we will delete the old one and generate a new one.

5. Conclusion

This document presents a new API enabling access to Star Registry information in JSON format.

Annex A: Examples

This annex provides examples of the API calls described in this document.

Most examples have been truncated for the sake of brevity.

https://star.watch/api/v1/registry/cloud_services


```
{
  "self": "https://star.watch/api/v1/registry/cloud_services",
  "cloud_services": [
    {
      "id": 1,
      "name": "InSite",
      "url": "https://star.watch/api/v1/registry/cloud_services/1",
      "created_at": "2017-10-27T18:55:02.707Z",
      "updated_at": "2017-10-27T18:55:02.707Z"
    },
    {
      "id": 24,
      "name": "Auth0",
      "url": "https://star.watch/api/v1/registry/cloud_services/24",
      "created_at": "2017-10-27T18:55:41.559Z",
      "updated_at": "2017-10-27T18:55:41.559Z"
    },
    {
      "id": 25,
      "name": "Avature",
      "url": "https://star.watch/api/v1/registry/cloud_services/25",
      "created_at": "2017-10-27T18:55:42.348Z",
      "updated_at": "2017-10-27T18:55:42.348Z"
    },
    {
      "id": 26,
      "name": "AvePoint Online Services",
      "url": "https://star.watch/api/v1/registry/cloud_services/26",
      "created_at": "2017-10-27T18:55:43.498Z",
      "updated_at": "2017-10-27T18:55:43.498Z"
    },
    {
      "id": 27,
      "name": "Axon",
      "url": "https://star.watch/api/v1/registry/cloud_services/27",
      "created_at": "2017-10-27T18:55:45.193Z",
      "updated_at": "2017-10-27T18:55:45.193Z"
    },
    {
      "id": 28,
      "name": "Behavox",
      "url": "https://star.watch/api/v1/registry/cloud_services/28",
      "created_at": "2017-10-27T18:55:48.592Z",
      "updated_at": "2017-10-27T18:55:48.592Z"
    },
    {
      "id": 29,
      "name": "BEIJING BEISEN CLOUD COMPUTING COMPANY LIMITED",
      "url": "https://star.watch/api/v1/registry/cloud_services/29",
      "created_at": "2017-10-27T18:55:49.808Z",
      "updated_at": "2017-10-27T18:55:49.808Z"
    },
    {
```

```
      "id": 30,
      "name": "BEIJING KINGSOFT CLOUD NETWORK TECHNOLOGY COMPANY LIMITED",
      "url": "https://star.watch/api/v1/registry/cloud_services/30",
      "created_at": "2017-10-27T18:55:51.606Z",
      "updated_at": "2017-10-27T18:55:51.606Z"
    }
  ]
}
```

https://star.watch/api/v1/registry/cloud_services/25


```
{
  "id": 25,
  "name": "Avature",
  "self": "https://star.watch/api/v1/registry/cloud_services/25",
  "description": "Avature is an HCM software company which employs more than 450
employees around the world and operates in six countries (USA, UK, Spain, China,
Australia and Argentina). At the moment, Avature has more than 650 customers
worldwide, including 101 of the Fortune 500, 23 of FTSE 100, the Big Four accounting
firms, 8 of the top 10 banks in the US. Our vision is to support strategic HR
initiatives by introducing a consumer web quality platform that can be customized
quickly and easily by our customers - allowing them to design and implement innovative
programs to compete for and retain talented people. We currently provide the broadest
range of recruiting solutions available from a single vendor. Avature is widely
credited for introducing CRM concepts to recruiting processes and is currently the
global leader in this category of recruiting solution.  In the last years we've
expanded our suite to include ATS, On-boarding, Employee Referral, Agency Management,
Hiring Manager, Events Management, In-Store Recruiting, Internal Mobility solutions.",
  "organization_id": 3,
  "created_at": "2017-10-27T18:55:42.348Z",
  "updated_at": "2017-10-27T18:55:42.348Z",
  "registry_entries": [
    {
      "id": 359,
      "type": "SelfAssessment",
      "specification_name": "Consensus Assessments Initiative Questionnaire v3.0.1",
      "specification_url": "https://cloudsecurityalliance.org/download/consensus-
assessments-initiative-questionnaire-v3-0-1/",
      "asset_url": "https://star.watch/en/registry/359/download_self_assessment",
      "url": "https://star.watch/api/v1/registry/caiq_assessments/359"
    }
  ]
}
```

https://star.watch/api/v1/registry/organizations


```
{
  "self": "https://star.watch/api/v1/registry/organizations",
  "organizations": [
    {
      id: 2,
      name: "411 Labs, Inc",
      url: "https://star.watch/api/v1/registry/organizations/2",
      created_at: "2017-09-13T16:51:49.000Z",
      updated_at: "2019-08-15T22:39:53.044Z"
    },
    {
      id: 3,
      name: "AC3",
      url: "https://star.watch/api/v1/registry/organizations/3",
      created_at: "2017-06-30T19:08:33.000Z",
      updated_at: "2019-08-15T22:39:53.049Z"
    },
    {
      id: 4,
      name: "Accenture Plc",
      url: "https://star.watch/api/v1/registry/organizations/4",
      created_at: "2017-07-06T23:08:29.000Z",
      updated_at: "2019-08-15T22:39:53.053Z"
    },
    {
      id: 5,
      name: "Acer CyberCenter Services Inc.",
      url: "https://star.watch/api/v1/registry/organizations/5",
      created_at: "2013-11-20T21:48:28.000Z",
      updated_at: "2019-08-15T22:39:53.056Z"
    },
    {
      id: 6,
      name: "Achievers Corporation",
      url: "https://star.watch/api/v1/registry/organizations/6",
      created_at: "2014-04-16T23:56:26.000Z",
      updated_at: "2019-08-15T22:39:53.060Z"
    }
 ]
}
```

https://star.watch/api/v1/registry/organizations/3


```
{
  id: 3,
  name: "AC3",
  self: "https://star.watch/api/v1/registry/organizations/3",
  description: "<p>AC3 is an ICT Managed Service Provider (MSP) specialising in
delivering solutions to both the public and private sectors. We combine the best
technology with the best people to deliver innovative IT solutions. We have been
designing, building and managing IT solutions since 1999.</p> <p>We believe that the
true benefit of IT is utilising it to unlock greater efficiency, so our customers can
focus on what's important to them; their business. Our key goal is to be a true
technology partner and solve once unsolvable problems. We deliver solutions across a
number of areas, including managed services and cloud hosting in our secure data
centres, professional services, procurement services and talent management.</p> <p>Our
vision is to be Australia's most dynamic technology partner and our team actively work
on achieving this through our essential behaviours of being nimble, smart and
straightforward.</p> ",
  website: "http://www.ac3.com.au",
  created_at: "2017-06-30T19:08:33.000Z",
  updated_at: "2019-08-15T22:39:53.049Z",
  cloud_services: [
    {
      id: 2,
      name: "AC3",
      url: "https://star.watch/api/v1/registry/cloud_services/2",
      created_at: "2019-08-15T22:39:25.531Z",
      updated_at: "2019-08-15T22:39:25.531Z"
    }
  ]
}
```

https://star.watch/api/v1/registry/caiq_assessments


```
{
  "self": "https://star.watch/api/v1/registry/caiq_assessments",
  "caiq_assessments": [
    {
      "id": 1,
      "name": "InSite",
      "url": "https://star.watch/api/v1/registry/caiq_assessments/1"
    },
    {
      "id": 2,
      "name": "AC3",
      "url": "https://star.watch/api/v1/registry/caiq_assessments/2"
    },
    {
      "id": 357,
      "name": "STARWatch",
      "url": "https://star.watch/api/v1/registry/caiq_assessments/357"
    },
    {
      "id": 359,
      "name": "Avature",
      "url": "https://star.watch/api/v1/registry/caiq_assessments/359"
    }
  ]
}
```

https://star.watch/api/v1/registry/caiq_assessments/359


```
{
  "id": 359,
  "self": "https://star.watch/api/v1/registry/caiq_assessments/359",
  "name": "Avature",
  "description": "",
  "created_at": "2017-10-27T20:12:06.170Z",
  "updated_at": "2017-10-27T20:18:56.941Z",
  "template_url": "https://star.watch/api/v1/registry/caiq_templates/1",
  "responses": [
    {
      "question_id": "AIS-01.1",
      "answer": "Yes",
      "comment": "Avature's security policies and controls, as well as the Software
Development Lifecycle, are in line with industry standards. Avature follows ISO 27001
and OWASP guidelines for secure development and testing."
    },
    {
      "question_id": "AIS-01.2",
      "answer": "Yes",
      "comment": "Testing process includes both automatic and manual testing.
Automated tests include a suite of over 3700 tests.\nAdditionally, regular
vulnerability scans are performed."
    },
    {
      "question_id": "AIS-01.3",
      "answer": "Yes",
      "comment": "Manual testing include code review, which is integrated as part of
Avature's SDLC."
    },
    {
      "question_id": "AIS-01.4",
      "answer": "Not Applicable",
      "comment": "Not applicable. Avature does not outsource software development."
    },
    {
      "question_id": "AIS-01.5",
      "answer": "Yes",
      "comment": "Avature's SDLC process includes automatic and manual testing, which
are performed prior to deployment to production. Any issue or security vulnerability
is assessed and treated as appropriate."
    },
    {
      "question_id": "AIS-02.1",
      "answer": "Yes",
      "comment": "Avature, in its capacity as data processor, complies with laws,
regulations and industry standard requirements regarding protection of personal data
in all countries in which the company operates. \nThe application can be configured as
instructed by the customer, who needs to define which regulations are applicable and
how to configure the system accordingly."
    },
    {
      "question_id": "AIS-02.2",
      "answer": "Yes",
      "comment": "The Avature application provides a sophisticated RBAC mechanism with
fine grain control over application features and data. Roles and permissions to each
Avature instance are defined based on customers' requirements, and documented in the
Avature system."
    },
    {
      "question_id": "AIS-03.1",
      "answer": "Yes",
```

```
      "comment": "Avature Applications validates all inputs to ensure data integrity.
In addition, application uses multiple forms of referential integrity policies both in
the database layer and in the application layer."
    },
    {
      "question_id": "AIS-04.1",
      "answer": "Yes",
      "comment": "Avature's security program is defined by its policies and security
controls, which are based on best practices and industry standards (mainly ISO
27001/2). Security controls are designed to provide confidentiality (e.g., encryption
in transit and at rest, access controls), integrity (e.g., backup, input control) and
availability (e.g., redundancy, replication)."
    },
    {
      "question_id": "AAC-01.1",
      "answer": "Yes",
      "comment": "Internal audits are performed based on ISO 27001 in alignment with
ISO 19011 audit guidelines. Avature IT Audit Policy provides guidelines to prevent
audit activities from disrupting business processes."
    },
    {
      "question_id": "AAC-03.1",
      "answer": "Yes",
      "comment": "Avature instances are separated from each other. Users from one
instance cannot access other instances. Each instance has its own database and the
data base cannot be accessed by any other instance."
    },
    {
      "question_id": "AAC-03.2",
      "answer": "Yes",
      "comment": "Avature can recover data for a specific customer."
    },
    {
      "question_id": "AAC-03.3",
      "answer": "Yes",
      "comment": "Different hosting regions are available for customers to choose
from."
    },
    {
      "question_id": "AAC-03.4",
      "answer": "Yes",
      "comment": "Avature's control framework is designed to capture requirements from
all interested parties. Changes in legislation and regulations are reviewed to
determine the impact. Avature constantly improves its security program to provide up
to date industry standard controls."
    },
    {
      "question_id": "TVM-03.2",
      "answer": "Yes",
      "comment": "Avature uses JavaScript code, which is subject to the Software
Development Lifecycle in line with Avature policies. All code goes through the SDLC
workflow, which includes automatic and manual testing and staged rollout."
    }
  ]
}
```

https://star.watch/api/v1/registry/caiq_templates


```
{
  "self": "https://star.watch/api/v1/registry/caiq_templates",
  "caiq_templates": [
    {
      "id": 1,
      "name": "Consensus Assessments Initiative Questionnaire v3.0.1",
      "url": "https://star.watch/api/v1/registry/caiq_templates/1",
      "created_at": "2017-10-27T18:54:59.024Z",
      "updated_at": "2017-10-27T18:55:01.947Z"
    }
  ]
}
```

https://star.watch/api/v1/registry/caiq_templates/1


```
{
  "id": 1,
  "self": "https://star.watch/api/v1/registry/caiq_templates/1",
  "created_at": "2017-10-27T18:54:59.024Z",
  "updated_at": "2017-10-27T18:55:01.947Z",
  "template_version": "3.0.1",
  "specification_name": "Consensus Assessments Initiative Questionnaire v3.0.1",
  "specification_url": "https://cloudsecurityalliance.org/download/consensus-
assessments-initiative-questionnaire-v3-0-1/",
  "domains": [
    {
      "domain_id": "AIS",
      "title": "Application and Interface Security",
      "controls": [
        {
          "control_id": "AIS-01",
          "title": "Application Security",
          "description": "Applications and programming interfaces (APIs) shall be
designed, developed, deployed, and tested in accordance with leading industry
standards (e.g., OWASP for web applications) and adhere to applicable legal,
statutory, or regulatory compliance obligations.",
          "questions": [
            {
              "question_id": "AIS-01.1",
              "description": "Do you use industry standards (Build Security in
Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider
Framework, NIST, etc.) to build in security for your Systems/Software Development
Lifecycle (SDLC)?"
            },
            {
              "question_id": "AIS-01.2",
              "description": "Do you use an automated source code analysis tool to
detect security defects in code prior to production?"
            },
            {
              "question_id": "AIS-01.3",
              "description": "Do you use manual source-code analysis to detect
security defects in code prior to production?"
            },
            {
              "question_id": "AIS-01.4",
              "description": "Do you verify that all of your software suppliers adhere
to industry standards for Systems/Software Development Lifecycle (SDLC) security?"
            },
            {
              "question_id": "AIS-01.5",
              "description": "(SaaS only) Do you review your applications for security
vulnerabilities and address any issues prior to deployment to production?"
            }
          ]
        },
        {
          "control_id": "AIS-02",
          "title": "Customer Access Requirements",
          "description": "Prior to granting customers access to data, assets, and
information systems, identified security, contractual, and regulatory requirements for
customer access shall be addressed. ",
          "questions": [
            {
              "question_id": "AIS-02.1",
```

```
              "description": "Are all identified security, contractual, and regulatory
requirements for customer access contractually addressed and remediated prior to
granting customers access to data, assets, and information systems?"
            },
            {
              "question_id": "AIS-02.2",
              "description": "Are all requirements and trust levels for customers'
access defined and documented?"
            }
          ]
        },
        {
          "control_id": "AIS-03",
          "title": "Data Integrity",
          "description": "Data input and output integrity routines (i.e.,
reconciliation and edit checks) shall be implemented for application interfaces and
databases to prevent manual or systematic processing errors, corruption of data, or
misuse.",
          "questions": [
            {
              "question_id": "AIS-03.1",
              "description": "Are data input and output integrity routines (i.e.,
reconciliation and edit checks) implemented for application interfaces and databases
to prevent manual or systematic processing errors or corruption of data?"
            }
          ]
        },
        {
          "control_id": "AIS-04",
          "title": "Data Security / Integrity",
          "description": "Policies and procedures shall be established and maintained
in support of data security to include (confidentiality, integrity, and availability)
across multiple system interfaces, jurisdictions, and business functions to prevent
improper disclosure, alternation, or destruction.",
          "questions": [
            {
              "question_id": "AIS-04.1",
              "description": "Is your Data Security Architecture designed using an
industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard,
FedRAMP, CAESARS)?"
            }
          ]
        }
      ]
    },
    {
      "domain_id": "AAC",
      "title": "Audit Assurance and Compliance",
      "controls": [
        {
          "control_id": "AAC-01",
          "title": "Audit Planning",
          "description": "Audit plans shall be developed and maintained to address
business process disruptions. Auditing plans shall focus on reviewing the
effectiveness of the implementation of security operations. All audit activities must
be agreed upon prior to executing any audits.",
          "questions": [
            {
              "question_id": "AAC-01.1",
              "description": "Do you produce audit assertions using a structured,
industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX,
GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?"
            }
          ]
        },
        {
          "control_id": "AAC-02",
```

```
          "title": "Independent Audits",
          "description": "Independent reviews and assessments shall be performed at
least annually to ensure that the organization addresses nonconformities of
established policies, standards, procedures, and compliance obligations.",
          "questions": [
            {
              "question_id": "AAC-02.1",
              "description": "Do you allow tenants to view your SOC2/ISO 27001 or
similar third-party audit or certification reports?"
            },
            {
              "question_id": "AAC-02.2",
              "description": "Do you conduct network penetration tests of your cloud
service infrastructure regularly as prescribed by industry best practices and
guidance?"
            },
            {
              "question_id": "AAC-02.3",
              "description": "Do you conduct application penetration tests of your
cloud infrastructure regularly as prescribed by industry best practices and guidance?"
            },
            {
              "question_id": "AAC-02.4",
              "description": "Do you conduct internal audits regularly as prescribed
by industry best practices and guidance?"
            },
            {
              "question_id": "AAC-02.5",
              "description": "Do you conduct external audits regularly as prescribed
by industry best practices and guidance?"
            },
            {
              "question_id": "AAC-02.6",
              "description": "Are the results of the penetration tests available to
tenants at their request?"
            },
            {
              "question_id": "AAC-02.7",
              "description": "Are the results of internal and external audits
available to tenants at their request?"
            },
            {
              "question_id": "AAC-02.8",
              "description": "Do you have an internal audit program that allows for
cross-functional audit of assessments?"
            }
          ]
        },
        {
          "control_id": "AAC-03",
          "title": "Information System Regulatory Mapping",
          "description": "Organizations shall create and maintain a control framework
which captures standards, regulatory, legal, and statutory requirements relevant for
their business needs. The control framework shall be reviewed at least annually to
ensure changes that could affect the business processes are reflected.",
          "questions": [
            {
              "question_id": "AAC-03.1",
              "description": "Do you have the ability to logically segment or encrypt
customer data such that data may be produced for a single tenant only, without
inadvertently accessing another tenant's data?"
            },
            {
              "question_id": "AAC-03.2",
              "description": "Do you have the capability to recover data for a
specific customer in the case of a failure or data loss?"
            },
```

```
            {
              "question_id": "AAC-03.3",
              "description": "Do you have the capability to restrict the storage of
customer data to specific countries or geographic locations?"
            },
            {
              "question_id": "AAC-03.4",
              "description": "Do you have a program in place that includes the ability
to monitor changes to the regulatory requirements in relevant jurisdictions, adjust
your security program for changes to legal requirements, and ensure compliance with
relevant regulatory requirements?"
            }
          ]
        }
      ]
    }
  ]
}
```

References

1. CSA Cloud Control Matrix. https://cloudsecurityalliance.org/group/cloud-controls-matrix/

2. CSA Consensus Assessment Initiative Questionnaire. https://cloudsecurityalliance.org/group/consensus-assessments/

3. G. Klyne, C. Newman, *RFC 3339: Date and Time on the Internet: Timestamps* Internet Engineering Task Force (IETF), July 2002.

4. T. Berners-Lee, R. Fielding, L. Masinter. *RFC 3986: Uniform Resource Identifier (URI): Generic Syntax*. The Internet Engineering Task Force, January 2005.

5. ECMA-404, European Computer Manufacturers Association, *The JSON Data Interchange Format*, Edition 1, October 2013.