API Network Diagram

MITRE

April 20, 2022

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

MITRE Segment Agenda

- Discuss Existing CWE Infrastructure
- Outline broad options for the API backing
- Requests for comments on alpha testing design choices
- Our desire for specification of required capabilities

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Current CWE/CAPEC Pipeline

- **Users/team submit entries/changes, leading to edits of individual CWE/CAPECs**
- **Commit individual CWE/CAPEC XML files to MITRE internal Gitlab**
- **Collate and process individual CWE/CAPEC's into the main XML file**
  - https://cwe.mitre.org/data/downloads.html for compressed collations
- **Generate HTML pages from CWE/CAPEC XML data through XSL transforms**
- **Reflect statically generated HTML to public web server**

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

CWE/CAPEC Schema

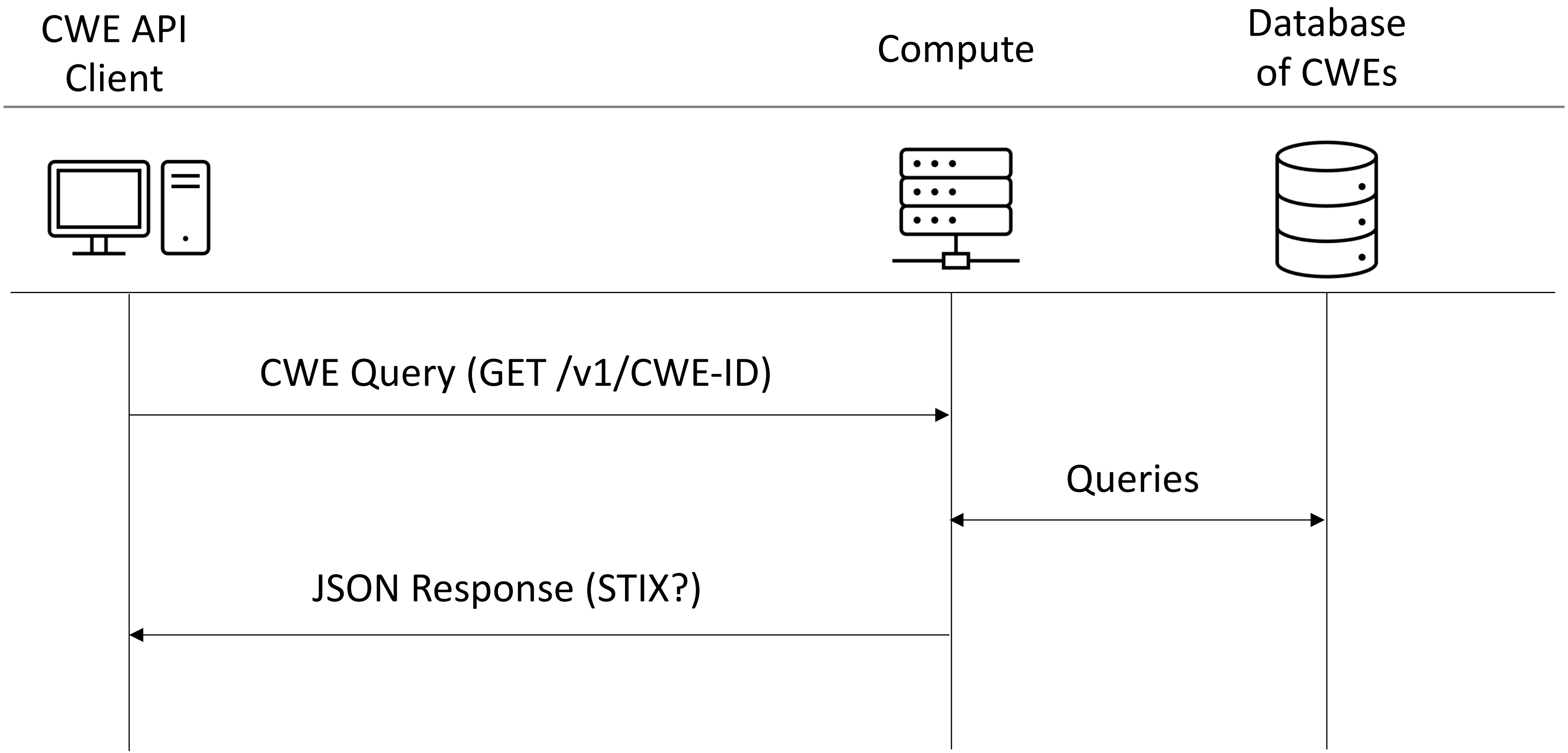
- **This schema version number refers to the XML schema (not the CWE/CAPEC version)**
- **Changes in field names, possible options for enumerations, etc.**
- **Should we match version numbers in API?**

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Current List of Requests
(Accelera: Brent Sherman, Kathy Herring Hayashi)

	API/Get Request	Example
1	List of all matching categories and view (HW)	Members of the category – debugging, security flow issues (e.g. 1196)
2	List of all matching specific field(s)	
3	Record of parent CWE	CHILD-ID = 1195 and return PARENT_ID(s)
4	Meta data of all possible values for CWE field	For collection building, sorting (e.g. 8 possible technologies)
5	Return entry Version and Timestamp	Request current version
6	List of entries modified between version releases	startver=1; endver=2
7	Delta between Entry Dates	Startdate=01/22/22; enddate=today

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.



CWE API Client

Compute

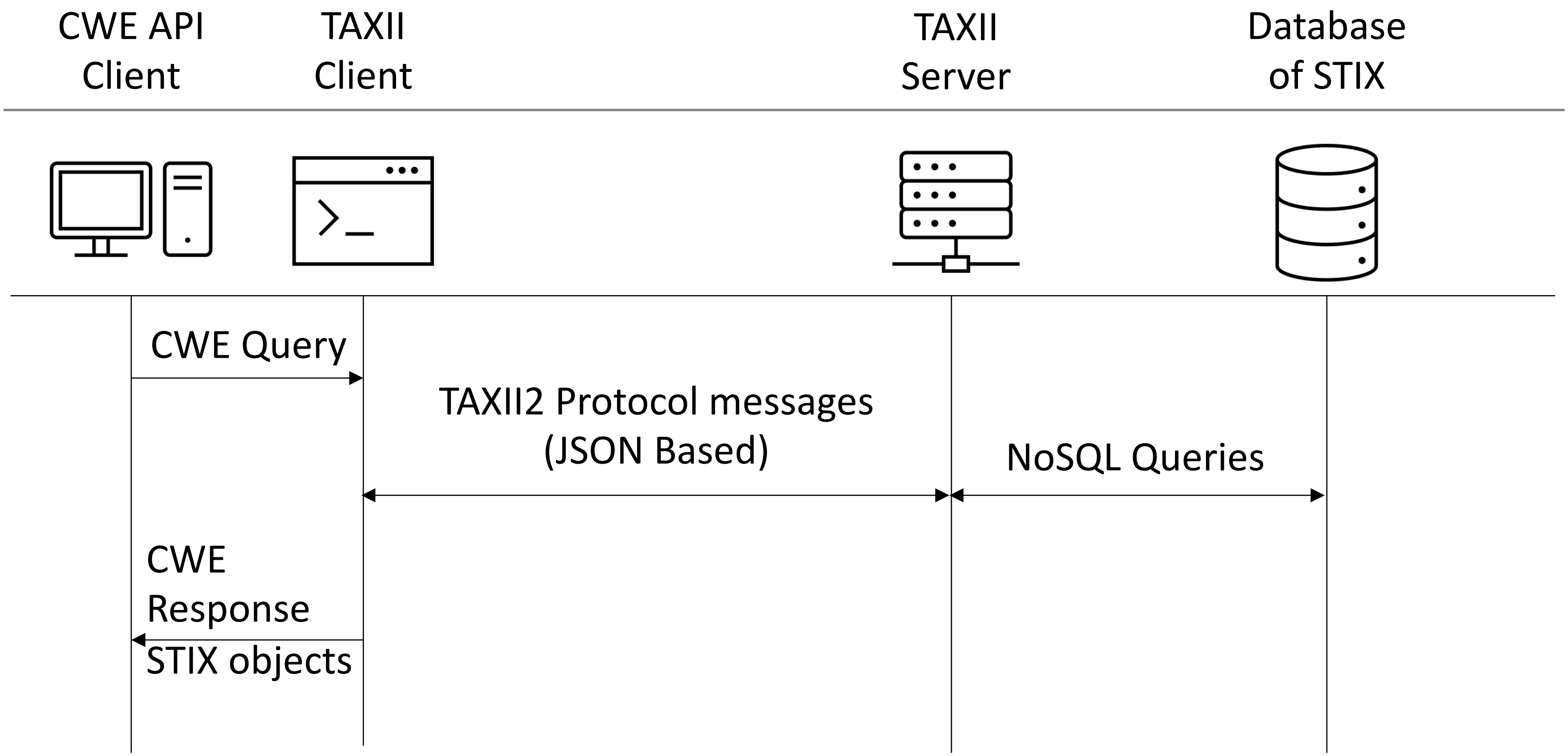
Database of CWEs

CWE Query (GET /v1/CWE-ID)

Queries

JSON Response (STIX?)

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.



CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Client side library for querying

- **To what extent are people willing to process CWE/CAPEC through an open-source library we develop?**
  - Distribute library which leverages the API or can operate on CWE/CAPEC XML
  - negatives being which language to use and maintenance

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Potential Simplification for v1

- **Deploy baseline API**
  - GET /cwe/id -> json of cwe-id
  - GET /view/id -> json of [cwe-id, cwe-id, cwe-id] if all in view
  - GET /all -> all CWEs with reduced set of fields
- **Implications:**
  - no search functionality to start with
  - standard API design considerations and performance not accounted for
  - Can be deployed now in an “as-is” state through the current CWE website
    - This server doesn’t have a ton of resources so it would be untenable in the long run

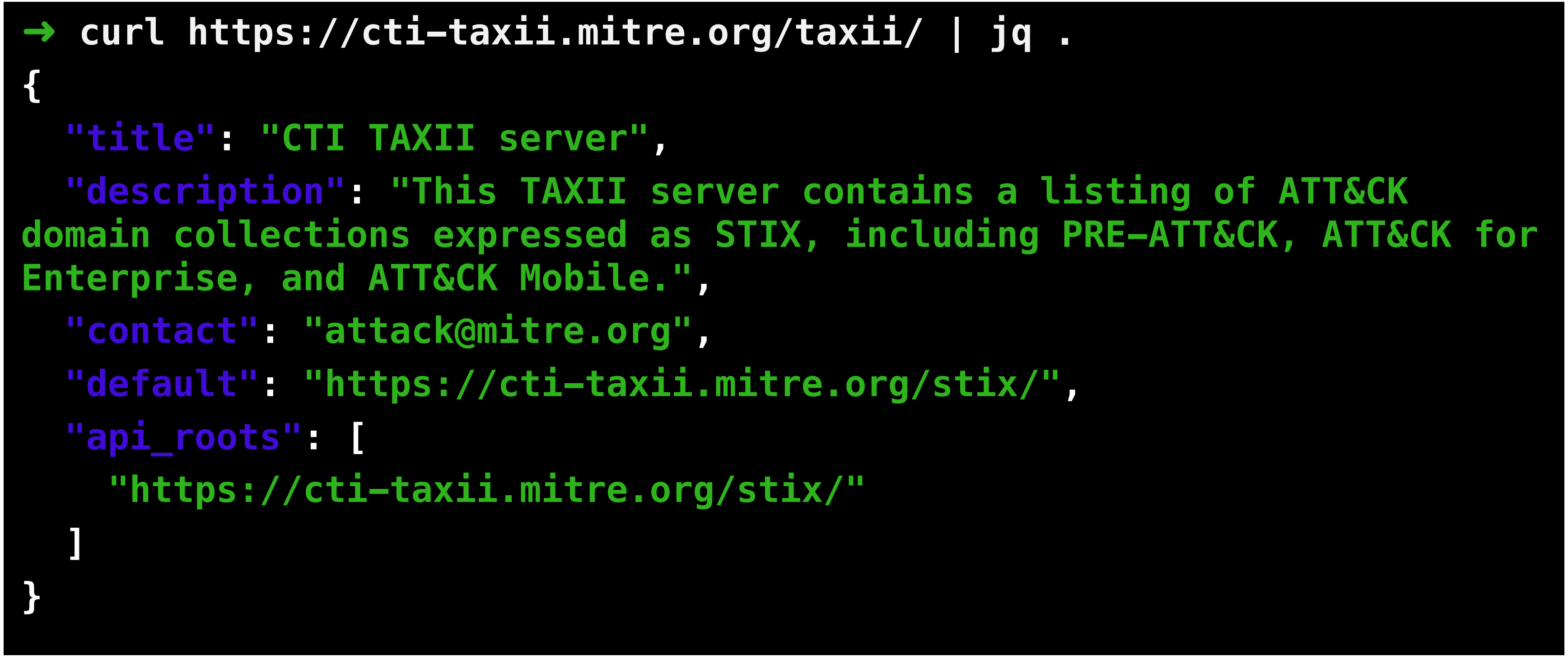
CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

TAXII Starting Point (TAXII API Endpoints)

URL	Methods	Resource Type
/taxii2/	GET	discovery
{api-root}/	GET	api
{api-root}/status/**{status-id}**/	GET	status
{api-root}/collections/	GET	collections
{api-root}/collections/**{id}**/	GET	collection
{api-root}/collections/**{id}**/manifest/	GET	manifest
{api-root}/collections/**{id}**/objects/	GET, POST	envelope
{api-root}/collections/**{id}**/objects/**{object-id}**/	GET, DELETE	envelope
{api-root}/collections/**{id}**/objects/**{object-id}**/versions/	GET	versions

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

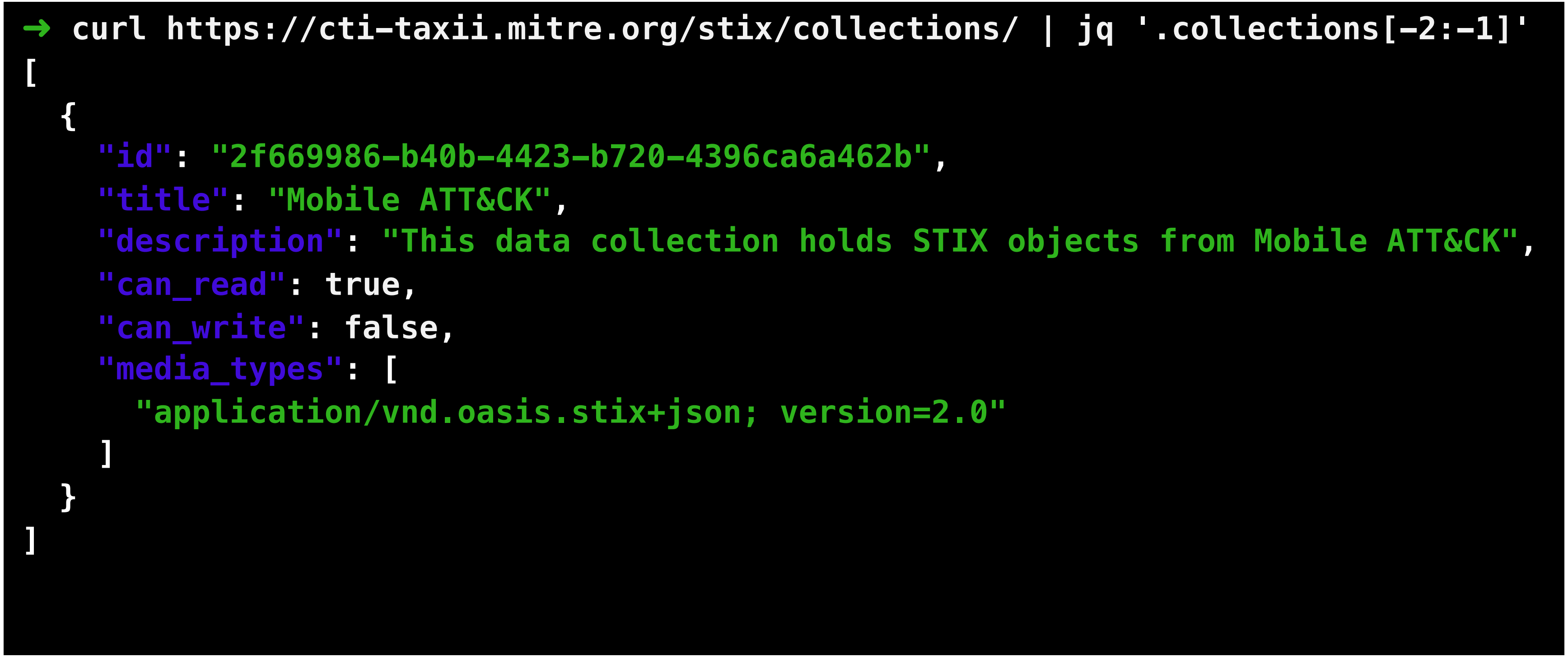
Discovery



```
→ curl https://cti-taxii.mitre.org/taxii/ | jq .
{
  "title": "CTI TAXII server",
  "description": "This TAXII server contains a listing of ATT&CK
domain collections expressed as STIX, including PRE-ATT&CK, ATT&CK for
Enterprise, and ATT&CK Mobile.",
  "contact": "attack@mitre.org",
  "default": "https://cti-taxii.mitre.org/stix/",
  "api_roots": [
    "https://cti-taxii.mitre.org/stix/"
  ]
}
```

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

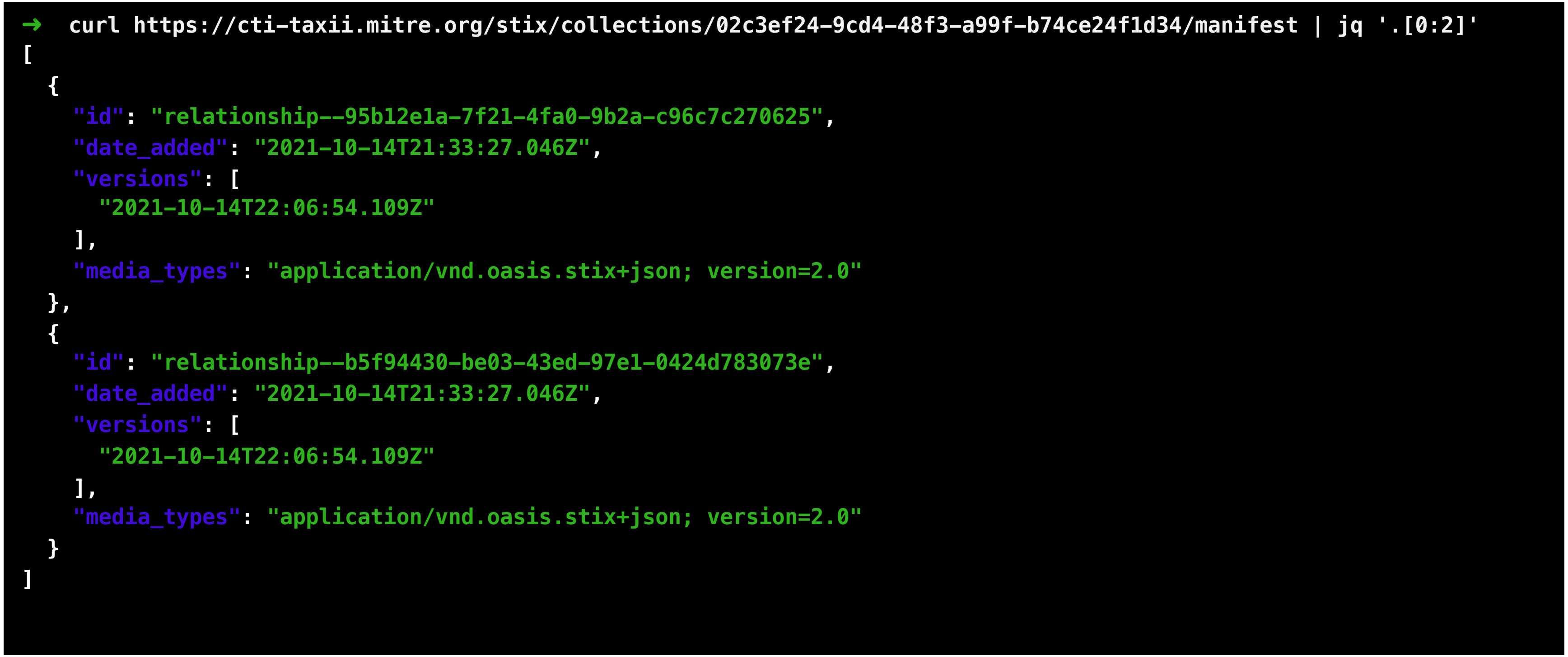
Collections



```
➜ curl https://cti-taxii.mitre.org/stix/collections/ | jq '.collections[-2:-1]'
[
  {
    "id": "2f669986-b40b-4423-b720-4396ca6a462b",
    "title": "Mobile ATT&CK",
    "description": "This data collection holds STIX objects from Mobile ATT&CK",
    "can_read": true,
    "can_write": false,
    "media_types": [
      "application/vnd.oasis.stix+json; version=2.0"
    ]
  }
]
```

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

Manifest for a Collection



```
➜  curl https://cti-taxii.mitre.org/stix/collections/02c3ef24-9cd4-48f3-a99f-b74ce24f1d34/manifest | jq '.[0:2]'
[
  {
    "id": "relationship--95b12e1a-7f21-4fa0-9b2a-c96c7c270625",
    "date_added": "2021-10-14T21:33:27.046Z",
    "versions": [
      "2021-10-14T22:06:54.109Z"
    ],
    "media_types": "application/vnd.oasis.stix+json; version=2.0"
  },
  {
    "id": "relationship--b5f94430-be03-43ed-97e1-0424d783073e",
    "date_added": "2021-10-14T21:33:27.046Z",
    "versions": [
      "2021-10-14T22:06:54.109Z"
    ],
    "media_types": "application/vnd.oasis.stix+json; version=2.0"
  }
]
```

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.

CWE@MITRE.ORG

CWE and CAPEC are sponsored by U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA). Copyright © 1999–2022, The MITRE Corporation. CWE, CAPEC, the CWE logo, and the CAPEC logo are trademarks of The MITRE Corporation.