JSON binding of IODEF

draft-ietf-mile-jsoniodef-03.txt
https://github.com/milewg/draft-ietf-mile-jsoniodef

Takeshi Takahashi, Roman Danyliw, and Mio Suzuki

Current status of the draft

1. Based on the discussion at the IETF 100 in Singapore, the draft was revised

2. We made the draft more concise. (60 pages -> 39 pages)

This draft is now much more concise than before

Table of contents (of the draft)

Volume reduced:
60 pages -> 39 pages

IODEF Data Types

IODEF Data Type	[RFC7970] Reference	JSON Data Type
INTEGER	Section 2.1	"integer" per [jsonschema]
REAL	Section 2.2	"number" per [jsonschema]
CHARACTER	Section 2.3	"string" per [jsonschema]
STRING	Section 2.3	"string" per [jsonschema]
ML_STRING	Section 2.4	see Section 2.2.1
BYTE	Section 2.5.1	"string" per [jsonschema]
BYTE[]	Section 2.5.1	"string" per [jsonschema]
HEXBIN	Section 2.5.2	"string" per [jsonschema]
HEXBIN[]	Section 2.5.2	"string" per [jsonschema]
ENUM	Section 2.6	"enum" array per [jsonschema]
DATETIME	Section 2.7	"string" per [jsonschema]
TIMEZONE	Section 2.8	"string" per [jsonschema]
PORTLIST	Section 2.9	"string" per [jsonschema]
POSTAL	Section 2.10	"string" per [jsonschema]
POSTAL_ML	Section 2.10	see ML_STRING, Section 2.2.1
PHONE	Section 2.11	"string" per [jsonschema]
EMAIL	Section 2.12	"string" per [jsonschema]
URL	Section 2.13	"string" per [jsonschema]
ID	Section 2.14	"string" per [jsonschema]
IDREF	Section 2.14	"string" per [jsonschema]
SOFTWARE	Section 2.15	see Section 2.2.2
STRUCTURED	RFC 7213	see Section 2.2.3
EXTENSION	Section 2.16	see Section 2.2.4

Figure 1

IODEF JSON Data Model

IODEF Class	Class Elements and Attribute	Corresponding Section in [RFC7970]
IODEF-Document	version lang? format-id? private-enum-name? private-enum-id? Incident+ AdditionalData*	3.1
Incident	purpose ext-purpose? status? ext-status? lang? restriction? ext-restriction? observable-id? IncidentID AlternativeID?	3.2

Mapping between JSON and XML IODEF (Sec 3.2)

1. This document treats attributes and elements of each class defined in [RFC7970] equally and is agnostic on the order of their appearances.
2. Flow class is deleted, and classes with its instances now directly have instances of EventData class that used to belong to the Flow classs.
3. ApplicationHeader class is deleted, and classes with its instances now directly have instances of ApplicationHeaderField class that used to belong to the ApplicationHeader class.
4. SignatureData class is deleted, and classes with its instances now directly have instance of Signature class that used to belong to the SignatureData class.
5. IndicatorData class is deleted, and classes with its instances now directly have the instances of Indicator class that used to belong to the IndicatorData class.
6. ObservableReference class is deleted, and classes with its instances now directly have uid-ref as an element.
7. Record class is deleted, and classes with its instances now directly have the instances of RecordData class that used to belong to the Record class.
8. The elements of ML_STRING type are prepared as two separate elements: one of STRING type and another of ML_STRING type, in order to maintain the simplicity of IODEF documents when writing with only STRING type characters.

JSON Schema is provided, but an issue exists

```
5.  The IODEF Data Model (JSON Schema)

{ "$schema": "http://json-schema.org/draft-04/schema#",
  "definitions": {
    "action": {"enum": ["nothing","contact-source-site","contact-target-site
",
                "contact-sender", "investigate","block-host","block-network",
                "block-port","rate-limit-host","rate-limit-network",
                "rate-limit-port","redirect-traffic","honeypot",
                "upgrade-software","rebuild-asset","harden-asset",
                "remediate-other","status-triage","status-new-info",
                "watch-and-report","training","defined-coa","ext-value"]},
    "duration": {"enum": ["second","minute","hour","day","month","quarter",
                  "year","ext-value"]},
    "lang": {"enum": ["en","jp"]},
    "purpose": {"enum": ["traceback","mitigation","reporting","watch","other
",
                "ext-value"]},
    "restriction": {"enum": ["public","partner","need-to-know","private",
                    "default","
    "status": {"enum": ["new",
               "ext-value"]},
```

JSON schema is not yet published as an RFC.
Meanwhile, CDDL is progressing rapidly.

Moving forward

1. There were several data types that were not defined in the version 03 draft. The 04 version will cope with that. (The github version already has addressed it.)

2. Please give us any feedback on the latest version.

3. How to reference JSON schema specification?