MILE   T. Takahashi
Internet-Draft   NICT
Intended status: Standards Track   R. Danyliw
Expires: January 16, 2019   CERT
                                                             M. Suzuki
                                                                   NICT
                                                          July 15, 2018

                        JSON binding of IODEF
                     draft-ietf-mile-jsoniodef-04

Abstract

   RFC7970 specified an information model and a corresponding XML data
   model for exchanging incident and indicator information. This draft
   provides an alternative data model implementation in JSON.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF). Note that other groups may also distribute
   working documents as Internet-Drafts. The list of current Internet-
   Drafts is at https://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time. It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on January 16, 2019.

Copyright Notice

Table of Contents

1. Introduction

   [RFC7970] defines a data representation for security incident reports
   and indicators commonly exchanged by operational security teams. It
   facilitates the automated exchange of this information to enable
   mitigation and watch-and-warning. Section 3 of [RFC7970] defined an
   information model using Unified Modeling Language (UML) and a
   corresponding Extensible Markup Language (XML) schema data model in
   Section 8. This UML-based information model and XML-based data model
   are referred to as IODEF UML and IODEF XML, respectively in this
   document.

   This document defines an alternate implementation of the IODEF UML
   information model by specifying a JavaScript Object Notation (JSON)
   data model using JSON Schema [jsonschema]. This JSON data model is
   referred to as IODEF JSON in this document.

   IODEF JSON provides all of the expressivity of IODEF XML. It gives
   implementers and operators an alternative format to exchange the same
   information.

   The normative IODEF JSON data model is found in Section 5. Section 2
   and Section 3 describe the data types and elements of this data
   model. Section 4 provides examples.

1.1. Requirements Language

   The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
   "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this
   document are to be interpreted as described in RFC 2119 [RFC2119].

2. IODEF Data Types

   The abstract IODEF JSON implements the abstract data types specified
   in Section 2 of [RFC7970].

2.1. Abstract Data Type to JSON Data Type Mapping

   IODEF JSON uses native and derived JSON data types. Figure 1
   describes the mapping between the abstract data types in Section 2 of
   [RFC7970] and their corresponding implementations in IODEF JSON.

+----------------+------------------+-----------------------------+
| IODEF Data Type | [RFC7970] | JSON Data Type |
| | Reference | |
+----------------+------------------+-----------------------------+
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

2.2. Complex JSON Types

2.2.1. Multilingual Strings

   A string that needs to be represented in a human-readable language
   different than the default encoding of the document is represented in
   the information model by the ML_STRING data type. This data type is
   implemented as an object with "value", "lang", and "translation-id"
   elements as defined in Section 5. Examples are shown below.

   "MLStringType": {
     "value": "free-form text",   //STRING
     "lang": "en",   //ENUM
     "translation-id": "jp2en0023"   //STRING
   }

2.2.2. Software and SoftwareReference

   A particular version of software is represented in the information
   model by the SOFTWARE data type. This software can be described by
   using a reference, a URL, or with free-form text. The SOFTWARE data
   type is implemented as an object with "SoftwareReference", "URL",
   "Description", and "Description_ML" elements as defined in Section 5.
   Examples are shown below.

   "SoftwareType": {
     "SoftwareReference": {...},   //SoftwareReference
     "Description": ["MS Windows"]   //STRING
   }

   SoftwareReference class is a reference to a particular version of
   software. Examples are shown below.

   "SoftwareReference": {
     "value": "cpe:/a:google:chrome:59.0.3071.115 ",   //STRING
     "spec-name": "cpe",   //ENUM
     "dtype": "string",   //ENUM
   }

2.2.3. StructuredInfo

   Information provided in a form of structured string, such as ID, or
   structured information, such as XML documents, is represented in the
   information model by the StructuredInfo data type. Note that this
   type was originally specified in RFC7203. The StructuredInfo data
   type is implemented as an object with "SpecID", "ext-SpecID",
   "ContentID", "RawData", "Reference" elements. An example for
   embedding a structured ID is shown below.

   "StructuredInformation": {
     "SpecID": "cve",   //ENUM
     "ContentID": "CVE-2007-5000"   //STRING
   }

   When embedding the raw data, base64 conversion should be used for
   encoding the data, as shown below.

   "StructuredInformation": {
     "SpecID": "oval",   //ENUM
     "RawData": "<<<strings encoded with base64>>>"   //BYTE
   }

2.2.4. EXTENSION

   Information not otherwise represented in the IODEF can be added using
   the EXTENSION data type. This data type is a generic extension
   mechanism. The EXTENSION data type is implemented as an
   ExtensionType object with "value", "name", "dtype", "ext-dtype",
   "meaning", "formatid", "restriction", "ext-restriction", and
   "observable-id" elements. An example for embedding a structured ID
   is shown below.

   "ExtensionType": {
     "value": "xxxxxxx",   //String
     "name": "Syslog",   //String
     "dtype": "string",   //String
     "meaning": "Syslog from the security appliance X",   //String
   }

3. IODEF JSON Data Model

3.1. Classes and Elements

   The following table shows the list of IODEF Classes, their elements,
   and the corresponding section in [RFC7970]. Note that the complete
   JSON schema is defined in Section 5.

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

	RelatedActivity*		
	DetectTime?		
	StartTime?		
	EndTime?		
	RecoveryTime?		
	ReportTime?		
	GenerationTime		
	Description*		
	Description_ML*		
	Discovery*		
	Assessment*		
	Method*		
	Contact+		
	EventData*		
	Indicator*		
	History?		
	AdditionalData*		
IncidentID	id	3.4	
	name		
	instance?		
	restriction?		
	ext-restriction?		
AlternativeID	restriction?	3.5	
	ext-restriction?		
	IncidentID+		
RelatedActivity	restriction?	3.6	
	ext-restriction?		
	IncidentID*		
	URL*		
	ThreatActor*		
	Campaign*		
	IndicatorID*		
	Confidence?		
	Description*		
	AdditionalData*		
ThreatActor	restriction?	3.7	
	ext-restriction?		
	ThreatActorID*		
	URL*		
	Description*		
	Description_ML*		
	AdditionalData*		
Campaign	restriction?		

```
|                            | ext-restriction?   |             |
|                            | CampaignID*        |             |
|                            | URL*               |             |
|                            | Description*       |             |
|                            | Description_ML*    |             |
|                            | AdditionalData*    | 3.8         |
+----------------------------+--------------------+-------------+
| Contact                    | role               |             |
|                            | ext-role?          |             |
|                            | type               |             |
|                            | ext-type?          |             |
|                            | restriction?       |             |
|                            | ext-restriction?   |             |
|                            | ContactName*,      |             |
|                            | ContactName_ML*,   |             |
|                            | ContactTitle*      |             |
|                            | ContactTitle_ML*   |             |
|                            | Description*       |             |
|                            | Description_ML*    |             |
|                            | RegistryHandle*    |             |
|                            | PostalAddress*     |             |
|                            | Email*             |             |
|                            | Telephone*         |             |
|                            | Timezone?          |             |
|                            | Contact*           |             |
|                            | AdditionalData*    | 3.9         |
+----------------------------+--------------------+-------------+
| RegistryHandle             | handle             |             |
|                            | registry           |             |
|                            | ext-registry?      | 3.9.1       |
+----------------------------+--------------------+-------------+
| PostalAddress              | type?              |             |
|                            | ext-type?          |             |
|                            | PAddress           |             |
|                            | Description*       |             |
|                            | Description_ML*    | 3.9.2       |
+----------------------------+--------------------+-------------+
| Email                      | type?              |             |
|                            | ext-type?          |             |
|                            | EmailTo            |             |
|                            | Description*       |             |
|                            | Description_ML*    | 3.9.3       |
+----------------------------+--------------------+-------------+
| Telephone                  | type?              |             |
|                            | ext-type?          |             |
|                            | TelephoneNumber    |             |
|                            | Description*       |             |
|                            | Description_ML*    | 3.9.4       |
```

```
+-------------------------------+--------------------+--------------+
| Discovery                     | source?            |              |
|                               | ext-source?        |              |
|                               | restriction?       |              |
|                               | ext-restriction?   |              |
|                               | Description*       |              |
|                               | Description_ML*    |              |
|                               | Contact*           |              |
|                               | DetectionPattern*  | 3.10         |
+-------------------------------+--------------------+--------------+
| DetectionPattern              | restriction?       | 3.10.1       |
|                               | ext-restriction?   |              |
|                               | observable-id?     |              |
|                               | Application        |              |
|                               | Description*       |              |
|                               | Description_ML*    |              |
|                               | DetectionConfiguration*  |       |
+-------------------------------+--------------------+--------------+
| Method                        | restriction?       |              |
|                               | ext-restriction?   |              |
|                               | Reference*         |              |
|                               | Description*       |              |
|                               | Description_ML*    |              |
|                               | AttackPattern*     |              |
|                               | Vulnerability*     |              |
|                               | Weakness*          | 3.11         |
+-------------------------------+--------------------+--------------+
| Reference                     | observable-id?     |              |
|                               | ReferenceName?     |              |
|                               | URL*               |              |
|                               | Description*       |              |
|                               | Description_ML*    | 3.11.1       |
+-------------------------------+--------------------+--------------+
| Assessment                    | occurence?         |              |
|                               | restriction?       |              |
|                               | ext-restriction?   |              |
|                               | observable-id?     |              |
|                               | IncidentCategory*  |              |
|                               | SystemImpact*      |              |
|                               | BusinessImpact*    |              |
|                               | TimeImpact*        |              |
|                               | MonetaryImpact*    |              |
|                               | IntendedImpact*    |              |
|                               | Counter*           |              |
|                               | MitigatingFactor*  |              |
|                               | MitigatingFactor_ML*|             |
|                               | Cause*             |              |
|                               | Cause_ML*          |              |
```

```
|                         | Confidence?      |             |
|                         | AdditionalData*  | 3.12        |
+-------------------------+------------------+-------------+
| SystemImpact            | severity?        |             |
|                         | completion?      |             |
|                         | type             |             |
|                         | ext-type?        |             |
|                         | Description*     |             |
|                         | Description_ML*  | 3.12.1      |
+-------------------------+------------------+-------------+
| BusinessImpact          | severity?        |             |
|                         | ext-severity?    |             |
|                         | type             |             |
|                         | ext-type?        |             |
|                         | Description*     |             |
|                         | Description_ML*  | 3.12.2      |
+-------------------------+------------------+-------------+
| TimeImpact              | value            |             |
|                         | severity?        |             |
|                         | metric           |             |
|                         | ext-metric?      |             |
|                         | duration?        |             |
|                         | ext-duration?    | 3.12.3      |
+-------------------------+------------------+-------------+
| MonetaryImpact          | value            |             |
|                         | severity?        |             |
|                         | currency?        | 3.12.4      |
+-------------------------+------------------+-------------+
| Confidence              | value            |             |
|                         | rating           |             |
|                         | ext-rating?      | 3.12.5      |
+-------------------------+------------------+-------------+
| History                 | restriction?     |             |
|                         | ext-restriction? |             |
|                         | HistoryItem+     | 3.13        |
+-------------------------+------------------+-------------+
| HistoryItem             | action           |             |
|                         | ext-action?      |             |
|                         | restriction?     |             |
|                         | ext-restriction? |             |
|                         | observable-id?   |             |
|                         | DateTime         |             |
|                         | IncidentID?      |             |
|                         | Contact?         |             |
|                         | Description*     |             |
|                         | Description_ML*  |             |
|                         | DefinedCOA*      |             |
|                         | AdditionalData*  | 3.13.1      |
```

```
+---------------------------+----------------------+-------------+
| EventData                 | restriction?         |             |
|                           | ext-restriction?     |             |
|                           | observable-id?       |             |
|                           | Description*         |             |
|                           | Description_ML*      |             |
|                           | DetectTime?          |             |
|                           | StartTime?           |             |
|                           | EndTime?             |             |
|                           | RecoveryTime?        |             |
|                           | ReportTime?          |             |
|                           | Contact*             |             |
|                           | Discovery*           |             |
|                           | Assessment?          |             |
|                           | Method*              |             |
|                           | System*              |             |
|                           | Expectation*         |             |
|                           | Record*              |             |
|                           | EventData*           |             |
|                           | AdditionalData*      | 3.14        |
+---------------------------+----------------------+-------------+
| Expectation               | action?              |             |
|                           | ext-action?          |             |
|                           | severity?            |             |
|                           | restriction?         |             |
|                           | ext-restriction?     |             |
|                           | Description*         |             |
|                           | Description_ML*      |             |
|                           | DefinedCOA*          |             |
|                           | StartTime?           |             |
|                           | EndTime?             |             |
|                           | Contact?             | 3.15        |
+---------------------------+----------------------+-------------+
| System                    | category?            |             |
|                           | ext-category?        |             |
|                           | interface?           |             |
|                           | spoofed?             |             |
|                           | virtual?             |             |
|                           | ownership?           |             |
|                           | ext-ownership?       |             |
|                           | restriction?         |             |
|                           | ext-restriction?     |             |
|                           | Node                 |             |
|                           | NodeRole*            |             |
|                           | Service*             |             |
|                           | OperatingSystem*     |             |
|                           | Counter*             |             |
|                           | AssetID*             |             |
```

```
|                           | Description*       |              |
|                           | Description_ML*    |              |
|                           | AdditionalData*    | 3.16         |
+---------------------------+--------------------+--------------+
| Node                      | DomainData*        |              |
|                           | Address*           |              |
|                           | PostalAddress?     |              |
|                           | Location*          |              |
|                           | Location_ML*       |              |
|                           | Counter*           | 3.17         |
+---------------------------+--------------------+--------------+
| Address                   | value              |              |
|                           | category           |              |
|                           | ext-category?      |              |
|                           | vlan-name?         |              |
|                           | vlan-num?          |              |
|                           | observable-id?     | 3.17.1       |
+---------------------------+--------------------+--------------+
| NodeRole                  | category           |              |
|                           | ext-category?      |              |
|                           | Description*       |              |
|                           | Description_ML*    | 3.17.2       |
+---------------------------+--------------------+--------------+
| Counter                   | value              |              |
|                           | type               |              |
|                           | ext-type?          |              |
|                           | unit               |              |
|                           | ext-unit?          |              |
|                           | meaning?           |              |
|                           | meaning_ML?        |              |
|                           | duration?          |              |
|                           | ext-duration?      | 3.17.3       |
+---------------------------+--------------------+--------------+
| DomainData                | system-status      |              |
|                           | ext-system-status? |              |
|                           | domain-status      |              |
|                           | ext-domain-status? |              |
|                           | observable-id?     |              |
|                           | Name               |              |
|                           | DateDomainWasChecked?|            |
|                           | RegistrationDate?  |              |
|                           | ExpirationDate?    |              |
|                           | RelatedDNS*        |              |
|                           | Nameservers*       |              |
|                           | DomainContacts?    | 3.18         |
+---------------------------+--------------------+--------------+
| Nameserver                | Server             |              |
|                           | Address*           | 3.18.1       |
```

```
+---------------------------+--------------------+--------------+
| DomainContacts            | SameDomainContact? |              |
|                           | Contact+           | 3.18.2       |
+---------------------------+--------------------+--------------+
| Service                   | ip-protocol?       |              |
|                           | observable-id?     |              |
|                           | ServiceName?       |              |
|                           | Port?              |              |
|                           | Portlist?          |              |
|                           | ProtoCode?         |              |
|                           | ProtoType?         |              |
|                           | ProtoField?        |              |
|                           | ApplicationHeaderField+|          |
|                           | EmailData?         |              |
|                           | Application?       | 3.19         |
+---------------------------+--------------------+--------------+
| ServiceName               | IANAService?       |              |
|                           | URL*               |              |
|                           | Description*       |              |
|                           | Description_ML*    | 3.19.1       |
+---------------------------+--------------------+--------------+
| EmailData                 | observable-id?     |              |
|                           | EmailTo*           |              |
|                           | EmailFrom?         |              |
|                           | EmailSubject?      |              |
|                           | EmailX-Mailer?     |              |
|                           | EmailHeaderField*  |              |
|                           | EmailHeaders?      |              |
|                           | EmailBody?         |              |
|                           | EmailMessage?      |              |
|                           | HashData*          |              |
|                           | Signature*         | 3.19.2       |
+---------------------------+--------------------+--------------+
| RecordData                | restriction?       |              |
|                           | ext-restriction?   |              |
|                           | observable-id?     |              |
|                           | DateTime?          |              |
|                           | Description*       |              |
|                           | Description_ML*    |              |
|                           | Application?       |              |
|                           | RecordPattern*     |              |
|                           | RecordItem*        |              |
|                           | URL*               |              |
|                           | FileData*          |              |
|                           | WindowsRegistryKeysModified*|     |
|                           | CertificateData*   |              |
|                           | AdditionalData*    | 3.19.3       |
+---------------------------+--------------------+--------------+
```

RecordPattern	type ext-type? offset? offsetunit? ext-offsetunit? instance? value	3.19.4	
WindowsRegistryKeysModified	observable-id? Key+	3.20	
Key	registryaction? ext-registryaction? observable-id? KeyName KeyValue?	3.20.1	
CertificateData	restriction? ext-restriction? observable-id? Certificate+	3.21	
Certificate	observable-id? X509Data Description* Description_ML*	3.21.1	
FileData	restriction? ext-restriction? observable-id? File+	3.22	
File	observable-id? FileName? FileSize? FileType? URL* HashData? Signature* AssociatedSoftware? FileProperties*	3.22.1	
HashData	scope HashTargetID? Hash* FuzzyHash*	3.23	
Hash	DigestMethod		

```
|                           | DigestValue         |             |
|                           | CanonicalizationMethod?|          |
|                           | Application?        | 3.23.1      |
+---------------------------+---------------------+-------------+
| FuzzyHash                 | FuzzyHashValue+     |             |
|                           | Application?        |             |
|                           | AdditionalData?     | 3.23.2      |
+---------------------------+---------------------+-------------+
| Indicator                 | restriction?        |             |
|                           | ext-restriction?    |             |
|                           | IndicatorID         |             |
|                           | AlternativeIndicatorID*|          |
|                           | Description*        |             |
|                           | Description_ML*     |             |
|                           | StartTime?          |             |
|                           | EndTime?            |             |
|                           | Confidence?         |             |
|                           | Contact*            |             |
|                           | Observable?         |             |
|                           | uid-ref?            |             |
|                           | IndicatorExpression?|            |
|                           | IndicatorReference? |             |
|                           | NodeRole*           |             |
|                           | AttackPhase*        |             |
|                           | Reference*          |             |
|                           | AdditionalData*     | 3.24        |
+---------------------------+---------------------+-------------+
| IndicatorID               | id                  |             |
|                           | name                |             |
|                           | version             | 3.24.1      |
+---------------------------+---------------------+-------------+
| AlternativeIndicatorID    | restriction?        |             |
|                           | ext-restriction?    |             |
|                           | IndicatorReference+ | 3.24.2      |
+---------------------------+---------------------+-------------+
| Observable                | restriction?        |             |
|                           | ext-restriction?    |             |
|                           | System?             |             |
|                           | Address?            |             |
|                           | DomainData?         |             |
|                           | Service?            |             |
|                           | EmailData?          |             |
|                           | WindowsRegistryKeysModified?|        |
|                           | FileData?           |             |
|                           | CertificateData?    |             |
|                           | RegistryHandle?     |             |
|                           | RecordData?         |             |
|                           | EventData?          |             |
```

```
|                          | Incident?          |             |
|                          | Expectation?       |             |
|                          | Reference?         |             |
|                          | Assessment?        |             |
|                          | DetectionPattern?  |             |
|                          | HistoryItem?       |             |
|                          | BulkObservable?    |             |
|                          | AdditionalData*    | 3.24.3      |
+--------------------------+--------------------+-------------+
| BulkObservable           | type?              |             |
|                          | ext-type?          |             |
|                          | BulkObservableFormat?|           |
|                          | BulkObservableList |             |
|                          | AdditionalData*    | 3.24.4      |
+--------------------------+--------------------+-------------+
| BulkObservableFormat     | Hash?              |             |
|                          | AdditionalData*    | 3.24.5      |
+--------------------------+--------------------+-------------+
| IndicatorExpression      | operator?          |             |
|                          | ext-operator?      |             |
|                          | IndicatorExpression*|            |
|                          | Observable*        |             |
|                          | uid-ref*           |             |
|                          | IndicatorReference*|             |
|                          | Confidence?        |             |
|                          | AdditionalData*    | 3.24.6      |
+--------------------------+--------------------+-------------+
| IndicatorReference       | uid-ref?           |             |
|                          | euid-ref?          |             |
|                          | version?           | 3.24.7      |
+--------------------------+--------------------+-------------+
| AttackPhase              | AttackPhaseID*     |             |
|                          | URL*               |             |
|                          | Description*       |             |
|                          | Description_ML*    |             |
|                          | AdditionalData*    | 3.24.8      |
+--------------------------+--------------------+-------------+
```

3.2. Mapping between JSON and XML IODEF

   o This document treats attributes and elements of each class defined
      in [RFC7970] equally and is agnostic on the order of their
      appearances.

   o Flow class is deleted, and classes with its instances now directly
      have instances of EventData class that used to belong to the Flow
      classs.

   o ApplicationHeader class is deleted, and classes with its instances
      now directly have instances of ApplicationHeaderField class that
      used to belong to the ApplicationHeader class.

   o SignatureData class is deleted, and classes with its instances now
      directly have instance of Signature class that used to belong to
      the SignatureData class.

   o 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.

   o ObservableReference class is deleted, and classes with its
      instances now directly have uid-ref as an element.

   o Record class is replaced by RecordData class, and RecordData class
      is renamed to Record class.

   o 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.

   o 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.

4. Examples

   This section provides example of IODEF documents. These examples do
   not represent the full capabilities of the data model or the the only
   way to encode particular information.

4.1. Minimal Example

   A document containing only the mandatory elements and attributes.

```
     {
       "version": "2.0",
       "lang": "en",
       "Incident": [{
           "purpose": "reporting",
           "restriction": "private",
           "IncidentID": {
             "id": "492382",
             "name": "csirt.example.com"
           },
           "GenerationTime": "2015-07-18T09:00:00-05:00",
           "Contact": [{
               "type": "organization",
               "role": "creator",
               "Email": [{
                 "EmailTo": "contact@csirt.example.com"
               }]
           }]
       }]
     }
```

4.2. Indicators from a Campaign

   An example of C2 domains from a given campaign.

```
{
  "version": "2.0",
  "lang": "en",
  "Incidents": [
    {
      "purpose": "watch",
      "restriction": "green",
      "IncidentID": {
        "id": "897923",
        "name": "csirt.example.com"
      },
      "RelatedActivity": [
        {
          "ThreatActor": [
            {
              "ThreatActorID": "TA-12-AGGRESSIVE-BUTTERFLY",
              "Description": "Aggressive Butterfly"
            }
          ],
          "Campaign": [
            {
              "CampaignID": "C-2015-59405",
              "Description": "Orange Giraffe"
```

```
            }
          ]
        }
      ],
      "GenerationTime": "2015-10-02T11:18:00-05:00",
      "Description": [
        "Summarizes the Indicators of Compromise for the Orange Giraffe camp
aign of the Aggressive Butterfly crime gang."
      ],
      "Assessment": [
        {
          "BusinessImpact": {
            "type": "breach-proprietary"
          }
        }
      ],
      "Contacts": [
        {
          "type": "organization",
          "role": "creator",
          "ContactName": "CSIRT for example.com",
          "Email": {
            "emailTo": "contact@csirt.example.com"
          }
        }
      ],
      "IndicatorList": [
        {
          "IndicatorID": {
            "id": "G90823490",
            "name": "csirt.example.com",
            "version": "1"
          },
          "Description": "C2 domains",
          "StartTime": "2014-12-02T11:18:00-05:00",
          "Observable": {
            "BulkObservable": {
              "type": "fqdn"
            },
            "BulkObservableList": [
              "kj290023j09r34.example.com",
              "09ijk23jfj0k8.example.net",
              "klknjwfjiowjefr923.example.org",
              "oimireik79msd.example.org"
            ]
          }
        }
      ]
    }
```

```
   ]
}

5.  The IODEF Data Model (CDDL)

start = iodef

;;; iodef.json: IODEF-Document

iodef = {
 version: text
 ? lang: lang
 ? format-id: text
 ? private-enum-name: text
 ? private-enum-id: text
 + Incident: [+ Incident]
 * AdditionalData: ExtensionType
}

duration = "second" / "minute" / "hour" / "day" / "month" / "quarter" /
           "year" / "ext-value"
lang = "en" / "jp"
restriction = "public" / "partner" / "need-to-know" / "private" /
              "default" / "white" / "green" / "amber" / "red" /
              "ext-value"
DATETIME = text
URLtype = text
IDtype = text

action = "nothing" / "contact-source-site" / "cotact-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" / "other" / "ext-value"

ExtensionType  = {
 ? Name: text
 ? dtype: "boolean" / "byte" / "bytes" / "character" / "date-time" /
          "ntpstamp" / "integer" / "portlist" / "real" / "string" /
          "file" / "path" / "frame" / "packet" / "ipv4-packet" /
          "ipv6-packet" / "url" / "csv" / "winreg" / "xml" / "ext-value"
 ? ext-dtype: text
 ? meaning: text
 ? formatid: text
 ? restriction: restriction
```

```
 ? ext-restriction: text
 ? observable-id: IDtype
}

SoftwareType = {
 ? SoftwareReference: SoftwareReference
 ? URL: URLtype
 ? Description: text
}

SoftwareReference = {
 ? value: text
 spec-name: text
 ? ext-spec-name: text
 ? dtype: text
 ? ext-dtype: text
}

Incident = {
 purpose: "traceback" / "mitigation" / "reporting" / "watch" / "other" /
          "ext-value"
 ? ext-purpose: text
 ? status: "new" / "in-progress"/ "forwarded" / "resolved" / "future" /
          "ext-value"
 ? ext-status: text
 ? lang: lang
 ? restriction: restriction
 ? ext-restriction: text
 ? observable-id: IDtype
 IncidentID: IncidentID
 ? AlternativeID: AlternativeID
 * RelatedActivity: RelatedActivity
 ? DetectTime: text
 ? StartTime: text
 ? EndTime: text
 ? RecoveryTime: text
 ? ReportTime: text
 GenerationTime: text
 * Description: text
 * Description_ML: text
 * Discovery: Discovery
 * Assessment: Assessment
 * Method: Method
 + Contacts: Contact
 * EventData: EventData
 * Indicator: Indicator
 ? History: History
 * AdditionalData: ExtensionType
```

```
}

IncidentID = {
 id: text
 name: text
 ? instance: text
 ? restriction: restriction
 ? ext-restriction: text
}

AlternativeID = {
 ? restriction: restriction
 ? ext-restriction: text
 + IncidentID: IncidentID
}

RelatedActivity = {
 ? restriction: restriction
 ? ext-restriction: text
 * IncidentID: IncidentID
 * URL: URLtype
 * ThreatActor: ThreatActor
 * Campaign: Campaign
 * IndicatorID: IndicatorID
 ? Confidence: Confidence
 * Description: text
 * AdditionalData: ExtensionType
}

ThreatActor = {
 ? restriction: restriction
 ? ext-restriction: text
 * ThreatActorID: text
 * URL: URLtype
 * Description: text
 * Description_ML: text
 * AdditionalData: ExtensionType
}

Campaign  = {
 ? restriction: restriction
 ? ext-restriction: text
 * CampaignID: text
 * URL: URLtype
 * Description: text
 * Description_ML: text
 * AdditionalData: ExtensionType
}
```

```
Contact = {
 role: "creator" / "reporter" / "admin" / "tech" / "provider" / "user" /
       "billing" / "legal" / "irt" / "abuse" / "cc" / "cc-irt" / "leo" /
       "vendor" / "vendor-support" / "victim" / "victim-notified" /
       "ext-value"
 ? ext-role: text
 type: "person" / "organization" / "ext-value"
 ? ext-type: text
 ? restriction: restriction
 ? ext-restriction: text
 * ContactName: text
 * ContactName_ML: text
 * ContactTitle: text
 * ContactTitle_ML: text
 * Description: text
 * Description_ML: text
 * RegistryHandle: RegistryHandle
 * PostalAddress: PostalAddress
 * Email: Email
 * Telephone: Telephone
 ? Timezone: text
 * Contact: Contact
 * AdditionalData: ExtensionType
}

RegistryHandle = {
 handle: text
 registry: "internic" / "apnic" / "arin" / "lacnic" / "ripe" / "afrinic" /
           "local" / "ext-value"
 ? ext-registry: text
}

PostalAddress = {
 ? type: text
 ? ext-type: text
 PAddress: text
 * Description: text
 * Description_ML: text
}

Email = {
 ? type: "direct" / "hotline" / "ext-value"
 ? ext-type: text
 EmailTo: text
 * Description: text
 * Description_ML: text
}
```

```
Telephone = {
 ? type: "wired" / "mobile" / "fax" / "hotline" / "ext-value"
 ? ext-type: text
 TelephoneNumber: text
 * Description: text
 * Description_ML: text
}

Discovery = {
 ? source: "nidps" / "hips" / "siem" / "av" / "third-party-monitoring" /
           "incident" / "os-log" / "application-log" / "device-log" /
           "network-flow" / "passive-dns" / "investiation" / "audit" /
           "international-notification" / "external-notification" /
           "leo" / "partner" / "actor" / "unknown" / "ext-value"
 ? ext-source: text
 ? restriction: restriction
 ? ext-restriction: text
 * Description: text
 * Description_ML: text
 * Contact: Contact
 * DetectionPattern: DetectionPattern
}

DetectionPattern = {
 ? restriction: restriction
 ? ext-restriction: text
 ? observable-id: IDtype
 Application: SoftwareType
 * Description: text
 * Description_ML: text
 * DetectionConfiguration: text
}

Method = {
 ? restriction: restriction
 ? ext-restriction: text
 * Reference: Reference
 * Description: text
 * Description_ML: text
 * AttackPattern: StructuredInformation
 * Vulnerability: StructuredInformation
 * Weakness: StructuredInformation
 ? AdditionalData: ExtensionType
}

StructuredInformation = {
 specID: text
 ? ext-specID: text
```

```
 ? contentID: text
 ? RawData: any
 ? URL: URLtype
}

Reference = {
 ? observable-id: IDtype
 ? ReferenceName: ReferenceName
 * URL: URLtype
 * Description: text
 * Description_ML: text
}

ReferenceName = {
 specIndex: int
 ID: text
}

Assessment = {
 ? occurrence: "actual" / "potential"
 ? restriction: restriction
 ? ext-restriction: text
 ? observable-id: IDtype
 * IncidentCategory: text
 * SystemImpact: SystemImpact
 * BusinessImpact: BusinessImpact
 * TimeImpact: TimeImpact
 * MonetaryImpact: MonetaryImpact
 * IntendedImpact: BusinessImpact
 * Counter: Counter
 * MitigatingFactor: text
 * MitigatingFactor_ML: text
 * Cause: text
 * Cause_ML: text
 ? Confidence: Confidence
 * AdditionalData: ExtensionType
}

SystemImpact = {
 ? severity: "low" / "medium" / "high"
 ? completion: "failed" / "succeeded"
 type: "takeover-account" / "takeover-service" / "takeover-system" /
       "cps-manipulation" / "cps-damage" / "availability-data" /
       "availability-account" / "availability-service" /
       "availability-system" / "damaged-system" / "damaged-data" /
       "breach-proprietary" / "breach-privacy" / "breach-credential" /
       "breack-configuration" / "integrity-data" /
       "integrity-configuration" / "integrity-hardware" /
```

```
        "traffic-redirection" / "monitoring-traffic" / "monitoring-host" /
        "policy" / "unknown" / "ext-value"
 ? ext-type: text
 * Description: text
 * Description_ML: text
}

BusinessImpact = {
 ? severity: "none" / "low" / "medium" / "high" / "unknown" / "ext-value"
 ? ext-severity: text
  type: "breach-proprietary" / "breach-privacy" / "breach-credential" /
        "loss-of-integrity" / "loss-of-service" / "theft-financial" /
        "theft-service" / "degraded-reputation" / "asset-damage" /
        "asset-manipulation" / "legal" / "extortion" / "unknown" /
        "ext-value"
 ? ext-type: text
 * Description: text
 * Description_ML: text
}

TimeImpact = {
 value: int
 ? severity: "low" / "medium" / "high"
 metric: "labor" / "elapsed" / "downtime" / "ext-value"
 ? ext-metric: text
 ? duration: duration
 ? ext-duration: text
}

MonetaryImpact = {
 value: int
 ? severity: "low" / "medium" / "high"
 ? currency: text
}

Confidence = {
 value: int
 rating: "low" / "medium" / "high" / "numeric" / "unknown" / "ext-value"
 ? ext-rating: text
}

History = {
 ? restriction: restriction
 ? ext-restriction: text
 + HistoryItem: HistoryItem
}

HistoryItem = {
```

```
 action: action
 ? ext-action: text
 ? restriction: restriction
 ? ext-restriction: text
 ? observable-id: IDtype
 DateTime: DATETIME
 ? IncidentID: IncidentID
 ? Contact: Contact
 * Description: text
 * Description_ML: text
 * DefinedCOA: text
 * AdditionalData: ExtensionType
}

EventData = {
 ? restriction: restriction
 ? ext-restriction: text
 ? observable-id: IDtype
 * Description: text
 * Description_ML: text
 ? DetectTime: DATETIME
 ? StartTime: DATETIME
 ? EndTime: DATETIME
 ? RecoveryTime: DATETIME
 ? ReportTime: DATETIME
 * Contact: Contact
 * Discovery: Discovery
 ? Assessment: Assessment
 * Method: Method
 ? System: System
 * Expectation: Expectation
 * RecordData: RecordData
 * EventData: EventData
 * AdditionalData: ExtensionType
}

Expectation = {
 ? action: action
 ? ext-action: text
 ? severity: "low" / "medium" / "high"
 ? restriction: restriction
 ? ext-restriction: text
 ? observable-id: IDtype
 * Description: text
 * Description_ML: text
 * DefinedCOA: text
 ? StartTime: DATETIME
 ? EndTime: DATETIME
```

```
 ? Contact: Contact
}

System = {
 ? category: "source" / "target" / "intermediate" / "sensor" /
"infrastructure" / "ext-value"
 ? ext-category: text
 ? interface: text
 ? spoofed: "unknown" / "yes" / "no"
 ? virtual: "yes" / "no" / "unknown"
 ? ownership: "organization" / "personal" / "partner" / "customer" /
               "no-relationship" / "unknown" / "ext-value"
 ? ext-ownership: text
 ? restriction: restriction
 ? ext-restriction: text
 ? observable-id: IDtype
 Node: Node
 * NodeRole: NodeRole
 * Service: Service
 * OperatingSystem: SoftwareType
 * Counter: Counter
 * AssetID: text
 * Description: text
 * Description_ML: text
 * AdditionalData: ExtensionType
}

Node = {
 * DomainData: DomainData
 * Address: Address
 ? PostalAddress: PostalAddress
 * Location: text
 * Location_ML: text
 * Counter: Counter
}

Address = {
 value: text
 category: "asn" / "atm" / "e-mail" / "ipv4-addr" / "ipv4-net" /
           "ipv4-net-masked" / "ipv4-net-mask" / "ipv6-addr" /
           "ipv6-net" / "ipv6-net-masked" / "mac" / "site-url" /
           "ext-value"
 ? ext-category: text
 ? vlan-name: text
 ? vlan-num: int
 ? observable-id: IDtype
}
```

```
NodeRole = {
 category: "client" / "client-enterprise" / "clent-partner" /
           "client-remote" / "client-kiosk" / "client-mobile" /
           "server-internal" / "server-public" / "www" / "mail" /
           "webmail" / "messaging" / "streaming" / "voice" / "file" /
           "ftp" / "p2p" / "name" / "directory" / "credential" /
           "print" / "application" / "database" / "backup" / "dhcp" /
           "assessment" / "source-control" / "config-management" /
           "monitoring" / "infra" / "infra-firewall" / "infra-router" /
           "infra-switch" / "camera" / "proxy" / "remote-access" /
           "log" / "virtualization" / "pos" /  "scada" /
           "scada-supervisory" / "sinkhole" / "honeypot" /
           "anomyzation" / "c2-server" / "malware-distribution" /
           "drop-server" / "hot-point" / "reflector" /
           "phishing-site" / "spear-phishing-site" / "recruiting-site" /
           "fraudulent-site" / "ext-value"
 ? ext-category: text
 * Description: text
 * Description_ML: text
}

Counter = {
 value: text
 type: "count" / "peak" / "average" / "ext-value"
 ? ext-type: text
 unit: "byte" / "mbit" / "packet" / "flow" / "session" / "alert" /
       "message" / "event" / "host" / "site" / "organization" /
       "ext-value"
 ? ext-unit: text
 ? meaning: text
 ? meaning_ML: text
 ? duration: duration
 ? ext-duration: text
}

DomainData = {
 system-status: "spoofed" / "fraudulent" / "innocent-hacked" /
                "innocent-hijacked" / "unknown" / "ext-value"
 ? ext-system-status: text
 domain-status: "reservedDelegation" / "assignedAndActive" /
                "assignedAndInactive" / "assignedAndOnHold" /
                "revoked" / "transferPending" / "registryLock" /
                "registrarLock" / "other" / "unknown" / "ext-value"
 ? ext-domain-status: text
 ? observable-id: IDtype
 Name: text
 ? DateDomainWasChecked: DATETIME
 ? RegistrationDate: DATETIME
```

```
 ? ExpirationDate: DATETIME
 * RelatedDNS: ExtensionType
 * NameServers: NameServers
 ? DomainContacts: DomainContacts
}

NameServers = {
 Server: text
 * Address: Address
}

DomainContacts = {
 ? SameDomainContact: text
 + Contact: Contact
}

Service = {
 ? ip-protocol: int
 ? observable-id: IDtype
 ? ServiceName: ServiceName
 ? Port: int
 ? Portlist: text
 ? ProtoCode: int
 ? ProtoType: int
 ? ProtoField: int
 + ApplicationHeaderField: ExtensionType
 ? EmailData: EmailData
 ? Application: SoftwareType
}

ServiceName = {
 ? IANAService: text
 * URL: URLtype
 * Description: text
 * Description_ML: text
}

EmailData = {
 ? observable-id: IDtype
 * EmailTo: text
 ? EmailFrom: text
 ? EmailSubject: text
 ? EmailX-Mailer: text
 * EmailHeaderField: ExtensionType
 ? EmailHeaders: text
 ? EmailBody: text
 ? EmailMessage: text
 * HashData: HashData
```

```
 * Signature: text
}

RecordData = {
 ? restriction: restriction
 ? ext-restriction: text
 ? observable-id: IDtype
 ? DateTime: DATETIME
 * Description: text
 * Description_ML: text
 ? Applicadtion: SoftwareType
 * RecordPattern: RecordPattern
 * RecordItem: ExtensionType
 * URL: URLtype
 * FileData: FileData
 * WindowsRegistryKeysModified: WindowsRegistryKeysModified
 * CertificateData: CertificateData
 * AdditionalData: ExtensionType
}

RecordPattern = {
 value: text
 type: "regex" / "binary" / "xpath" / "ext-value"
 ? ext-type: text
 ? offset: int
 ? offsetunit: "line" / "byte" / "ext-value"
 ? ext-offsetunit: text
 ? instance: int
}

WindowsRegistryKeysModified = {
 ? observable-id: IDtype
 + Key: Key
}

Key = {
 ? registryaction: "add-key" / "add-value" / "delete-key" /
                   "delete-value" / "modify-key" / "modify-value" /
                   "ext-value"
 ? ext-registryaction: text
 ? observable-id: IDtype
 KeyName: text
 ? KeyValue: text
}

CertificateData = {
 ? restriction: restriction
 ? ext-restriction: text
```

```
 ? observable-id: IDtype
 + Certificate: Certificate
}

Certificate = {
 ? observable-id: IDtype
 X509Data: text
 * Description: text
 * Description_ML: text
}

FileData = {
 ? restriction: restriction
 ? ext-restriction: text
 ? observable-id: IDtype
 + File: File
}

File = {
 ? observable-id: IDtype
 ? FileName: text
 ? FileSize: int
 ? FileType: text
 * URL: URLtype
 ? HashData: HashData
 * Signature: text
 ? AssociatedSoftware: SoftwareType
 * FileProperties: ExtensionType
}

HashData = {
 scope: "file-contents" / "file-pe-section" / "file-pe-iat" /
        "file-pe-resource" / "file-pdf-object" / "email-hash" /
        "email-hash-header" / "email-hash-body"
 ? HashTargetID: text
 * Hash: Hash
 * FuzzyHash: FuzzyHash
}

Hash = {
 DigestMethod: text
 DigestValue: text
 ? CanonicalizationMethod: any
 ? Application: SoftwareType
}

FuzzyHash = {
 + FuzzyHashValue: text
```

```
 ? Application: SoftwareType
 * AdditionalData: ExtensionType
}

Indicator = {
 ? restriction: restriction
 ? ext-restriction: text
 IndicatorID: IndicatorID
 * AlternativeIndicatorID: AlternativeIndicatorID
 * Description: text
 * Description_ML: text
 ? StartTime: DATETIME
 ? EndTime: DATETIME
 ? Confidence: Confidence
 * Contact: Contact
 ? Observable: Observable
 ? uid-ref: text
 ? IndicatorExpression: IndicatorExpression
 ? IndicatorReference: IndicatorReference
 * NodeRole: NodeRole
 * AttackPhase: AttackPhase
 * Reference: Reference
 * AdditionalData: ExtensionType
}

IndicatorID = {
 id: IDtype
 name: text
 version: text
}

AlternativeIndicatorID = {
 ? restriction: restriction
 ? ext-restriction: text
 + IndicatorReference: IndicatorReference
}

Observable = {
 ? restriction: restriction
 ? ext-restriction: text
 ? System: System
 ? Address: Address
 ? DomainData: DomainData
 ? EmailData: EmailData
 ? Service: Service
 ? WindowsRegistryKeysModified: WindowsRegistryKeysModified
 ? FileData: FileData
 ? CertificateData: CertificateData
```

```
 ? RegistryHandle: RegistryHandle
 ? RecordData: RecordData
 ? EventData: EventData
 ? Incident: Incident
 ? Expectation: Expectation
 ? Reference: Reference
 ? Assessment: Assessment
 ? DetectionPattern: DetectionPattern
 ? HistoryItem: HistoryItem
 ? BulkObservable: BulkObservable
 * AdditionalData: ExtensionType
}

BulkObservable = {
 ? type: "asn" / "atm" / "e-mail" / "ipv4-addr" / "ipv4-net" /
         "ipv4-net-mask" / "ipv6-addr" / "ipv6-net" / "ipv6-net-mask" /
         "mac" / "site-url" / "domain-name" / "domain-to-ipv4" /
         "domain-to-ipv6" / "domain-to-ipv4-timestamp" /
         "domain-to-ipv6-timestamp" / "ipv4-port" / "ipv6-port" /
         "windows-reg-key" / "file-hash" / "email-x-mailer" /
         "email-subject" / "http-user-agent" / "http-request-uri" /
         "mutex" / "file-path" / "user-name" / "ext-value"
 ? ext-type: text
 ? BulkObservableFormat: BulkObservableFormat
 BulkObservableList: text
 * AdditionalData: ExtensionType
}

BulkObservableFormat = {
 ? Hash: Hash
 * AdditionalData: ExtensionType
}

IndicatorExpression = {
 ? operator: "not" / "and" / "or" / "xor"
 ? ext-operator: text
 * IndicatorExpression: IndicatorExpression
 * Observable: Observable
 * uid-ref: text
 * IndicatorReference: IndicatorReference
 ? Confidence: Confidence
 * AdditionalData: ExtensionType
}

IndicatorReference = {
 ? uid-ref: text
 ? euid-ref: text
 ? version: text
```

```
}

AttackPhase = {
 * AttackPhaseID: text
 * URL: URLtype
 * Description: text
 * AdditionalData: ExtensionType
}
```

                    Figure 2: Data Model in CDDL

6. Acknowledgements

   We would like to thank Henk Birkholz and Carsten Bormann for their
   insightful comments on CDDL.

7. IANA Considerations

   This document registers a JSON schema.

8. Security Considerations

   This memo does not provide any further security considerations than
   the one described in [RFC7970].

9. Normative References

   [jsonschema]
               "JSON Schema", 2006.

               http://json-schema.org/

   [RFC2119]   Bradner, S., "Key words for use in RFCs to Indicate
               Requirement Levels", BCP 14, RFC 2119,
               DOI 10.17487/RFC2119, March 1997,
               <https://www.rfc-editor.org/info/rfc2119>.

   [RFC7970]   Danyliw, R., "The Incident Object Description Exchange
               Format Version 2", RFC 7970, DOI 10.17487/RFC7970,
               November 2016, <https://www.rfc-editor.org/info/rfc7970>.

Appendix A. The IODEF Data Model (JSON Schema)

   This section provides a JSON schema that defines the IODEF Data Model
   defined in this draft.

```
{ "$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","white","green","amber","red","ext-value"]},
   "status": {"enum": ["new","in-progress","forwarded","resolved",
              "future","ext-value"]},
   "DATETIME": {"type": "string"},
   "PORTLIST": {"type": "string"},
   "URLtype": {"type": "string"},
   "IDtype": {"type": "string"},
   "ExtensionType": {
     "type": "object",
     "properties": {
       "name": {"type": "string"},
       "dtype": {"enum": ["boolean","byte","bytes","character","date-time",
                  "ntpstamp","integer","portlist","real","string","file",
                  "path","frame","packet","ipv4-packet","ipv6-packet","url",
                  "csv","winreg","xml","ext-value"]},
       "ext-dtype": {"type": "string"},
       "meaning": {"type": "string"},
       "formatid": {"type": "string"},
       "restriction": {"$ref": "#/definitions/restriction"},
       "ext-restriction": {"type": "string"},
       "observable-id": {"$ref": "#/definitions/IDtype"}}},
   "ExtensionTypeList": {
     "type": "array",
     "items": {"$ref": "#/definitions/ExtensionType"}},
   "SoftwareType": {
     "type": "object",
     "properties": {
       "SoftwareReference": {"$ref": "#/definitions/SoftwareReference"},
       "URL": {"$ref": "#/definitions/URLtype"},
       "Description": {"type": "array", "items": {"type":"string"}}},
     "required": [],
     "additionalProperties": false},
   "SoftwareReference": {
     "type": "object",
     "properties": {
```

```
      "value": {"type": "string"},
      "spec-name": {"type": "string"},
      "ext-spec-name": {"type": "string"},
      "dtype": {"type": "string"},
      "ext-dtype": {"type": "string"}},
    "required": ["spec-name"],
    "additionalProperties": false},
  "StructuredInfo": {
    "type": "object",
    "properties": {
      "specID": {"type": "string"},
      "ext-specID": {"type": "string"},
      "contentID": {"type": "string"},
      "RawData": {"type": "string"},
      "URL": {"$ref": "#/definitions/URLtype"}},
    "required": ["specID"],
    "additionalProperties": false},
  "Incident": {
    "title": "Incident",
    "description": "JSON schema for Incident class",
    "type": "object",
    "properties": {
      "purpose": {"$ref": "#/definitions/purpose"},
      "ext-purpose": {"type": "string"},
      "status": {"$ref": "#/definitions/status"},
      "ext-status": {"type": "string"},
      "lang": {"$ref": "#/definitions/lang"},
      "restriction": {"$ref": "#/definitions/restriction"},
      "ext-restriction": {"type": "string"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "IncidentID": {"$ref": "#/definitions/IncidentID"},
      "AlternativeID": {"$ref": "#/definitions/AlternativeID"},
      "RelatedActivity": {
        "type": "array",
        "items": {"$ref": "#/definitions/RelatedActivity"}},
      "DetectTime": {"type": "string"},
      "StartTime": {"type": "string"},
      "EndTime": {"type": "string"},
      "RecoveryTime": {"type": "string"},
      "ReportTime": {"type": "string"},
      "GenerationTime": {"type": "string"},
      "Description": {"type": "array","items": {"type": "string"}},
      "Discovery": {
        "type": "array","items": {"$ref": "#/definitions/Discovery"}},
      "Assessment": {
        "type": "array","items": {"$ref": "#/definitions/Assessment"}},
      "Methods": {
        "type": "array","items": {"$ref": "#/definitions/Method"}},
```

```
        "Contacts": {
          "type": "array","items": {"$ref": "#/definitions/Contact"}},
        "EventData": {
          "type": "array","items": {"$ref": "#/definitions/EventData"}},
        "IndicatorList": {
          "type": "array","items": {"$ref": "#/definitions/Indicator"}},
        "History": {"$ref": "#/definitions/History"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["IncidentID","GenerationTime","Contacts","purpose"],
      "additionalProperties": false},
    "IncidentID": {
      "title": "IncidentID",
      "description": "JSON schema for IncidentID class",
      "type": "object",
      "properties": {
        "id": {"type": "string"},
        "name": {"type": "string"},
        "instance": {"type": "string"},
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"}},
      "required": ["name"],
      "additionalProperties": false},
    "AlternativeID": {
      "title": "AlternativeID",
      "description": "JSON schema for AlternativeID class",
      "type": "object",
      "properties": {
        "IncidentID": {
          "type": "array","items":{"$ref": "#/definitions/IncidentID"}},
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"}},
      "required": ["IncidentID"],
      "additionalProperties": false},
    "RelatedActivity": {
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "IncidentID": {
          "type": "array","items": {"$ref": "#/definitions/IncidentID"}},
        "URL": {
          "type": "array","items": {"$ref": "#/definitions/URLtype"}},
        "ThreatActor": {
          "type": "array","items": {"$ref": "#/definitions/ThreatActor"}},
        "Campaign": {
          "type": "array","items": {"$ref": "#/definitions/Campaign"}},
        "IndicatorID": {
          "type": "array","items": {"$ref": "#/definitions/IndicatorID"}},
        "Confidence": {"$ref": "#/definitions/Confidence"},
```

```
      "Description": { "type": "array","items": {"type": "string"}},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
    "additionalProperties": false},
  "ThreatActor": {
    "properties": {
      "restriction": {"$ref": "#/definitions/restriction"},
      "ext-restriction": {"type": "string"},
      "ThreatActorID": {"type": "array", "items": {"type": "string"}},
      "Description": {"type": "array", "items": {"type": "string"}},
      "URL": {"type":"array","items":{"$ref":"#/definitions/URLtype"}},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
    "additionalProperties": false},
  "Campaign": {
    "properties": {
      "restriction": {"$ref": "#/definitions/restriction"},
      "ext-restriction": {"type": "string"},
      "CampaignID": {"type": "array", "items": {"type": "string"}},
      "URL": {"type":"array", "items":{"$ref":"#/definitions/URLtype"}},
      "Description": {"type": "array", "items": {"type": "string"}},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}}},
  "Contact": {
    "type": "object",
    "properties": {
      "role": {
        "enum": ["creator","reporter","admin","tech","provider","user",
                 "billing","legal","irt","abuse","cc","cc-irt","leo",
                 "vendor","vendor-support","victim","victim-notified",
                 "ext-value"]},
      "ext-role": {"type": "string"},
      "type": {"enum": ["person","organization","ext-value"]},
      "ext-type": {"type": "string"},
      "restriction": {"$ref": "#/definitions/restriction"},
      "ext-restriction": {"type": "string"},
      "ContactName": {"type": "array", "items": {"type": "string"}},
      "ContactTitle": {"type": "array", "items": {"type": "string"}},
      "Description": {"type": "array", "items": {"type": "string"}},
      "RegistryHandle": {
        "type":"array", "items":{"$ref":"#/definitions/RegistryHandle"}},
      "PostalAddress": {
        "type":"array", "items":{"$ref":"#/definitions/PostalAddress"}},
      "Email": {"type": "array", "items": {"$ref": "#/definitions/Email"}}
,
      "Telephone": {
        "type": "array", "items": {"$ref": "#/definitions/Telephone"}},
      "Timezone": {"type": "string"},
      "Contact": {
        "type": "array", "items": {"$ref": "#/definitions/Contact"}},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
    "required": ["role","type"],
```

```
        "additionalProperties": false},
    "RegistryHandle": {
      "type": "object",
      "properties": {
        "handle": {"type": "string"},
        "registry": {
          "enum": ["internic","apnic","arin","lacnic","ripe","afrinic",
                   "local","ext-value"]},
        "ext-registry": {"type": "string"}},
      "required": ["registry"],
      "additionalProperties": false},
    "PostalAddress": {
      "type": "object",
      "properties": {
        "type": {"type": "string"},
        "ext-type": {"type": "string"},
        "PAddress": {"type": "string"},
        "Description": {"type": "array", "items": {"type": "string"}}},
      "required": ["PAddress"],
      "additionalProperties": false},
    "Email": {
      "type": "object",
      "properties": {
        "type": {
          "enum":["direct","hotline","ext-value"]},
        "ext-type": {"type": "string"},
        "EmailTo": {"type": "string"},
        "Description": {"type": "array", "items": {"type": "string"}}},
      "required": ["EmailTo"],
      "additionalProperties": false},
    "Telephone": {
      "type": "object",
      "properties": {
        "type": {
          "enum":["wired","mobile","fax","hotline","ext-value"]},
        "ext-type": {"type": "string"},
        "TelephoneNumber": {"type": "string"},
        "Description": {"type": "array", "items": {"type": "string"}}},
      "required": ["TelephoneNumber"],
      "additionalProperties": false},
    "Discovery": {
      "type": "object",
      "properties": {
        "source": {
          "enum":["nidps","hips","siem","av","third-party-monitoring",
                  "incident","os-log","application-log","device-log",
                  "network-flow","passive-dns","investigation","audit",
                  "internal-notification","external-notification","leo",
```

```
                   "partner","actor","unknown","ext-value"]},
        "ext-source": {"type": "string"},
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "Description": {"type": "array", "items": {"type": "string"}},
        "Contact": {
          "type": "array", "items": {"$ref": "#/definitions/Contact"}},
        "DetectionPattern": {
          "type":"array",
          "items":{"$ref":"#/definitions/DetectionPattern"}}},
      "required": [],
      "additionalProperties": false},
    "DetectionPattern": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Application": {"$ref": "#/definitions/SoftwareType"},
        "Description": {"type": "array", "items": {"type": "string"}},
        "DetectionConfiguration": {
          "type": "array", "items": {"type": "string"}}},
      "required": ["Application"],
      "additionalProperties": false},
    "Method": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "References": {
          "type": "array","items": {"$ref": "#/definitions/Reference"}},
        "Description": {"type": "array", "items": {"type": "string"}},
        "AttackPattern": {
          "type":"array", "items":{"$ref":"#/definitions/StructuredInfo"}},
        "Vulnerability": {
          "type":"array", "items":{"$ref":"#/definitions/StructuredInfo"}},
        "Weakness": {
          "type":"array", "items":{"$ref":"#/definitions/StructuredInfo"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "Reference": {
      "type": "object",
      "properties": {
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "ReferenceName": {"type": "string"},
        "URL":{"type":"array", "items":{"$ref":"#/definitions/URLtype"}},
        "Description": {"type": "array", "items": {"type": "string"}}},
```

```
      "required": [],
      "additionalProperties": false},
    "Assessment": {
      "type": "object",
      "properties": {
        "occurrence": {"enum":["actual","potential"]},
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "IncidentCategory": {"type": "array", "items": {"type": "string"}},
        "SystemImpact": {
          "type": "array", "items": {"$ref": "#/definitions/SystemImpact"}},
        "BusinessImpact": {
          "type":"array", "items":{"$ref":"#/definitions/BusinessImpact"}},
        "TimeImpact": {
          "type": "array", "items": {"$ref": "#/definitions/TimeImpact"}},
        "MonetaryImpact": {
          "type":"array", "items":{"$ref":"#/definitions/MonetaryImpact"}},
        "IntendedImpact": {
          "type":"array", "items":{"$ref":"#/definitions/BusinessImpact"}},
        "Counter": {
          "type": "array", "items": {"$ref": "#/definitions/Counter"}},
        "MitigatingFactor": {
          "type": "array", "items": {"$type": "string"}},
        "Cause": {"type": "array", "items": {"$type": "string"}},
        "Confidence": {"$ref": "#/definitions/Confidence"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "SystemImpact": {
      "type": "object",
      "properties": {
        "severity": {
          "enum":["low","medium","high"]},
        "completion": {"enum":["failed","succeeded"]},
        "type": {
          "enum":["takeover-account","takeover-service","takeover-system",
                  "cps-manipulation","cps-damage","availability-data",
                  "availability-account","availability-service",
                  "availability-system","damaged-system","damaged-data",
                  "breach-proprietary","breach-privacy","breach-credential",
                  "breach-configuration","integrity-data",
                  "integrity-configuration","integrity-hardware",
                  "traffic-redirection","monitoring-traffic",
                  "monitoring-host","policy","unknown","ext-value"]},
        "ext-type": {"type": "string"},
        "Description": {"type": "array","items": {"type": "string"}}},
      "required": ["type"],
```

```
      "additionalProperties": false},
    "BusinessImpact": {
      "type": "object",
      "properties": {
        "severity": {
          "enum":["none","low","medium","high","unknown","ext-value"]},
        "ext-severity": {"type":"string"},
        "type": {
          "enum":["breach-proprietary","breach-privacy","breach-credential",
                  "loss-of-integrity","loss-of-service","theft-financial",
                  "theft-service","degraded-reputation","asset-damage",
                  "asset-manipulation","legal","extortion","unknown",
                  "ext-value"]},
        "ext-type": {"type": "string"},
        "Description": {"type": "array","items": {"type": "string"}}},
      "required": ["type"],
      "additionalProperties": false},
    "TimeImpact": {
      "type": "object",
      "properties": {
        "value": {"type": "number"},
        "severity": {"enum": ["low","medium","high"]},
        "metric": {"enum": ["labor","elapsed","downtime","ext-value"]},
        "ext-metric": {"type": "string"},
        "duration": {"$ref":"#/definitions/duration"},
        "ext-duration": {"type": "string"}},
      "required": ["metric"],
      "additionalProperties": false},
    "MonetaryImpact": {
      "type": "object",
      "properties": {
        "value": {"type": "number"},
        "severity": {"enum":["low","medium","high"]},
        "currency": {"type": "string"}},
      "required": [],
      "additionalProperties": false},
    "Confidence": {
      "type": "object",
      "properties": {
        "value": {"type": "number"},
        "rating": {
          "enum": ["low","medium","high","numeric","unknown","ext-value"]},
        "ext-rating": {"type":"string"}},
      "required": ["rating"],
      "additionalProperties": false},
    "History": {
      "type": "object",
      "properties": {
```

```
          "restriction": {"$ref": "#/definitions/restriction"},
          "ext-restriction": {"type": "string"},
          "HistoryItem": {
            "type": "array","items": {"$ref": "#/definitions/HistoryItem"}}},
        "required": ["HistoryItem"],
        "additionalProperties": false},
      "HistoryItem": {
        "type": "object",
        "properties": {
          "action": {"$ref": "#/definitions/action"},
          "ext-action": {"type": "string"},
          "restriction": {"$ref": "#/definitions/restriction"},
          "ext-restriction": {"type": "string"},
          "observable-id": {"$ref": "#/definitions/IDtype"},
          "DateTime": {"$ref": "#/definitions/DATETIME"},
          "IncidentID": {"$ref": "#/definitions/IncidentID"},
          "Contact": {"$ref": "#/definitions/Contact"},
          "Description": {"type": "array","items": {"type": "string"}},
          "DefinedCOA": {"type": "array","items": {"type": "string"}},
          "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
        "required": ["DateTime","action"],
        "additionalProperties": false},
      "EventData": {
        "type": "object",
        "properties": {
          "restriction": {"$ref": "#/definitions/restriction"},
          "ext-restriction": {"type": "string"},
          "observable-id": {"$ref": "#/definitions/IDtype"},
          "Description": {"type": "array","items": {"type": "string"}},
          "DetectTime": {"type": "string"},
          "StartTime": {"type": "string"},
          "EndTime": {"type": "string"},
          "RecoveryTime": {"type": "string"},
          "ReportTime": {"type": "string"},
          "Contact": {
            "type": "array","items": {"$ref": "#/definitions/Contact"}},
          "Discovery": {
            "type": "array","items": {"$ref": "#/definitions/Discovery"}},
          "Assessment": {"$ref": "#/definitions/Assessment"},
          "Method": {
            "type": "array","items": {"$ref": "#/definitions/Method"}},
          "System": {
            "type": "array","items": {"$ref": "#/definitions/System"}},
          "Expectation": {
            "type": "array","items": {"$ref": "#/definitions/Expectation"}},
          "RecordData": {"type": "array",
                         "items": {"$ref": "#/definitions/RecordData"}},
          "EventData": {
```

```
        "type": "array","items": {"$ref": "#/definitions/EventData"}},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
    "required": ["ReportTime"],
    "additionalProperties": false},
  "Expectation": {
    "type": "object",
    "properties": {
      "action": {"$ref":"#/definitions/action"},
      "ext-action": {"type": "string"},
      "severity": {"enum": ["low","medium","high"]},
      "restriction": {"$ref": "#/definitions/restriction"},
      "ext-restriction": {"type": "string"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "Description": {"type": "array","items": {"type": "string"}},
      "DefinedCOA": {"type": "array","items": {"type": "string"}},
      "StartTime": {"type": "string"},
      "EndTime": {"type": "string"},
      "Contact": {"$ref": "#/definitions/Contact"}},
    "required": [],
    "additionalProperties": false},
  "System": {
    "type": "object",
    "properties": {
      "category": {
        "enum": ["source","target","intermediate","sensor",
                 "infrastructure","ext-value"]},
      "ext-category": {"type": "string"},
      "interface": {"type": "string"},
      "spoofed": {"enum": ["unknown","yes","no"]},
      "virtual": {"enum": ["yes","no","unknown"]},
      "ownership": {
        "enum":["organization","personal","partner","customer",
                "no-relationship","unknown","ext-value"]},
      "ext-ownership": {"type": "string"},
      "restriction": {"$ref": "#/definitions/restriction"},
      "ext-restriction": {"type": "string"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "Node": {"$ref": "#/definitions/Node"},
      "NodeRole": {
        "type": "array","items": {"$ref": "#/definitions/NodeRole"}},
      "Service": {
        "type": "array","items": {"$ref": "#/definitions/Service"}},
      "OperatingSystem": {
        "type": "array","items": {"$ref": "#/definitions/SoftwareType"}},
      "Counter": {
        "type": "array","items": {"$ref": "#/definitions/Counter"}},
      "AssetID": {"type": "array","items": {"type": "string"}},
      "Description": {"type": "array","items": {"type": "string"}},
```

```
       "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
     "required": ["Node"],
     "additionalProperties": false},
   "Node": {
     "type": "object",
     "properties": {
       "DomainData": {
         "type": "array","items": {"$ref": "#/definitions/DomainData"}},
       "Address": {
         "type": "array","items": {"$ref": "#/definitions/Address"}},
       "PostalAddress": {"type": "string"},
       "Location": {"type": "array","items": {"type": "string"}},
       "Counter": {"type":"array",
                   "items":{"$ref":"#/definitions/Counter"}}},
     "required": [],
     "additionalProperties": false},
   "Address": {
     "type": "object",
     "properties": {
       "value": {"type": "string"},
       "category": {
         "enum":["asn","atm","e-mail","ipv4-addr","ipv4-net",
                 "ipv4-net-masked","ipv4-net-mask","ipv6-addr","ipv6-net",
                 "ipv6-net-masked","mac","site-url","ext-value"]},
       "ext-category": {"type": "string"},
       "vlan-name": {"type": "string"},
       "vlan-num": {"type": "integer"},
       "observable-id": {"$ref": "#/definitions/IDtype"}},
     "required": ["category"],
     "additionalProperties": false},
   "NodeRole": {
     "type": "object",
     "properties": {
       "category": {
         "enum":["client","client-enterprise","clent-partner",
                 "client-remote","client-kiosk","client-mobile",
                 "server-internal","server-public","www","mail","webmail",
                 "messaging","streaming","voice","file","ftp","p2p","name",
                 "directory","credential","print","application","database",
                 "backup","dhcp","assessment","source-control",
                 "config-management","monitoring","infra","infra-firewall",
                 "infra-router","infra-switch","camera","proxy",
                 "remote-access","log","virtualization","pos", "scada",
                 "scada-supervisory","sinkhole","honeypot","anomyzation",
                 "c2-server","malware-distribution","drop-server",
                 "hot-point","reflector","phishing-site",
                 "spear-phishing-site","recruiting-site",
                 "fraudulent-site","ext-value"]},
```

```
      "ext-category": {"type": "string"},
      "Description": {"type": "array","items": {"type": "string"}}},
    "required": ["category"],
    "additionalProperties": false},
  "Counter": {
    "type": "object",
    "properties": {
      "value": {"type": "string"},
      "type": {"enum": ["count","peak","average","ext-value"]},
      "ext-type": {"type": "string"},
      "unit": {"enum": ["byte","mbit","packet","flow","session","alert",
               "message","event","host","site","organization",
               "ext-value"]},
      "ext-unit": {"type": "string"},
      "meaning": {"type": "string"},
      "duration": {"$ref":"#/definitions/duration"},
      "ext-duration": {"type": "string"}},
    "required": ["type","unit"],
    "additionalProperties": false},
  "DomainData": {
    "type": "object",
    "properties": {
      "system-status": {
        "enum": ["spoofed","fraudulent","innocent-hacked",
                 "innocent-hijacked","unknown","ext-value"]},
      "ext-system-status": {"type": "string"},
      "domain-status": {
        "enum": [
          "reservedDelegation","assignedAndActive","assignedAndInactive",
          "assignedAndOnHold","revoked","transferPending","registryLock",
          "registrarLock","other","unknown","ext-value"]},
      "ext-domain-status": {"type": "string"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "Name": {"type": "string"},
      "DateDomainWasChecked": {"$ref": "#/definitions/DATETIME"},
      "RegistrationDate": {"$ref": "#/definitions/DATETIME"},
      "ExpirationDate": {"$ref": "#/definitions/DATETIME"},
      "RelatedDNS": {
        "type": "array","items": {"$ref": "#/definitions/ExtensionType"}},
      "NameServers": {
        "type": "array","items": {"$ref": "#/definitions/NameServers"}},
      "DomainContacts": {
        "$ref": "#/definitions/DomainContacts"}},
    "required": ["Name","system-status","domain-status"],
    "additionalProperties": false},
  "NameServers": {
    "type": "object",
    "properties": {
```

```
      "Server": {"type": "string"},
      "Address": {"type":"array",
                  "items":{"$ref":"#/definitions/Address"}}},
    "required": ["Server","Address"],
    "additionalProperties": false},
  "DomainContacts": {
    "type": "object",
    "properties": {
      "SameDomainContact": {"type": "string"},
      "Contact": {"type":"array",
                  "items":{"$ref":"#/definitions/Contact"}}},
    "required": ["Contact"],
    "additionalProperties": false},
  "Service": {
    "type": "object",
    "properties": {
      "ip-protocol": {"type": "integer"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "ServiceName": {"$ref": "#/definitions/ServiceName"},
      "Port": {"type": "integer"},
      "Portlist": {"$ref": "#/definitions/PORTLIST"},
      "ProtoCode": {"type": "integer"},
      "ProtoType": {"type": "integer"},
      "ProtoField": {"type": "integer"},
      "ApplicationHeaderField":{"$ref":"#/definitions/ExtensionTypeList"},
      "EmailData": {"$ref": "#/definitions/EmailData"},
      "Application": {"$ref": "#/definitions/SoftwareType"}},
    "required": [],
    "additionalProperties": false},
  "ServiceName": {
    "type": "object",
    "properties": {
      "IANAService": {"type": "string"},
      "URL": {"type": "array","items": {"$ref": "#/definitions/URLtype"}},
      "Description": {"type": "array","items": {"type": "string"}}},
    "required": [],
    "additionalProperties": false},
  "EmailData": {
    "type": "object",
    "properties": {
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "EmailTo": {"type": "array","items": {"type": "string"}},
      "EmailFrom": {"type": "string"},
      "EmailSubject": {"type": "string"},
      "EmailX-Mailer": {"type": "string"},
      "EmailHeaderField": {
         "type": "array","items": {"$ref": "#/definitions/ExtensionType"}},
      "EmailHeaders": {"type": "string"},
```

```
      "EmailBody": {"type": "string"},
      "EmailMessage": {"type": "string"},
      "HashData": {
        "type": "array","items": {"$ref": "#/definitions/HashData"}},
      "Signature": {"type": "array","items": {"type": "string"}}},
    "required": [],
    "additionalProperties": false},
  "RecordData": {
    "type": "object",
    "properties": {
      "restriction": {"$ref": "#/definitions/restriction"},
      "ext-restriction": {"type": "string"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "DateTime": {"$ref": "#/definitions/DATETIME"},
      "Description": {"type": "array","items": {"type": "string"}},
      "Applicadtion": {"$ref": "#/definitions/SoftwareType"},
      "RecordPattern": {
        "type": "array","items": {"$ref": "#/definitions/RecordPattern"}},
      "RecordItem": {
        "type": "array","items": {"$ref": "#/definitions/ExtensionType"}},
      "URL": {
        "type": "array","items": {"$ref": "#/definitions/URLtype"}},
      "FileData": {
        "type": "array","items": {"$ref": "#/definitions/FileData"}},
      "WindowsRegistryKeysModified": {
        "type": "array",
        "items": {"$ref": "#/definitions/WindowsRegistryKeysModified"}},
      "CertificateData": {
        "type":"array","items":{"$ref":"#/definitions/CertificateData"}},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
    "required": [],
    "additionalProperties": false
  },
  "RecordPattern": {
    "type": "object",
    "properties": {
      "value": {"type": "string"},
      "type": {"enum": ["regex","binary","xpath","ext-value"]},
      "ext-type": {"type": "string"},
      "offset": {"type": "integer"},
      "offsetunit": {"enum":["line","byte","ext-value"]},
      "ext-offsetunit": {"type": "string"},
      "instance": {"type": "integer"}},
    "required": ["type"],
    "additionalProperties": false},
  "WindowsRegistryKeysModified": {
    "type": "object",
    "properties": {
```

```
           "observabile-id": {"$ref": "#/definitions/IDtype"},
           "Key": {"type": "array","items": {"$ref": "#/definitions/Key"}}},
         "required": ["Key"],
         "additionalProperties": false},
       "Key": {
         "type": "object",
         "properties": {
           "registryaction": {"enum": ["add-key","add-value","delete-key",
                               "delete-value","modify-key","modify-value",
                               "ext-value"]},
           "ext-registryaction": {"type": "string"},
           "observable-id": {"$ref": "#/definitions/IDtype"},
           "KeyName": {"type":"string"},
           "KeyValue": {"type": "string"}},
         "required": ["KeyName"],
         "additionalProperties": false},
       "CertificateData": {
         "type": "object",
         "properties": {
           "restriction": {"$ref": "#/definitions/restriction"},
           "ext-restriction": {"type": "string"},
           "observable-id": {"$ref": "#/definitions/IDtype"},
           "Certificate": {
             "type": "array","items": {"$ref": "#/definitions/Certificate"}}},
         "required": ["Certificate"],
         "additionalProperties": false},
       "Certificate": {
         "type": "object",
         "properties": {
           "observable-id": {"$ref": "#/definitions/IDtype"},
           "X509Data": {type: "string"},
           "Description": {"type": "array","items": {"type": "string"}}},
         "required": ["X509Data"],
         "additionalProperties": false},
       "FileData": {
         "type": "object",
         "properties": {
           "restriction": {"$ref": "#/definitions/restriction"},
           "ext-restriction": {"type": "string"},
           "observable-id": {"$ref": "#/definitions/IDtype"},
           "File": {"type": "array","items": {"$ref": "#/definitions/File"}}},
         "required": ["File"],
         "additionalProperties": false},
       "File": {
         "type": "object",
         "properties": {
           "FileName": {"type": "string"},
           "FileSize": {"type": "integer"},
```

```
      "FileType": {"type": "string"},
      "URL": {"type": "array","items": {"$ref": "#/definitions/URLtype"}},
      "HashData": {"$ref": "#/definitions/HashData"},
      "Signature": {"type": "array","items": {"type": "string"}},
      "AssociatedSoftware": {"$ref": "#/definitions/SoftwareType"},
      "FileProperties": {
        "type":"array","items":{"$ref":"#/definitions/ExtensionType"}}},
    "required": [],
    "additionalProperties": false},
  "HashData": {
    "type": "object",
    "properties": {
      "scope": {"enum": ["file-contents","file-pe-section","file-pe-iat",
                "file-pe-resource","file-pdf-object","email-hash",
                "email-hash-header","email-hash-body"]},
      "HashTargetID": {"type": "string"},
      "Hash": {"type": "array","items": {"$ref": "#/definitions/Hash"}},
      "FuzzyHash": {
        "type": "array","items": {"$ref": "#/definitions/FuzzyHash"}}},
    "required": ["scope"],
    "additionalProperties": false},
  "Hash": {
    "type": "object",
    "properties": {
      "DigestMethod": {"type": "string"},
      "DigestValue": {"type": "string"},
      "CanonicalizationMethod": {},
      "Application": {"$ref": "#/definitions/SoftwareType"}},
    "required": ["DigestMethod","DigestValue"],
    "additionalProperties": false},
  "FuzzyHash": {
    "type": "object",
    "properties": {
      "FuzzyHashValue": {
        "type": "array","items": {"$ref": "#/definitions/ExtensionType"}},
      "Application": {"$ref": "#/definitions/SoftwareType"},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
    "required": ["FuzzyHashValue"],
    "additionalProperties": false},
  "Indicator": {
    "type": "object",
    "properties": {
      "restriction": {"$ref": "#/definitions/restriction"},
      "ext-restriction": {"type": "string"},
      "IndicatorID": {"$ref": "#/definitions/IndicatorID"},
      "AlternativeIndicatorID": {
        "type": "array",
        "items": {"$ref": "#/definitions/AlternativeIndicatorID"}},
```

```
        "Description": {"type": "array","items": {"type": "string"}},
        "StartTime": {"$ref": "#/definitions/DATETIME"},
        "EndTime": {"$ref": "#/definitions/DATETIME"},
        "Confidence": {"$ref": "#/definitions/Confidence"},
        "Contact": {
          "type": "array","items": {"$ref": "#/definitions/Contact"}},
        "Observable": {"$ref": "#/definitions/Observable"},
        "uid-ref": {"type": "string"},
        "IndicatorExpression":{"$ref":"#/definitions/IndicatorExpression"},
        "IndicatorReference": {"$ref": "#/definitions/IndicatorReference"},
        "NodeRole": {
          "type": "array","items": {"$ref": "#/definitions/NodeRole"}},
        "AttackPhase": {
          "type": "array","items": {"$ref": "#/definitions/AttackPhase"}},
        "Reference": {
          "type": "array","items": {"$ref": "#/definitions/Reference"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["IndicatorID"],
      "additionalProperties": false},
    "IndicatorID": {
      "type": "object",
      "properties": {
        "id": {"type": "string"},
        "name": {"type": "string"},
        "version": {"type": "string"}},
      "required": ["name","version"],
      "additionalProperties": false},
    "AlternativeIndicatorID": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "IndicatorReference": {
          "type": "array",
          "items": {"$ref": "#/definitions/IndicatorReference"}}},
      "required": ["IndicatorReference"],
      "additionalProperties": false},
    "Observable": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "System": {"$ref": "#/definitions/System"},
        "Address": {"$ref": "#/definitions/Address"},
        "DomainData": {"$ref": "#/definitions/DomainData"},
        "EmailData": {"$ref": "#/definitions/EmailData"},
        "Service": {"$ref": "#/definitions/Service"},
        "WindowsRegistryKeysModified": {
```

```
              "$ref": "#/definitions/WindowsRegistryKeysModified"},
          "FileData": {"$ref": "#/definitions/FileData"},
          "CertificateData": {"$ref": "#/definitions/CertificateData"},
          "RegistryHandle": {"$ref": "#/definitions/RegistryHandle"},
          "RecordData": {"type": "array",
                         "item": {"$ref": "#/definitions/Record"}},
          "EventData": {"$ref": "#/definitions/EventData"},
          "Incident": {"$ref": "#/definitions/Incident"},
          "Expectation": {"$ref": "#/definitions/Expectation"},
          "Reference": {"$ref": "#/definitions/Reference"},
          "Assessment": {"$ref": "#/definitions/Assessment"},
          "DetectionPattern": {"$ref": "#/definitions/DetectionPattern"},
          "HistoryItem": {"$ref": "#/definitions/HistoryItem"},
          "BulkObservable": {"$ref": "#/definitions/BulkObservable"},
          "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
       "required": [],
       "additionalProperties": false},
    "BulkObservable": {
       "type": "object",
       "properties": {
          "type": {"enum": ["asn","atm","e-mail","ipv4-addr","ipv4-net",
                   "ipv4-net-mask","ipv6-addr","ipv6-net","ipv6-net-mask",
                   "mac","site-url","domain-name","domain-to-ipv4",
                   "domain-to-ipv6","domain-to-ipv4-timestamp",
                   "domain-to-ipv6-timestamp","ipv4-port","ipv6-port",
                   "windows-reg-key","file-hash","email-x-mailer",
                   "email-subject","http-user-agent","http-request-url",
                   "mutex","file-path","user-name","ext-value"]},
          "ext-type": {"type": "string"},
          "BulkObservableFormant":{
             "$ref": "#/definitions/BulkObservableFormat"},
          "BulkObservableList": {"type": "array", "item":{"type": "string"}},
          "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
       "required": [],
       "additionalProperties": false},
    "BulkObservableFormat": {
       "type": "object",
       "properties": {
          "Hash": {"$ref": "#/definitions/Hash"},
          "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
       "required": [],
       "additionalProperties": false},
    "IndicatorExpression": {
       "type": "object",
       "properties": {
          "operator": {"enum": ["not","and","or","xor"]},
          "ext-operator": {"type": "string"},
          "IndicatorExpression": {
```

```
            "type": "array",
            "items": {"$ref": "#/definitions/IndicatorExpression"}},
         "Observable": {
            "type": "array","items": {"$ref": "#/definitions/Observable"}},
         "uid-ref": {"type": "string"},
         "IndicatorReference": {
            "type": "array",
           "items": {"$ref": "#/definitions/IndicatorReference"}},
         "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
       "required": [],
       "additionalProperties": false},
     "IndicatorReference": {
       "type": "object",
       "properties": {
         "uid-ref": {"type": "string"},
         "euid-ref": {"type": "string"},
         "version": {"type": "string"}},
       "required": [],
       "additionalProperties": false},
     "AttackPhase": {
       "type": "object",
       "properties": {
         "AttackPhaseID": {"type": "array","items": {"type": "string"}},
         "URL": {"type": "array","items": {"$ref": "#/definitions/URLtype"}},
         "Description": {"type": "array","items": {"type": "string"}},
         "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
       "required": [],
       "additionalProperties": false}},
   "title": "IODEF-Document",
   "description": "JSON schema for IODEF-Document class",
   "type": "object",
   "properties": {
     "version": {"type": "string"},
     "lang": {"$ref": "#/definitions/lang"},
     "format-id": {"type": "string"},
     "private-enum-name": {"type": "string"},
     "private-enum-id": {"type": "string"},
     "Incident": {
       "type": "array","items": {"$ref": "#/definitions/Incident"}},
       "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
   "required": ["version","Incident"],
   "additionalProperties": false}
```

                        Figure 3: JSON schema

Authors' Addresses

    Takeshi Takahashi
    National Institute of Information and Communications Technology
    4-2-1 Nukui-Kitamachi
    Koganei, Tokyo 184-8795
    Japan

    Phone: +81 42 327 5862
    Email: takeshi_takahashi@nict.go.jp

    Roman Danyliw
    CERT, Software Engineering Institute, Carnegie Mellon University
    4500 Fifth Avenue
    Pittsburgh, PA
    USA

    Email: rdd@cert.org

    Mio Suzuki
    National Institute of Information and Communications Technology
    4-2-1 Nukui-Kitamachi
    Koganei, Tokyo 184-8795
    Japan

    Email: mio@nict.go.jp