CBOR/JSON binding of IODEF
draft-ietf-mile-jsoniodef-08

Abstract

   The Incident Object Description Exchange Format defined in RFC 7970
   provides an information model and a corresponding XML data model for
   exchanging incident and indicator information. This draft gives
   implementers and operators an alternative format to exchange the same
   information by defining an alternative data model implementation in
   CBOR/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 December 31, 2019.

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

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 CDDL [RFC8610] and 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", "NOT RECOMMENDED", "MAY", and
   "OPTIONAL" in this document are to be interpreted as described in BCP
   14 [RFC2119][RFC8174] when, and only when, they appear in all
   capitals, as shown here.

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] Reference	JSON Data Type
INTEGER	Section 2.1	"integer" per [jsonschema]
REAL	Section 2.2	"number" per [jsonschema]
CHARACTER	Section 2.3	"string" per [jsonschema]
STRING	Section 2.3	"string" per [jsonschema]
ML_STRING	Section 2.4	see Section 2.2.1
BYTE	Section 2.5.1	"string" per [jsonschema]
BYTE[]	Section 2.5.1	"string" per [jsonschema]
HEXBIN	Section 2.5.2	"string" per [jsonschema]
HEXBIN[]	Section 2.5.2	"string" per [jsonschema]
ENUM	Section 2.6	"enum" array per [jsonschema]
DATETIME	Section 2.7	"string" per [jsonschema]
TIMEZONE	Section 2.8	"string" per [jsonschema]
PORTLIST	Section 2.9	"string" per [jsonschema]
POSTAL	Section 2.10	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
STRUCTUREDINFO	[RFC 7203]	see Section 2.2.3
EXTENSION	Section 2.16	see Section 2.2.4

Figure 1: JSON Data Types

```
+----------------+------------------+-------------------------------+
| IODEF Data Type | CBOR Data Type  |          CDDL prelude         |
|                 |                 | [draft-ietf-cbor-cddl-05]     |
+----------------+------------------+-------------------------------+
| INTEGER         | 0, 1, 6 tag 2,  | integer                       |
|                 |  6 tag 3        |                               |
| REAL            | 7 bits 26       | float32                       |
| CHARACTER       | 3               | text                          |
| STRING          | 3               | text                          |
| ML_STRING       | 5               | Maps/Structs (Section 3.5.1)  |
| BYTE            | 6 tag 22        | eb64legacy                    |
| BYTE[]          | 6 tag 22        | eb64legacy                    |
| HEXBIN          | 2               | bytes                         |
| HEXBIN[]        | 2               | bytes                         |
| ENUM            | -               | Choices (Section 2.2.2)       |
| DATETIME        | 6 tag 0         | tdate                         |
| TIMEZONE        | 3               | text                          |
| PORTLIST        | 3               | text                          |
| POSTAL          | 3               | ML_STRING (Section 2.2.1)     |
| PHONE           | 3               | text                          |
| EMAIL           | 3               | text                          |
| URL             | 6 tag 32        | uri                           |
| ID              | 3               | text                          |
| IDREF           | 3               | text                          |
| SOFTWARE        | 5               | Maps/Structs (Section 3.5.1)  |
| STRUCTUREDINFO  | 5               | Maps/Structs (Section 3.5.1)  |
| EXTENSION       | 5               | Maps/Structs (Section 3.5.1)  |
+----------------+------------------+-------------------------------+
```

Figure 2: CBOR Data Types

2.2. Complex JSON Types

2.2.1. Multilingual Strings

   A string that needs to be represented in a human-readable language
   different from the default encoding of the document is represented in
   the information model by the ML_STRING data type. This data type is
   implemented as either an object with "value", "lang", and
   "translation-id" elements or a text string 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 Software Reference

   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 Uniform Resource Locator (URL) [RFC3986], or
   with free-form text. The SOFTWARE data type is implemented as an
   object with "SoftwareReference", "URL", and "Description" 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. Structured Information

   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.

   "StructuredInfo": {
     "SpecID": "urn:ietf:params:xml:ns:mile:cwe:3.3",   //ENUM
     "ContentID": "CWE-89"   //STRING
   }

   When embedding the raw data, base64 encoding defined in Section 4 of
   [RFC4648] should be used for encoding the data, as shown below.

   "StructuredInfo": {
     "SpecID": "urn:ietf:params:xml:ns:mile:mmdef:1.2",   //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",                                         //ENUM
  "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 using CDDL.

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

```
|                           | RelatedActivity*   |              |
|                           | DetectTime?        |              |
|                           | StartTime?         |              |
|                           | EndTime?           |              |
|                           | RecoveryTime?      |              |
|                           | ReportTime?        |              |
|                           | GenerationTime     |              |
|                           | Description*       |              |
|                           | 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*       |              |
|                           | AdditionalData*    |              |
+---------------------------+--------------------+--------------+
| Campaign                  | restriction?       |              |
|                           | ext-restriction?   |              |
|                           | CampaignID*        |              |
```

```
|                            | URL*                 |              |
|                            | Description*         |              |
|                            | AdditionalData*      | 3.8          |
+----------------------------+----------------------+--------------+
| Contact                    | role                 |              |
|                            | ext-role?            |              |
|                            | type                 |              |
|                            | ext-type?            |              |
|                            | restriction?         |              |
|                            | ext-restriction?     |              |
|                            | ContactName*,        |              |
|                            | ContactTitle*        |              |
|                            | Description*         |              |
|                            | RegistryHandle*      |              |
|                            | PostalAddress*       |              |
|                            | Email*               |              |
|                            | Telephone*           |              |
|                            | Timezone?            |              |
|                            | Contact*             |              |
|                            | AdditionalData*      | 3.9          |
+----------------------------+----------------------+--------------+
| RegistryHandle             | handle               |              |
|                            | registry             |              |
|                            | ext-registry?        | 3.9.1        |
+----------------------------+----------------------+--------------+
| PostalAddress              | type?                |              |
|                            | ext-type?            |              |
|                            | PAddress             |              |
|                            | Description*         | 3.9.2        |
+----------------------------+----------------------+--------------+
| Email                      | type?                |              |
|                            | ext-type?            |              |
|                            | EmailTo              |              |
|                            | Description*         | 3.9.3        |
+----------------------------+----------------------+--------------+
| Telephone                  | type?                |              |
|                            | ext-type?            |              |
|                            | TelephoneNumber      |              |
|                            | Description*         | 3.9.4        |
+----------------------------+----------------------+--------------+
| Discovery                  | source?              |              |
|                            | ext-source?          |              |
|                            | restriction?         |              |
|                            | ext-restriction?     |              |
|                            | Description*         |              |
|                            | Contact*             |              |
|                            | DetectionPattern*    | 3.10         |
+----------------------------+----------------------+--------------+
```

```
|  DetectionPattern        | restriction?        | 3.10.1       |
|                          | ext-restriction?    |              |
|                          | observable-id?      |              |
|                          | Application         |              |
|                          | Description*        |              |
|                          | DetectionConfiguration*  |         |
+--------------------------+---------------------+--------------+
|  Method                  | restriction?        |              |
|                          | ext-restriction?    |              |
|                          | Reference*          |              |
|                          | Description*        |              |
|                          | AttackPattern*      |              |
|                          | Vulnerability*      |              |
|                          | Weakness*           |              |
|                          | AdditionalData*     | 3.11         |
+--------------------------+---------------------+--------------+
|  Reference               | observable-id?      |              |
|                          | ReferenceName?      |              |
|                          | URL*                |              |
|                          | Description*        | 3.11.1       |
+--------------------------+---------------------+--------------+
|  Assessment              | occurence?          |              |
|                          | restriction?        |              |
|                          | ext-restriction?    |              |
|                          | observable-id?      |              |
|                          | IncidentCategory*   |              |
|                          | SystemImpact*       |              |
|                          | BusinessImpact*     |              |
|                          | TimeImpact*         |              |
|                          | MonetaryImpact*     |              |
|                          | IntendedImpact*     |              |
|                          | Counter*            |              |
|                          | MitigatingFactor*   |              |
|                          | Cause*              |              |
|                          | Confidence?         |              |
|                          | AdditionalData*     | 3.12         |
+--------------------------+---------------------+--------------+
|  SystemImpact            | severity?           |              |
|                          | completion?         |              |
|                          | type                |              |
|                          | ext-type?           |              |
|                          | Description*        | 3.12.1       |
+--------------------------+---------------------+--------------+
|  BusinessImpact          | severity?           |              |
|                          | ext-severity?       |              |
|                          | type                |              |
|                          | ext-type?           |              |
|                          | Description*        | 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* DefinedCOA* AdditionalData*	 3.13.1
EventData	restriction? ext-restriction? observable-id? Description* DetectTime? StartTime? EndTime? RecoveryTime? ReportTime? Contact* Discovery* Assessment? Method* System* Expectation* RecordData*	

	EventData*		
	AdditionalData*	3.14	
Expectation	action?		
	ext-action?		
	severity?		
	restriction?		
	ext-restriction?		
	observable-id?		
	Description*		
	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*		
	AdditionalData*	3.17	
Node	DomainData*		
	Address*		
	PostalAddress?		
	Location*		
	Counter*	3.18	
Address	value		
	category		
	ext-category?		
	vlan-name?		
	vlan-num?		
	observable-id?	3.18.1	
NodeRole	category		
	ext-category?		

```
|                            | Description*         | 3.18.2       |
+----------------------------+---------------------+--------------+
| Counter                    | value               |              |
|                            | type                |              |
|                            | ext-type?           |              |
|                            | unit                |              |
|                            | ext-unit?           |              |
|                            | meaning?            |              |
|                            | duration?           |              |
|                            | ext-duration?       | 3.18.3       |
+----------------------------+---------------------+--------------+
| DomainData                 | system-status       |              |
|                            | ext-system-status?  |              |
|                            | domain-status       |              |
|                            | ext-domain-status?  |              |
|                            | observable-id?      |              |
|                            | Name                |              |
|                            | DateDomainWasChecked?|             |
|                            | RegistrationDate?   |              |
|                            | ExpirationDate?     |              |
|                            | RelatedDNS*         |              |
|                            | Nameservers*        |              |
|                            | DomainContacts?     | 3.19         |
+----------------------------+---------------------+--------------+
| Nameserver                 | Server              |              |
|                            | Address*            | 3.19.1       |
+----------------------------+---------------------+--------------+
| DomainContacts             | SameDomainContact?  |              |
|                            | Contact+            | 3.19.2       |
+----------------------------+---------------------+--------------+
| Service                    | ip-protocol?        |              |
|                            | observable-id?      |              |
|                            | ServiceName?        |              |
|                            | Port?               |              |
|                            | Portlist?           |              |
|                            | ProtoCode?          |              |
|                            | ProtoType?          |              |
|                            | ProtoField?         |              |
|                            | ApplicationHeaderField*|           |
|                            | EmailData?          |              |
|                            | Application?        | 3.20         |
+----------------------------+---------------------+--------------+
| ServiceName                | IANAService?        |              |
|                            | URL*                |              |
|                            | Description*        | 3.20.1       |
+----------------------------+---------------------+--------------+
| EmailData                  | observable-id?      |              |
|                            | EmailTo*            |              |
```

```
|                            | EmailFrom?        |            |
|                            | EmailSubject?     |            |
|                            | EmailX-Mailer?    |            |
|                            | EmailHeaderField* |            |
|                            | EmailHeaders?     |            |
|                            | EmailBody?        |            |
|                            | EmailMessage?     |            |
|                            | HashData*         |            |
|                            | Signature*        | 3.21       |
+----------------------------+-------------------+------------+
| RecordData                 | restriction?      |            |
|                            | ext-restriction?  |            |
|                            | observable-id?    |            |
|                            | DateTime?         |            |
|                            | Description*      |            |
|                            | Application?      |            |
|                            | RecordPattern*    |            |
|                            | RecordItem*       |            |
|                            | URL*              |            |
|                            | FileData*         |            |
|                            | WindowsRegistryKeysModified*|  |
|                            | CertificateData*  |            |
|                            | AdditionalData*   | 3.22.1     |
+----------------------------+-------------------+------------+
| RecordPattern              | type              |            |
|                            | ext-type?         |            |
|                            | offset?           |            |
|                            | offsetunit?       |            |
|                            | ext-offsetunit?   |            |
|                            | instance?         |            |
|                            | value             | 3.22.2     |
+----------------------------+-------------------+------------+
| WindowsRegistryKeysModified | observable-id?   | 3.23       |
|                            | Key+              |            |
+----------------------------+-------------------+------------+
| Key                        | registryaction?   |            |
|                            | ext-registryaction?|           |
|                            | observable-id?    |            |
|                            | KeyName           |            |
|                            | KeyValue?         | 3.23.1     |
+----------------------------+-------------------+------------+
| CertificateData            | restriction?      |            |
|                            | ext-restriction?  |            |
|                            | observable-id?    |            |
|                            | Certificate+      | 3.24       |
+----------------------------+-------------------+------------+
| Certificate                | observable-id?    |            |
|                            | X509Data          |            |
```

	Description*	3.24.1
FileData	restriction? ext-restriction? observable-id? File+	3.25
File	observable-id? FileName? FileSize? FileType? URL* HashData? Signature* AssociatedSoftware? FileProperties*	3.25.1
HashData	scope HashTargetID? Hash* FuzzyHash*	3.26
Hash	DigestMethod DigestValue CanonicalizationMethod? Application?	3.26.1
FuzzyHash	FuzzyHashValue+ Application? AdditionalData*	3.26.2
Indicator	restriction? ext-restriction? IndicatorID AlternativeIndicatorID* Description* StartTime? EndTime? Confidence? Contact* Observable? uid-ref? IndicatorExpression? IndicatorReference? NodeRole* AttackPhase* Reference* AdditionalData*	3.29

```
+----------------------------+----------------------+--------------+
| IndicatorID                | id                   |              |
|                            | name                 |              |
|                            | version              | 3.29.1       |
+----------------------------+----------------------+--------------+
| AlternativeIndicatorID     | restriction?         |              |
|                            | ext-restriction?     |              |
|                            | IndicatorID+         | 3.29.2       |
+----------------------------+----------------------+--------------+
| Observable                 | restriction?         |              |
|                            | ext-restriction?     |              |
|                            | System?              |              |
|                            | Address?             |              |
|                            | DomainData?          |              |
|                            | Service?             |              |
|                            | EmailData?           |              |
|                            | WindowsRegistryKeysModified?|       |
|                            | FileData?            |              |
|                            | CertificateData?     |              |
|                            | RegistryHandle?      |              |
|                            | RecordData?          |              |
|                            | EventData?           |              |
|                            | Incident?            |              |
|                            | Expectation?         |              |
|                            | Reference?           |              |
|                            | Assessment?          |              |
|                            | DetectionPattern?    |              |
|                            | HistoryItem?         |              |
|                            | BulkObservable?      |              |
|                            | AdditionalData*      | 3.29.3       |
+----------------------------+----------------------+--------------+
| BulkObservable             | type?                |              |
|                            | ext-type?            |              |
|                            | BulkObservableFormat?|              |
|                            | BulkObservableList   |              |
|                            | AdditionalData*      | 3.29.4       |
+----------------------------+----------------------+--------------+
| BulkObservableFormat       | Hash?                |              |
|                            | AdditionalData*      | 3.29.5       |
+----------------------------+----------------------+--------------+
| IndicatorExpression        | operator?            |              |
|                            | ext-operator?        |              |
|                            | IndicatorExpression* |              |
|                            | Observable*          |              |
|                            | uid-ref*             |              |
|                            | IndicatorReference*  |              |
|                            | Confidence?          |              |
|                            | AdditionalData*      | 3.29.6       |
```

```
+---------------------------+--------------------+--------------+
| IndicatorReference        | uid-ref?           |              |
|                           | euid-ref?          |              |
|                           | version?           | 3.29.7       |
+---------------------------+--------------------+--------------+
| AttackPhase               | AttackPhaseID*     |              |
|                           | URL*               |              |
|                           | Description*       |              |
|                           | AdditionalData*    | 3.29.8       |
+---------------------------+--------------------+--------------+
```

Figure 3: IODEF Classes

3.2. Mapping between CBOR/JSON and XML IODEF

   o This document treats attributes and elements of each class defined
      in [RFC7970] with no distinction 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
      class.

   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 MLStringType were modified to support simple string by
      allowing the type to have not only a predefined object type but

        also text type, in order to allow simple descriptions of elements
        of the type.

    o The elements of ML_STRING type in XML IODEF document are presented
       as either STRING type or ML_STRING type in CBOR/JSON IODEF
       document.

    o Data models of the extension classes defined by [RFC7203] and
       referenced by [RFC7970] are represented by StructuredInfo class
       defined in this document.

    o Signature, X509Data, and RawData are encoded with base64 and are
       represented as string (BYTE type) in CBOR/JSON IODEF documents.

4. Examples

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

4.1. Minimal Example

    A document containing only the mandatory elements and attributes is
    shown below in JSON and CBOR, respectively.

```
{
  "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"}]
      }]
  }]
}
```

                    Figure 4: A Minimal Example in JSON

    A3   # map(3)
      67   # text(7)

```
      76657273696F6E                         # "version"
    63                                        # text(3)
      322E30                                  # "2.0"
    64                                        # text(4)
      6C616E67                                # "lang"
    62                                        # text(2)
      656E                                    # "en"
    68                                        # text(8)
      496E636964656E74                        # "Incident"
    81                                        # array(1)
      A5                                      # map(5)
        67                                    # text(7)
          707572706F7365                      # "purpose"
        69                                    # text(9)
          7265706F7274696E67                  # "reporting"
        6B                                    # text(11)
          7265737472696374696F6E              # "restriction"
        67                                    # text(7)
          70726976617465                      # "private"
        6A                                    # text(10)
          496E636964656E744944                # "IncidentID"
        A2                                    # map(2)
          62                                  # text(2)
            6964                              # "id"
          66                                  # text(6)
            343932333832                      # "492382"
          64                                  # text(4)
            6E616D65                          # "name"
          71                                  # text(17)
            63736972742E6578616D706C652E636F6D # "csirt.example.com"
        6E                                    # text(14)
          47656E65726174696F6E54696D65        # "GenerationTime"
        C0                                    # tag(0)
          78 19                               # text(25)
            323031352D30372D31385430393A30303A30302D30353A3030
                                              # "2015-07-18T09:00:00-05:00"
        67                                    # text(7)
          436F6E74616374                      # "Contact"
        81                                    # array(1)
          A3                                  # map(3)
            64                                # text(4)
              74797065                        # "type"
            6C                                # text(12)
              6F7267616E697A6174696F6E        # "organization"
            64                                # text(4)
              726F6C65                        # "role"
            67                                # text(7)
              63726561746F72                  # "creator"
```

```
             65                             # text(5)
                456D61696C                  # "Email"
             81                             # array(1)
               A1                           # map(1)
                  67                         # text(7)
                     456D61696C546F         # "EmailTo"
                  78 19                      # text(25)
                     636F6E746163744063736972742E6578616D706C652E636F6D
                                            # "contact@csirt.example.com"
```

                   Figure 5: A Minimal Example in CBOR

4.2. Indicators from a Campaign

   An example of C2 domains from a given campaign is shown below in JSON
   and CBOR, respectively.

```
{
  "version": "2.0",
  "lang": "en",
  "Incident": [{
    "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 campaign of the Aggressive Butterfly crime gang."],
    "Assessment": [{
      "Impact": [{"BusinessImpact": {"type": "breach-proprietary"}}]
    }],
    "Contact": [{
      "type": "organization",
      "role": "creator",
      "ContactName": ["CSIRT for example.com"],
      "Email": [{
```

```
        "EmailTo": "contact@csirt.example.com"
      }]
    }],
    "Indicator": [{
      "IndicatorID": {
        "id": "G90823490",
        "name": "csirt.example.com",
        "version": "1"
      },
      "Description": ["C2 domains"],
      "StartTime": "2014-12-02T11:18:00-05:00",
      "Observable": {
        "BulkObservable": {
          "type": "ipv6-addr",
          "BulkObservableList": "kj290023j09r34.example.com"}
      }
    }]
  }]
}
```

                Figure 6: Indicators from a Campaign in JSON

```
A3                                       # map(3)
  67                                     # text(7)
    76657273696F6E                       # "version"
  63                                     # text(3)
    322E30                               # "2.0"
  64                                     # text(4)
    6C616E67                             # "lang"
  62                                     # text(2)
    656E                                 # "en"
  68                                     # text(8)
    496E636964656E74                     # "Incident"
  81                                     # array(1)
    A9                                   # map(9)
      67                                 # text(7)
        707572706F7365                   # "purpose"
      65                                 # text(5)
        7761746368                       # "watch"
      6B                                 # text(11)
        7265737472696374696F6E           # "restriction"
      65                                 # text(5)
        677265656E                       # "green"
      6A                                 # text(10)
        496E636964656E744944             # "IncidentID"
      A2                                 # map(2)
        62                               # text(2)
          6964                           # "id"
```

```
      66                                  # text(6)
        383937393233                      # "897923"
      64                                  # text(4)
        6E616D65                          # "name"
      71                                  # text(17)
        63736972742E6578616D706C652E636F6D # "csirt.example.com"
    6F                                    # text(15)
      52656C61746564416374697669747   # "RelatedActivity"
    81                                    # array(1)
      A2                                  # map(2)
        6B                                # text(11)
          54687265617441637   # "ThreatActor"
        81                                # array(1)
          A2                              # map(2)
            6D                            # text(13)
              5468726561744163746F724944 # "ThreatActorID"
            81                            # array(1)
              78 1A                       # text(26)
                54412D31322D41474752455353  4956452D425554544552464
                C59                       # "TA-12-AGGRESSIVE-BUTTERFLY"
            6B                            # text(11)
              4465736372697074696F6E      # "Description"
            81                            # array(1)
              74                          # text(20)
                4167677265737369766520427574746572666C79
                                          # "Aggressive Butterfly"
        68                                # text(8)
          43616D706169676E                # "Campaign"
        81                                # array(1)
          A2                              # map(2)
            6A                            # text(10)
              43616D706169676E4944        # "CampaignID"
            81                            # array(1)
              6C                          # text(12)
                432D323031352D3539343035  # "C-2015-59405"
            6B                            # text(11)
              4465736372697074696F6E      # "Description"
            81                            # array(1)
              6E                          # text(14)
                4F72616E676520476972616666 65 # "Orange Giraffe"
    6E                                    # text(14)
      47656E65726174696F6E54696D65        # "GenerationTime"
    C0                                    # tag(0)
      78 19                               # text(25)
        323031352D31302D30325431313A31383A30302D30353A3030
                                          # "2015-10-02T11:18:00-05:00"
    6B                                    # text(11)
      4465736372697074696F6E              # "Description"
```

```
81                                       # array(1)
  78 6F                                  # text(111)
    53756D6D6172697A65732074686520496E64696361746F7273206F6620436
    F6D70726F6D69736520666F7220746865204F72616E676520476972616666
    652063616D706169676E206F6620746865204167677265737369766520427
    574746572666C79206372696D652067616E672E
        # "Summarizes the Indicators of Compromise for the Orange
          Giraffe campaign of the Aggressive Butterfly crime gang."
6A                                       # text(10)
  4173736573736D656E74                   # "Assessment"
81                                       # array(1)
  A1                                     # map(1)
    66                                   # text(6)
      496D70616374                       # "Impact"
    81                                   # array(1)
      A1                                 # map(1)
        6E                               # text(14)
          427573696E657373496D70616374 # "BusinessImpact"
        A1                               # map(1)
          64                             # text(4)
            74797065                     # "type"
          72                             # text(18)
            6272656163682D70726F7072696574617279
                                         # "breach-proprietary"
67                                       # text(7)
  436F6E7461637.4                        # "Contact"
81                                       # array(1)
  A4                                     # map(4)
    64                                   # text(4)
      74797065                           # "type"
    6C                                   # text(12)
      6F7267616E697A6174696F6E           # "organization"
    64                                   # text(4)
      726F6C65                           # "role"
    67                                   # text(7)
      63726561746F72                     # "creator"
    6B                                   # text(11)
      436F6E746163744E616D65             # "ContactName"
    81                                   # array(1)
      75                                 # text(21)
        435349525420666F72206578616D706C652E636F6D
                                         # "CSIRT for example.com"
    65                                   # text(5)
      456D61696C                         # "Email"
    81                                   # array(1)
      A1                                 # map(1)
        67                               # text(7)
          456D61696C546F                 # "EmailTo"
```

```
            78 19                         # text(25)
              636F6E746163744063736972742E6578616D706C652E636F6D
                                          # "contact@csirt.example.com"
      69                                  # text(9)
        496E64696361746F72                # "Indicator"
      81                                  # array(1)
        A4                                # map(4)
          6B                              # text(11)
            496E64696361746F724944        # "IndicatorID"
          A3                              # map(3)
            62                            # text(2)
              6964                        # "id"
            69                            # text(9)
              473930383233343930          # "G90823490"
            64                            # text(4)
              6E616D65                    # "name"
            71                            # text(17)
              63736972742E6578616D706C652E636F6D
                                          # "csirt.example.com"
            67                            # text(7)
              76657273696F6E              # "version"
            61                            # text(1)
              31                          # "1"
          6B                              # text(11)
            4465736372697074696F6E        # "Description"
          81                              # array(1)
            6A                            # text(10)
              433220646F6D61696E73        # "C2 domains"
          69                              # text(9)
            537461727454696D65            # "StartTime"
          C0                              # tag(0)
            78 19                         # text(25)
              323031342D31322D30325431313A31383A30302D30353A3030
                                          # "2014-12-02T11:18:00-05:00"
          6A                              # text(10)
            4F627365727661626C65          # "Observable"
          A1                              # map(1)
            6E                            # text(14)
              42756C6B4F627365727661626C65 # "BulkObservable"
            A2                            # map(2)
              64                          # text(4)
                74797065                  # "type"
              69                          # text(9)
                697076362D61646472        # "ipv6-addr"
              72                          # text(18)
                42756C6B4F627365727661626C654C697374
                                          # "BulkObservableList"
              78 1A                       # text(26)
```

               6B6A3239303032336A30397233342E6578616D706C652E636F6D
                                    # "kj290023j09r34.example.com"

             Figure 7: Indicators from a Campaign in CBOR

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 = "" / text .regexp "[a-zA-Z]{1,8}(-[a-zA-Z0-9]{1,8})*"

restriction = "public" / "partner" / "need-to-know" / "private" /
              "default" / "white" / "green" / "amber" / "red" /
              "ext-value"
SpecID = "urn:ietf:params:xml:ns:mile:mmdef:1.2" /  "private"
IDtype = text .regexp "[a-zA-Z_][a-zA-Z0-9_.-]*"
IDREFType = IDtype
URLtype = uri
TimeZonetype = text .regexp "Z|[\+\-](0[0-9]|1[0-4]):[0-5][0-9]"
PortlistType = text .regexp "\\d+(\\-\\d+)?(,\\d+(\\-\\d+)?)*"
action = "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" / "other" / "ext-value"

DATETIME = tdate

BYTE = eb64legacy

MLStringType = {
```

```
      value: text
    ? lang: lang
    ? translation-id: text
} / text

PositiveFloatType = float32 .gt 0

PAddressType = MLStringType

ExtensionType  = {
 value: text
 ? name: text
 dtype: "boolean" / "byte" / "bytes" / "character" / "date-time" /
         "ntpstamp" / "integer" / "portlist" / "real" / "string" /
         "file" / "path" / "frame" / "packet" / "ipv4-packet" / "json"/
         "ipv6-packet" / "url" / "csv" / "winreg" / "xml" / "ext-value"
         .default "string"
 ? ext-dtype: text
 ? meaning: text
 ? formatid: text
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 ? observable-id: IDtype
}

SoftwareType = {
 ? SoftwareReference: SoftwareReference
 ? URL: [+ URLtype]
 ? Description: [+ MLStringType]
}

SoftwareReference = {
 ? value: text
 spec-name: "custom" / "cpe" / "swid" / "ext-value"
 ? ext-spec-name: text
 ? dtype: "bytes" / "integer" / "real" / "string" / "xml" / "ext-value"
         .default "string"
 ? 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 .default "private"
 ? ext-restriction: text
 ? observable-id: IDtype
 IncidentID: IncidentID
 ? AlternativeID: AlternativeID
 ? RelatedActivity: [+ RelatedActivity]
 ? DetectTime: DATETIME
 ? StartTime: DATETIME
 ? EndTime: DATETIME
 ? RecoveryTime: DATETIME
 ? ReportTime: DATETIME
 GenerationTime: DATETIME
 ? Description: [+ MLStringType]
 ? Discovery: [+ Discovery]
 ? Assessment: [+ Assessment]
 ? Method: [+ Method]
 Contact: [+ Contact]
 ? EventData: [+ EventData]
 ? Indicator: [+ Indicator]
 ? History: History
 ? AdditionalData: [+ ExtensionType]
}

IncidentID = {
 id: text
 name: text
 ? instance: text
 ? restriction: restriction .default "private"
 ? ext-restriction: text
}

AlternativeID = {
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 IncidentID: [+ IncidentID]
}

RelatedActivity = {
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 ? IncidentID: [+ IncidentID]
 ? URL: [+ URLtype]
 ? ThreatActor: [+ ThreatActor]
 ? Campaign: [+ Campaign]
 ? IndicatorID: [+ IndicatorID]
 ? Confidence: Confidence
 ? Description: [+ text]
 ? AdditionalData: [+ ExtensionType]
```

```
}

ThreatActor = {
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 ? ThreatActorID: [+ text]
 ? URL: [+ URLtype]
 ? Description: [+ MLStringType]
 ? AdditionalData: [+ ExtensionType]
}

Campaign  = {
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 ? CampaignID: [+ text]
 ? URL: [+ URLtype]
 ? Description: [+ MLStringType]
 ? 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 .default "private"
 ? ext-restriction: text
 ? ContactName: [+ MLStringType]
 ? ContactTitle: [+ MLStringType]
 ? Description: [+ MLStringType]
 ? RegistryHandle: [+ RegistryHandle]
 ? PostalAddress: [+ PostalAddress]
 ? Email: [+ Email]
 ? Telephone: [+ Telephone]
 ? Timezone: TimeZonetype
 ? Contact: [+ Contact]
 ? AdditionalData: [+ ExtensionType]
}

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

```
PostalAddress = {
 ? type: "street" / "mailing" / "ext-value"
 ? ext-type: text
 PAddress: PAddressType
 ? Description: [+ MLStringType]
}

Email = {
 ? type: "direct" / "hotline" / "ext-value"
 ? ext-type: text
 EmailTo: text
 ? Description: [+ MLStringType]
}

Telephone = {
 ? type: "wired" / "mobile" / "fax" / "hotline" / "ext-value"
 ? ext-type: text
 TelephoneNumber: text
 ? Description: [+ MLStringType]
}

Discovery = {
 ? source: "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: text
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 ? Description: [+ MLStringType]
 ? Contact: [+ Contact]
 ? DetectionPattern: [+ DetectionPattern]
}

DetectionPattern = {
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 ? observable-id: IDtype
 (Description: [+ MLStringType] // DetectionConfiguration: [+ text])
 Application: SoftwareType
}

Method = {
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 ? Reference: [+ Reference]
 ? Description: [+ MLStringType]
```

```
 ? AttackPattern: [+ StructuredInfo]
 ? Vulnerability: [+ StructuredInfo]
 ? Weakness: [+ StructuredInfo]
 ? AdditionalData: [+ ExtensionType]
}

StructuredInfo = {
 SpecID: SpecID
 ? ext-SpecID: text
 ? ContentID: text
 ? (RawData: [+ BYTE] // Reference:[+ Reference])
 ? Platform:[+ Platform]
 ? Scoring:[+ Scoring]
}

Platform = {
    SpecID: SpecID
    ? ext-SpecID: text
    ? ContentID: text
    ? RawData: [+ BYTE]
    ? Reference: [+ Reference]
}
Scoring = {
    SpecID: SpecID
    ? ext-SpecID: text
    ? ContentID: text
    ? RawData: [+ BYTE]
    ? Reference: [+ Reference]
}
Reference = {
 ? observable-id: IDtype
 ? ReferenceName: ReferenceName
 ? URL: [+ URLtype]
 ? Description: [+ MLStringType]
}

ReferenceName = {
 specIndex: integer
 ID: IDtype
}

Assessment = {
 ? occurrence: "actual" / "potential"
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 ? observable-id: IDtype
 ? IncidentCategory: [+ MLStringType]
 Impact: [+ {SystemImpact: SystemImpact} /
```

```
           {BusinessImpact: BusinessImpact} / {TimeImpact: TimeImpact} /
           {MonetaryImpact: MonetaryImpact} /
           {IntendedImpact: BusinessImpact}]
 ? Counter: [+ Counter]
 ? MitigatingFactor: [+ MLStringType]
 ? Cause: [+ MLStringType]
 ? 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" /
       "breach-configuration" / "integrity-data" /
       "integrity-configuration" / "integrity-hardware" /
       "traffic-redirection" / "monitoring-traffic" / "monitoring-host"/
       "policy" / "unknown" / "ext-value" .default "unknown"
 ? ext-type: text
 ? Description: [+ MLStringType]
}

BusinessImpact = {
 ? severity:"none" / "low" / "medium" / "high" / "unknown" / "ext-value"
            .default "unknown"
 ? 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" .default "unknown"
 ? ext-type: text
 ? Description: [+ MLStringType]
}

TimeImpact = {
 value: PositiveFloatType
 ? severity: "low" / "medium" / "high"
 metric: "labor" / "elapsed" / "downtime" / "ext-value"
 ? ext-metric: text
 ? duration: duration .default "hour"
 ? ext-duration: text
}
```

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

Confidence = {
 value: float32
 rating: "low" / "medium" / "high" / "numeric" / "unknown" / "ext-value"
 ? ext-rating: text
}

History = {
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 HistoryItem: [+ HistoryItem]
}

HistoryItem = {
 action: action .default "other"
 ? ext-action: text
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 ? observable-id: IDtype
 DateTime: DATETIME
 ? IncidentID: IncidentID
 ? Contact: Contact
 ? Description: [+ MLStringType]
 ? DefinedCOA: [+ text]
 ? AdditionalData: [+ ExtensionType]
}

EventData = {
 ? restriction: restriction .default "default"
 ? ext-restriction: text
 ? observable-id: IDtype
 ? Description: [+ MLStringType]
 ? 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 .default "other"
 ? ext-action: text
 ? severity: "low" / "medium" / "high"
 ? restriction: restriction .default "default"
 ? ext-restriction: text
 ? observable-id: IDtype
 ? Description: [+ MLStringType]
 ? 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" .default "unknown"
 ? virtual: "yes" / "no" / "unknown" .default "unknown"
 ? ownership: "organization" / "personal" / "partner" / "customer" /
              "no-relationship" / "unknown" / "ext-value"
 ? ext-ownership: text
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 ? observable-id: IDtype
 Node: Node
 ? NodeRole: [+ NodeRole]
 ? Service: [+ Service]
 ? OperatingSystem: [+ SoftwareType]
 ? Counter: [+ Counter]
 ? AssetID: [+ text]
 ? Description: [+ MLStringType]
 ? AdditionalData: [+ ExtensionType]
}

Node = {
 (DomainData:[+ DomainData]
  ? Address:[+ Address] //
  ? DomainData:[+ DomainData]
  Address:[+ Address])
 ? PostalAddress: PostalAddress
```

```
 ? Location: [+ MLStringType]
 ? 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-uri" /
           "ext-value" .default "ipv6-addr"
 ? ext-category: text
 ? vlan-name: text
 ? vlan-num: integer
 ? observable-id: IDtype
}

NodeRole = {
 category: "client" / "client-enterprise" / "client-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" / "hop-point" / "reflector" /
           "phishing-site" / "spear-phishing-site" / "recruiting-site" /
           "fraudulent-site" / "ext-value"
 ? ext-category: text
 ? Description: [+ MLStringType]
}

Counter = {
 value: float32
 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
 ? duration: duration .default "hour"
 ? 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: integer
 ? observable-id: IDtype
 ? ServiceName: ServiceName
 ? Port: integer
 ? Portlist: PortlistType
 ? ProtoCode: integer
 ? ProtoType: integer
 ? ProtoField: integer
 ? ApplicationHeaderField: [+ ExtensionType]
 ? EmailData: EmailData
 ? Application: SoftwareType
}

ServiceName = {
 ? IANAService: text
 ? URL: [+ URLtype]
 ? Description: [+ MLStringType]
}
```

```
EmailData = {
 ? observable-id: IDtype
 ? EmailTo: [+ text]
 ? EmailFrom: text
 ? EmailSubject: text
 ? EmailX-Mailer: text
 ? EmailHeaderField: [+ ExtensionType]
 ? EmailHeaders: text
 ? EmailBody: text
 ? EmailMessage: text
 ? HashData: [+ HashData]
 ? Signature: [+ BYTE]
}

RecordData = {
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 ? observable-id: IDtype
 ? DateTime: DATETIME
 ? Description: [+ MLStringType]
 ? Application: SoftwareType
 ? RecordPattern: [+ RecordPattern]
 ? RecordItem: [+ ExtensionType]
 ? URL: [+ URLtype]
 ? FileData: [+ FileData]
 ? WindowsRegistryKeysModified: [+ WindowsRegistryKeysModified]
 ? CertificateData: [+ CertificateData]
 ? AdditionalData: [+ ExtensionType]
}

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

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 .default "private"
 ? ext-restriction: text
 ? observable-id: IDtype
 Certificate: [+ Certificate]
}

Certificate = {
 ? observable-id: IDtype
 X509Data: BYTE
 ? Description: [+ MLStringType]
}

FileData = {
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 ? observable-id: IDtype
 File: [+ File]
}

File = {
 ? observable-id: IDtype
 ? FileName: text
 ? FileSize: integer
 ? FileType: text
 ? URL: [+ URLtype]
 ? HashData: HashData
 ? Signature: [+ BYTE]
 ? AssociatedSoftware: SoftwareType
 ? FileProperties: [+ ExtensionType]
}

HashData = {
 scope: "file-contents" / "file-pe-section" / "file-pe-iat" /
        "file-pe-resource" / "file-pdf-object" / "email-hash" /
        "email-headers-hash" / "email-body-hash" / "ext-value"
 ? HashTargetID: text
 ? Hash: [+ Hash]
 ? FuzzyHash: [+ FuzzyHash]
}
```

```
Hash = {
 DigestMethod: BYTE
 DigestValue: BYTE
 ? CanonicalizationMethod: BYTE
 ? Application: SoftwareType
}

FuzzyHash = {
 FuzzyHashValue: [+ ExtensionType]
 ? Application: SoftwareType
 ? AdditionalData: [+ ExtensionType]
}

Indicator = {
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 IndicatorID: IndicatorID
 ? AlternativeIndicatorID: [+ AlternativeIndicatorID]
 ? Description: [+ MLStringType]
 ? StartTime: DATETIME
 ? EndTime: DATETIME
 ? Confidence: Confidence
 ? Contact: [+ Contact]
 (Observable: Observable // uid-ref: IDREFType //
  IndicatorExpression: IndicatorExpression //
  IndicatorReference: IndicatorReference)
 ? NodeRole: [+ NodeRole]
 ? AttackPhase: [+ AttackPhase]
 ? Reference: [+ Reference]
 ? AdditionalData: [+ ExtensionType]
}

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

AlternativeIndicatorID = {
 ? restriction: restriction .default "private"
 ? ext-restriction: text
 IndicatorID: [+ IndicatorID]
}

Observable = {
 ? restriction: restriction .default "private"
 ? 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-uri" / "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" .default "and"
 ? ext-operator: text
 ? IndicatorExpression: [+ IndicatorExpression]
 ? Observable: [+ Observable]
 ? uid-ref: [+ IDREFType]
 ? IndicatorReference: [+ IndicatorReference]
 ? Confidence: Confidence
 ? AdditionalData: [+ ExtensionType]
}

IndicatorReference = {
 (uid-ref: IDREFType // euid-ref: text)
 ? version: text
}

AttackPhase = {
 ? AttackPhaseID: [+ text]
```

```
 ? URL: [+ URLtype]
 ? Description: [+ MLStringType]
 ? AdditionalData: [+ ExtensionType]
}
```

                    Figure 8: Data Model in CDDL

6. IANA Considerations

    This document does not require any IANA actions.

7. Security Considerations

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

8. Acknowledgments

    We would like to thank Henk Birkholz, Carsten Bormann, Yasuaki
    Morita, and Takahiko Nagata for their insightful comments on CDDL.

9. References

9.1. Normative References

    [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>.

    [RFC3986]   Berners-Lee, T., Fielding, R., and L. Masinter, "Uniform
                Resource Identifier (URI): Generic Syntax", STD 66,
                RFC 3986, DOI 10.17487/RFC3986, January 2005,
                <https://www.rfc-editor.org/info/rfc3986>.

    [RFC4648]   Josefsson, S., "The Base16, Base32, and Base64 Data
                Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006,
                <https://www.rfc-editor.org/info/rfc4648>.

    [RFC7203]   Takahashi, T., Landfield, K., and Y. Kadobayashi, "An
                Incident Object Description Exchange Format (IODEF)
                Extension for Structured Cybersecurity Information",
                RFC 7203, DOI 10.17487/RFC7203, April 2014,
                <https://www.rfc-editor.org/info/rfc7203>.

    [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>.

   [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC
              2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174,
              May 2017, <https://www.rfc-editor.org/info/rfc8174>.

   [RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data
              Definition Language (CDDL): A Notational Convention to
              Express Concise Binary Object Representation (CBOR) and
              JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610,
              June 2019, <https://www.rfc-editor.org/info/rfc8610>.

9.2. Informative References

   [jsonschema]
              Francis Galiegue, Kris Zyp, and Gary Court, "JSON Schema:
              core definitions and terminology", 2013.

Appendix A. Data Types used in this document

   The CDDL prelude used in this document is mapped to JSON as shown in
   the table below.

CDDL Prelude	Use of JSON	Instance	Validation
bytes	n/a	string	tool available
text	string	string	unnecessary
tdate	n/a	string	7.3.1 date-time
integer	n/a	number	integer
eb64legacy	n/a	string	tool available
uri	n/a	string	7.3.6 uri
float32	float32	number	unnecessary

                  Figure 9: CDDL Prelude mapping in JSON

Appendix B. The IODEF Data Model (JSON Schema)

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

```
{ "$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","other",
      "ext-value"]},
    "duration":{"enum":["second","minute","hour","day","month",
      "quarter","year","ext-value"]},
    "SpecID":{
      "enum":["urn:ietf:params:xml:ns:mile:mmdef:1.2","private"]},
    "lang": {
      "type":"string","pattern":"^$|[a-zA-Z]{1,8}(-[a-zA-Z0-9]{1,8})*"},
    "purpose": {"enum": ["traceback","mitigation","reporting","watch",
      "other","ext-value"]},
    "restriction":{"enum":["public","partner","need-to-know","private",
      "default","white","green","amber","red","ext-value"]},
    "status": {"enum": ["new","in-progress","forwarded","resolved",
      "future","ext-value"]},
    "DATETIME": {"type": "string","format": "date-time"},
    "BYTE": {"type": "string"},
    "PortlistType": {
      "type": "string","pattern": "\\d+(\\-\\d+)?(,\\d+(\\-\\d+)?)*"},
    "TimeZonetype": {
      "type":"string","pattern":"Z|[\\+\\-](0[0-9]|1[0-4]):[0-5][0-9]"},
    "URLtype": {
      "type": "string",
      "pattern":
        "^(([^:/?#]+):)?(//([^/?#]*))?([^?#]*)(\\?([^#]*))?(#(.*))?"},
    "IDtype": {"type": "string","pattern": "[a-zA-Z_][a-zA-Z0-9_.-]*"},
    "IDREFType": {"$ref": "#/definitions/IDtype"},
    "MLStringType": {
      "oneOf": [{"type": "string"},
               {"type": "object",
                 "properties": {
                   "value": {"type": "string"},
                   "lang": {"$ref": "#/definitions/lang"},
                   "translation-id": {"type": "string"}},
                 "required": ["value"],
                 "additionalProperties":false}]},
    "PositiveFloatType": {"type": "number","minimum": 0},
    "PAddressType": {"$ref": "#/definitions/MLStringType"},
    "ExtensionType": {
      "type": "object",
      "properties": {
        "value": {"type": "string"},
        "name": {"type": "string"},
        "dtype":{"enum":["boolean","byte","bytes","character", "json",
          "date-time","ntpstamp","integer","portlist","real","string",
          "file","path","frame","packet","ipv4-packet","ipv6-packet",
          "url", "csv","winreg","xml","ext-value"],"default": "string"},
        "ext-dtype": {"type": "string"},
        "meaning": {"type": "string"},
```

```
         "formatid": {"type": "string"},
         "restriction": {
           "$ref": "#/definitions/restriction","default": "private"},
         "ext-restriction": {"type": "string"},
         "observable-id": {"$ref": "#/definitions/IDtype"}},
      "required": ["value","dtype"],
      "additionalProperties":false},
    "ExtensionTypeList": {
      "type": "array",
      "items": {"$ref": "#/definitions/ExtensionType"},
      "minItems": 1},
    "SoftwareType": {
      "type": "object",
      "properties": {
        "SoftwareReference":{"$ref": "#/definitions/SoftwareReference"},
        "URL": {
          "type": "array",
          "items": {"$ref": "#/definitions/URLtype",
          "minItems": 1}},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1 }},
      "required": [],
      "additionalProperties": false},
    "SoftwareReference": {
      "type": "object",
      "properties": {
        "value": {"type": "string"},
        "spec-name": {"enum": ["custom","cpe","swid","ext-value"]},
        "ext-spec-name": {"type": "string"},
        "dtype": {"enum": ["bytes","integer","real","string","xml",
                          "ext-value"] ,  "default": "string"},
        "ext-dtype": {"type": "string"}},
      "required": ["spec-name"],
      "additionalProperties": false},
    "StructuredInfo": {
      "type": "object",
      "properties": {
        "SpecID": {"$ref":"#/definitions/SpecID"},
        "ext-SpecID": {"type": "string"},
        "ContentID": {"type": "string"},
        "RawData": {
           "type": "array",
           "items": {"$ref":"#/definitions/BYTE"},
           "minItems": 1
        },
        "Reference": {
```

```
            "type": "array",
            "items": {"$ref": "#/definitions/Reference"},
            "minItems": 1
          },
          "Platform": {
            "type": "array",
            "items": {"$ref": "#/definitions/Platform"},
            "minItems": 1
          },
          "Scoring": {
            "type": "array",
            "items": {"$ref": "#/definitions/Scoring"},
            "minItems": 1}},
        "allOf": [
            {"required": ["SpecID"]},
            {"anyOf": [
              {"oneOf": [
                {"required":["Reference"]},
                {"required":["RawData"]}]},
              { "not" : {"required":["Reference", "RawData"]}}]}]],
        "additionalProperties": false},
      "Platform": {
        "type": "object",
        "properties": {
          "SpecID": {"$ref":"#/definitions/SpecID"},
          "ext-SpecID": {"type": "string"},
          "ContentID": {"type": "string"},
          "RawData": {
            "type": "array",
            "items": {"$ref":"#/definitions/BYTE"},
            "minItems": 1
          },
          "Reference": {
            "type": "array",
            "items": {"$ref": "#/definitions/Reference"},
            "minItems": 1}},
        "required": ["SpecID"],
        "additionalProperties": false},
      "Scoring": {
        "type": "object",
        "properties": {
          "SpecID": {"$ref":"#/definitions/SpecID"},
          "ext-SpecID": {"type": "string"},
          "ContentID": {"type": "string"},
          "RawData": {
            "type": "array",
            "items": {"$ref":"#/definitions/BYTE"},
            "minItems": 1
```

```
      },
      "Reference": {
        "type": "array",
        "items": {"$ref": "#/definitions/Reference"},
        "minItems": 1}},
    "required": ["SpecID"],
    "additionalProperties": false},
  "Incident": {
    "title": "Incident",
    "description": "JSON schema for Incident class",
    "type": "object",
    "properties": {
      "purpose": {"$ref": "#/definitions/purpose"},
      "ext-purpose": {"type": "string"},
      "status": {"$ref": "#/definitions/status"},
      "ext-status": {"type": "string"},
      "lang": {"$ref": "#/definitions/lang"},
      "restriction": {"$ref": "#/definitions/restriction",
                      "default": "private"},
      "ext-restriction": {"type": "string"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "IncidentID": {"$ref": "#/definitions/IncidentID"},
      "AlternativeID": {"$ref": "#/definitions/AlternativeID"},
      "RelatedActivity": {
        "type": "array",
        "items": {"$ref": "#/definitions/RelatedActivity"},
        "minItems": 1},
      "DetectTime": {"$ref": "#/definitions/DATETIME"},
      "StartTime": {"$ref": "#/definitions/DATETIME"},
      "EndTime": {"$ref": "#/definitions/DATETIME"},
      "RecoveryTime": {"$ref": "#/definitions/DATETIME"},
      "ReportTime": {"$ref": "#/definitions/DATETIME"},
      "GenerationTime": {"$ref": "#/definitions/DATETIME"},
      "Description": {
        "type": "array",
        "items": {"$ref": "#/definitions/MLStringType"},
        "minItems": 1},
      "Discovery": {
        "type": "array",
        "items": {"$ref": "#/definitions/Discovery"},
        "minItems": 1},
      "Assessment": {
        "type": "array",
        "items": {"$ref": "#/definitions/Assessment"},
        "minItems": 1},
      "Method": {
        "type": "array",
        "items": {"$ref": "#/definitions/Method"},
```

```
            "minItems": 1},
          "Contact": {
            "type": "array",
            "items": {"$ref": "#/definitions/Contact"},
            "minItems": 1},
          "EventData": {
            "type": "array",
            "items": {"$ref": "#/definitions/EventData"},
            "minItems": 1},
          "Indicator": {
            "type": "array",
            "items": {"$ref": "#/definitions/Indicator"},
            "minItems": 1},
          "History": {"$ref": "#/definitions/History"},
          "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
        "required": ["IncidentID","GenerationTime","Contact","purpose"],
        "additionalProperties": false},
      "IncidentID": {
        "title": "IncidentID",
        "description": "JSON schema for IncidentID class",
        "type": "object",
        "properties": {
          "id": {"type": "string"},
          "name": {"type": "string"},
          "instance": {"type": "string"},
          "restriction": {"$ref": "#/definitions/restriction",
                          "default": "private"},
          "ext-restriction": {"type": "string"}},
        "required": ["id","name"],
        "additionalProperties": false},
      "AlternativeID": {
        "title": "AlternativeID",
        "description": "JSON schema for AlternativeID class",
        "type": "object",
        "properties": {
          "IncidentID": {
            "type": "array",
            "items":{"$ref": "#/definitions/IncidentID"},
            "minItems": 1},
          "restriction": {"$ref": "#/definitions/restriction",
                          "default": "private"},
          "ext-restriction": {"type": "string"}},
        "required": ["IncidentID"],
        "additionalProperties": false},
      "RelatedActivity": {
        "properties": {
          "restriction": {"$ref": "#/definitions/restriction",
                          "default": "private"},
```

```
        "ext-restriction": {"type": "string"},
        "IncidentID": {
          "type": "array",
          "items": {"$ref": "#/definitions/IncidentID"},
          "minItems": 1},
        "URL": {
          "type": "array",
          "items": {"$ref": "#/definitions/URLtype"},
          "minItems": 1},
        "ThreatActor": {
          "type": "array",
          "items": {"$ref": "#/definitions/ThreatActor"},
          "minItems": 1},
        "Campaign": {
          "type": "array",
          "items": {"$ref": "#/definitions/Campaign"},
          "minItems": 1},
        "IndicatorID": {
          "type": "array",
          "items": {"$ref": "#/definitions/IndicatorID"},
          "minItems": 1},
        "Confidence": {"$ref": "#/definitions/Confidence"},
        "Description": {
          "type": "array",
          "items": {"type": "string"},
          "minItems": 1},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "additionalProperties": false},
    "ThreatActor": {
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "ThreatActorID": {
          "type": "array",
          "items": {"type": "string"},
          "minItems": 1},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "URL": {
          "type":"array",
          "items":{"$ref":"#/definitions/URLtype"},
          "minItems": 1},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "additionalProperties": false},
    "Campaign": {
```

```
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "CampaignID": {
          "type": "array",
          "items": {"type": "string"},
          "minItems": 1},
        "URL": {
          "type":"array",
          "items":{"$ref":"#/definitions/URLtype"},
          "minItems": 1},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "AdditionalData": {"$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": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "ContactName": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "ContactTitle": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "RegistryHandle": {
          "type":"array",
          "items":{"$ref":"#/definitions/RegistryHandle"},
          "minItems": 1},
        "PostalAddress": {
```

```
            "type":"array",
            "items":{"$ref":"#/definitions/PostalAddress"},
            "minItems": 1},
        "Email": {
          "type": "array",
          "items": {"$ref": "#/definitions/Email"},
          "minItems": 1},
        "Telephone": {
          "type": "array",
          "items": {"$ref": "#/definitions/Telephone"},
          "minItems": 1},
        "Timezone": {"$ref": "#/definitions/TimeZonetype"},
        "Contact": {
          "type": "array",
          "items": {"$ref": "#/definitions/Contact"},
          "minItems": 1},
        "AdditionalData": {"$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": ["handle","registry"],
      "additionalProperties": false},
    "PostalAddress": {
      "type": "object",
      "properties": {
        "type": {
          "enum": ["street","mailing","ext-value"]},
        "ext-type": {"type": "string"},
        "PAddress": {"$ref": "#/definitions/PAddressType"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1}},
      "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": {"$ref": "#/definitions/MLStringType"},
            "minItems": 1}},
        "required": ["EmailTo"],
        "additionalProperties": false},
      "Telephone": {
        "type": "object",
        "properties": {
          "type": {
            "enum":["wired","mobile","fax","hotline","ext-value"]},
          "ext-type": {"type": "string"},
          "TelephoneNumber": {"type": "string"},
          "Description": {
            "type": "array",
            "items": {"$ref": "#/definitions/MLStringType"},
            "minItems": 1}},
        "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": {"$ref": "#/definitions/restriction",
                          "default": "private"},
          "ext-restriction": {"type": "string"},
          "Description": {
            "type": "array",
            "items": {"$ref": "#/definitions/MLStringType"},
            "minItems": 1},
          "Contact": {
            "type": "array",
            "items": {"$ref": "#/definitions/Contact"},
            "minItems": 1},
          "DetectionPattern": {
            "type":"array",
            "items":{"$ref":"#/definitions/DetectionPattern"},
            "minItems": 1}},
        "required": [],
        "additionalProperties": false},
      "DetectionPattern": {
```

```
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Application": {"$ref": "#/definitions/SoftwareType"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "DetectionConfiguration": {
          "type": "array",
          "items": {"type": "string"},
          "minItems": 1}},
      "allOf": [
        {"required": ["Application"]},
        {"oneOf": [
          {"required":["Description"]},
          {"required":["DetectionConfiguration"]}]}],
      "additionalProperties": false},
    "Method": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "Reference": {
          "type": "array",
          "items": {"$ref": "#/definitions/Reference"},
          "minItems": 1},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "AttackPattern": {
          "type":"array",
          "items":{"$ref":"#/definitions/StructuredInfo"},
          "minItems": 1},
        "Vulnerability": {
          "type":"array",
          "items":{"$ref":"#/definitions/StructuredInfo"},
          "minItems": 1},
        "Weakness": {
          "type":"array",
          "items":{"$ref":"#/definitions/StructuredInfo"},
          "minItems": 1},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
```

```
      "required": [],
      "additionalProperties": false},
    "Reference": {
      "type": "object",
      "properties": {
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "ReferenceName": {"$ref":"#/definitions/ReferenceName"},
        "URL":{
          "type":"array",
          "items":{"$ref":"#/definitions/URLtype"},
          "minItems": 1},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1}},
      "required": [],
      "additionalProperties": false},
    "ReferenceName" : {
      "type": "object",
      "properties": {
        "specIndex": {"type": "number"},
        "ID": {"$ref":"#/definitions/IDtype"}},
      "required": ["specIndex","ID"],
      "additionalProperties": false},
    "Assessment": {
      "type": "object",
      "properties": {
        "occurrence": {"enum":["actual","potential"]},
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "IncidentCategory": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "Impact": {
         "type": "array",
         "items": {
           "properties": {
             "SystemImpact":{"$ref":"#/definitions/SystemImpact"},
             "BusinessImpact":{"$ref":"#/definitions/BusinessImpact"},
             "TimeImpact":{"$ref":"#/definitions/TimeImpact"},
             "MonetaryImpact":{"$ref":"#/definitions/MonetaryImpact"},
             "IntendedImpact":{"$ref":"#/definitions/BusinessImpact"}},
           "additionalProperties":false},
         "minItems" : 1
        },
```

```
          "Counter": {
            "type": "array",
            "items": {"$ref": "#/definitions/Counter"},
            "minItems": 1},
          "MitigatingFactor": {
            "type": "array",
            "items": {"$ref": "#/definitions/MLStringType"},
            "minItems": 1},
          "Cause": {
            "type": "array",
            "items": {"$ref": "#/definitions/MLStringType"},
            "minItems": 1},
          "Confidence": {"$ref": "#/definitions/Confidence"},
          "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
        "required": ["Impact"],
        "additionalProperties": false},
      "SystemImpact": {
        "type": "object",
        "properties": {
          "severity": {"enum":["low","medium","high"]},
          "completion": {"enum":["failed","succeeded"]},
          "type": {
            "enum":["takeover-account","takeover-service",
              "takeover-system","cps-manipulation","cps-damage",
              "availability-data","availability-account",
              "availability-service","availability-system",
              "damaged-system","damaged-data","breach-proprietary",
              "breach-privacy","breach-credential",
              "breach-configuration","integrity-data",
              "integrity-configuration","integrity-hardware",
              "traffic-redirection","monitoring-traffic",
              "monitoring-host","policy","unknown","ext-value"]},
          "ext-type": {"type": "string"},
          "Description": {
            "type": "array",
            "items": {"$ref": "#/definitions/MLStringType"},
            "minItems": 1}},
        "required": ["type"],
        "additionalProperties": false},
      "BusinessImpact": {
        "type": "object",
        "properties": {
          "severity": {"enum":["none","low","medium","high","unknown",
                    "ext-value"],"default": "unknown"},
          "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": {"$ref": "#/definitions/MLStringType"},
        "minItems": 1}},
    "required": ["type"],
    "additionalProperties": false},
  "TimeImpact": {
    "type": "object",
    "properties": {
      "value": {"$ref": "#/definitions/PositiveFloatType"},
      "severity": {"enum": ["low","medium","high"]},
      "metric": {"enum": ["labor","elapsed","downtime","ext-value"]},
      "ext-metric": {"type": "string"},
      "duration": {"$ref":"#/definitions/duration","default": "hour"},
      "ext-duration": {"type": "string"}},
    "required": ["value","metric"],
    "additionalProperties": false},
  "MonetaryImpact": {
    "type": "object",
    "properties": {
      "value": {"$ref": "#/definitions/PositiveFloatType"},
      "severity": {"enum":["low","medium","high"]},
      "currency": {"type": "string"}},
    "required": ["value"],
    "additionalProperties": false},
  "Confidence": {
    "type": "object",
    "properties": {
      "value": {"type": "number"},
      "rating": {"enum": ["low","medium","high","numeric","unknown",
                 "ext-value"]},
      "ext-rating": {"type":"string"}},
    "required": ["value","rating"],
    "additionalProperties": false},
  "History": {
    "type": "object",
    "properties": {
      "restriction": {"$ref": "#/definitions/restriction",
                      "default": "private"},
      "ext-restriction": {"type": "string"},
      "HistoryItem": {
        "type": "array",
        "items": {"$ref": "#/definitions/HistoryItem"},
        "minItems": 1}},
    "required": ["HistoryItem"],
```

```
      "additionalProperties": false},
    "HistoryItem": {
      "type": "object",
      "properties": {
        "action": {"$ref": "#/definitions/action","default": "other"},
        "ext-action": {"type": "string"},
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "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": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "DefinedCOA": {
          "type": "array",
          "items": {"type": "string"},
          "minItems": 1},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["DateTime","action"],
      "additionalProperties": false},
    "EventData": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Description": {"type": "array",
          "items": { "$ref":"#/definitions/MLStringType"}},
        "DetectTime": {"$ref": "#/definitions/DATETIME"},
        "StartTime": {"$ref": "#/definitions/DATETIME"},
        "EndTime": {"$ref": "#/definitions/DATETIME"},
        "RecoveryTime": {"$ref": "#/definitions/DATETIME"},
        "ReportTime": {"$ref": "#/definitions/DATETIME"},
        "Contact": {
          "type": "array",
          "items": {"$ref": "#/definitions/Contact"},
          "minItems": 1},
        "Discovery": {
          "type": "array",
          "items": {"$ref": "#/definitions/Discovery"},
          "minItems": 1},
        "Assessment": {"$ref": "#/definitions/Assessment"},
        "Method": {
```

```
          "type": "array",
          "items": {"$ref": "#/definitions/Method"},
          "minItems": 1},
        "System": {
          "type": "array",
          "items": {"$ref": "#/definitions/System"},
          "minItems": 1},
        "Expectation": {
          "type": "array",
          "items": {"$ref": "#/definitions/Expectation"},
          "minItems": 1},
        "RecordData": {
          "type": "array",
          "items": {"$ref": "#/definitions/RecordData"},
          "minItems": 1},
        "EventData": {
          "type": "array",
          "items": {"$ref": "#/definitions/EventData"},
          "minItems": 1},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "Expectation": {
      "type": "object",
      "properties": {
        "action": {"$ref":"#/definitions/action","default": "other"},
        "ext-action": {"type": "string"},
        "severity": {"enum": ["low","medium","high"]},
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "default"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "DefinedCOA": {
          "type": "array",
          "items": {"type": "string"},
          "minItems": 1},
        "StartTime": {"$ref": "#/definitions/DATETIME"},
        "EndTime": {"$ref": "#/definitions/DATETIME"},
        "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"],"default":"unknown"},
      "virtual": {"enum": ["yes","no","unknown"],"default":"unknown"},
      "ownership": {
        "enum":["organization","personal","partner","customer",
                "no-relationship","unknown","ext-value"]},
      "ext-ownership": {"type": "string"},
      "restriction": {"$ref": "#/definitions/restriction",
                      "default": "private"},
      "ext-restriction": {"type": "string"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "Node": {"$ref": "#/definitions/Node"},
      "NodeRole": {
        "type": "array",
        "items": {"$ref": "#/definitions/NodeRole"},
        "minItems": 1},
      "Service": {
        "type": "array",
        "items": {"$ref": "#/definitions/Service"},
        "minItems": 1},
      "OperatingSystem": {
        "type": "array",
        "items": {"$ref": "#/definitions/SoftwareType"},
        "minItems": 1},
      "Counter": {
        "type": "array",
        "items": {"$ref": "#/definitions/Counter"},
        "minItems": 1},
      "AssetID": {
        "type": "array",
        "items": {"type": "string"},
        "minItems": 1},
      "Description": {
        "type": "array",
        "items": {"$ref": "#/definitions/MLStringType"},
        "minItems": 1},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
    "required": ["Node"],
    "additionalProperties": false},
  "Node": {
    "type": "object",
    "properties": {
      "DomainData": {
        "type": "array",
```

```
          "items": {"$ref": "#/definitions/DomainData"},
          "minItems": 1},
        "Address": {
          "type": "array",
          "items": {"$ref": "#/definitions/Address"},
          "minItems": 1},
        "PostalAddress": {"$ref": "#/definitions/PostalAddress"},
        "Location": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "Counter": {
          "type":"array",
          "items":{"$ref":"#/definitions/Counter"},
          "minItems": 1}},
      "anyOf": [
          {"required": ["DomainData"]},
          {"required": ["Address"]}
      ],
      "additionalProperties": false},
    "Address": {
      "type": "object",
      "properties": {
        "value": {"type": "string"},
        "category": {
          "enum":["asn","atm","e-mail","ipv4-addr","ipv4-net",
            "ipv4-net-masked","ipv4-net-mask","ipv6-addr","ipv6-net",
            "ipv6-net-masked","mac","site-uri","ext-value"],
            "default": "ipv6-addr"},
        "ext-category": {"type": "string"},
        "vlan-name": {"type": "string"},
        "vlan-num": {"type": "number"},
        "observable-id": {"$ref": "#/definitions/IDtype"}},
      "required": ["value","category"],
      "additionalProperties": false},
    "NodeRole": {
      "type": "object",
      "properties": {
        "category": {
          "enum":["client","client-enterprise","client-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",
            "hop-point","reflector","phishing-site",
            "spear-phishing-site","recruiting-site","fraudulent-site",
            "ext-value"]},
        "ext-category": {"type": "string"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1}},
      "required": ["category"],
      "additionalProperties": false},
    "Counter": {
      "type": "object",
      "properties": {
        "value": {"type": "number"},
        "type": {"enum": ["count","peak","average","ext-value"]},
        "ext-type": {"type": "string"},
        "unit":{"enum":["byte","mbit","packet","flow","session","alert",
          "message","event","host","site","organization","ext-value"]},
        "ext-unit": {"type": "string"},
        "meaning": {"type": "string"},
        "duration": {"$ref":"#/definitions/duration","default": "hour"},
        "ext-duration": {"type": "string"}},
      "required": ["value","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"},
          "minItems": 1},
```

```
      "NameServers": {
        "type": "array",
        "items": {"$ref": "#/definitions/NameServers"},
        "minItems": 1},
      "DomainContacts": {"$ref": "#/definitions/DomainContacts"}},
    "required": ["Name","system-status","domain-status"],
    "additionalProperties": false},
  "NameServers": {
    "type": "object",
    "properties": {
      "Server": {"type": "string"},
      "Address": {
        "type":"array",
        "items":{"$ref":"#/definitions/Address"},
        "minItems": 1}},
    "required": ["Server","Address"],
    "additionalProperties": false},
  "DomainContacts": {
    "type": "object",
    "properties": {
      "SameDomainContact": {"type": "string"},
      "Contact": {
        "type":"array",
        "items":{"$ref":"#/definitions/Contact"},
        "minItems": 1}},
    "oneOf": [
      {"required": ["SameDomainContact"]},
      {"required": ["Contact"]}],
    "additionalProperties": false},
  "Service": {
    "type": "object",
    "properties": {
      "ip-protocol": {"type": "number"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "ServiceName": {"$ref": "#/definitions/ServiceName"},
      "Port": {"type": "number"},
      "Portlist": {"$ref": "#/definitions/PortlistType"},
      "ProtoCode": {"type": "number"},
      "ProtoType": {"type": "number"},
      "ProtoField": {"type": "number"},
      "ApplicationHeaderField":{
        "$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": {"$ref": "#/definitions/URLtype"}},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1}},
      "required": [],
      "additionalProperties": false},
    "EmailData": {
      "type": "object",
      "properties": {
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "EmailTo": {
          "type": "array",
          "items": {"type": "string"},
          "minItems": 1},
        "EmailFrom": {"type": "string"},
        "EmailSubject": {"type": "string"},
        "EmailX-Mailer": {"type": "string"},
        "EmailHeaderField": {
          "type": "array",
          "items": {"$ref": "#/definitions/ExtensionType"},
          "minItems": 1},
        "EmailHeaders": {"type": "string"},
        "EmailBody": {"type": "string"},
        "EmailMessage": {"type": "string"},
        "HashData": {
          "type": "array",
          "items": {"$ref": "#/definitions/HashData"},
          "minItems": 1},
        "Signature": {
          "type": "array",
          "items": {"$ref": "#/definitions/BYTE"},
          "minItems": 1}},
      "required": [],
      "additionalProperties": false},
    "RecordData": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "DateTime": {"$ref": "#/definitions/DATETIME"},
        "Description": {
          "type": "array",
```

```
            "items": {"$ref": "#/definitions/MLStringType"},
            "minItems": 1},
          "Application": {"$ref": "#/definitions/SoftwareType"},
          "RecordPattern": {
            "type": "array",
            "items": {"$ref": "#/definitions/RecordPattern"},
            "minItems": 1},
          "RecordItem": {
            "type": "array",
            "items": {"$ref": "#/definitions/ExtensionType"},
            "minItems": 1},
          "URL": {
            "type": "array",
            "items": {"$ref": "#/definitions/URLtype"},
            "minItems": 1},
          "FileData": {
            "type": "array",
            "items": {"$ref": "#/definitions/FileData"},
            "minItems": 1},
          "WindowsRegistryKeysModified": {
            "type": "array",
            "items": {"$ref":"#/definitions/WindowsRegistryKeysModified"},
            "minItems": 1},
          "CertificateData": {
            "type":"array",
            "items":{"$ref":"#/definitions/CertificateData"},
            "minItems": 1},
          "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
        "required": [],
        "additionalProperties": false},
      "RecordPattern": {
        "type": "object",
        "properties": {
          "value": {"type": "string"},
          "type": {"enum": ["regex","binary","xpath","ext-value"],
                   "default": "regex"},
          "ext-type": {"type": "string"},
          "offset": {"type": "number"},
          "offsetunit": {"enum":["line","byte","ext-value"] ,
                         "default": "line"},
          "ext-offsetunit": {"type": "string"},
          "instance": {"type": "number"}},
        "required": ["value","type"],
        "additionalProperties": false},
      "WindowsRegistryKeysModified": {
        "type": "object",
        "properties": {
          "observable-id": {"$ref": "#/definitions/IDtype"},
```

```
      "Key": {
        "type": "array",
        "items": {"$ref": "#/definitions/Key"},
        "minItems": 1}},
    "required": ["Key"],
    "additionalProperties": false},
  "Key": {
    "type": "object",
    "properties": {
      "registryaction": {"enum": ["add-key","add-value","delete-key",
                          "delete-value","modify-key","modify-value",
                          "ext-value"]},
      "ext-registryaction": {"type": "string"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "KeyName": {"type":"string"},
      "KeyValue": {"type": "string"}},
    "required": ["KeyName"],
    "additionalProperties": false},
  "CertificateData": {
    "type": "object",
    "properties": {
      "restriction": {"$ref": "#/definitions/restriction",
                      "default": "private"},
      "ext-restriction": {"type": "string"},
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "Certificate": {
        "type": "array",
        "items": {"$ref": "#/definitions/Certificate"},
        "minItems": 1}},
    "required": ["Certificate"],
    "additionalProperties": false},
  "Certificate": {
    "type": "object",
    "properties": {
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "X509Data": {"$ref": "#/definitions/BYTE"},
      "Description": {
        "type": "array",
        "items": {"$ref": "#/definitions/MLStringType"},
        "minItems": 1}},
    "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": {"$ref": "#/definitions/File"},
        "minItems": 1}},
    "required": ["File"],
    "additionalProperties": false},
  "File": {
    "type": "object",
    "properties": {
      "observable-id": {"$ref": "#/definitions/IDtype"},
      "FileName": {"type": "string"},
      "FileSize": {"type": "number"},
      "FileType": {"type": "string"},
      "URL": {
        "type": "array",
        "items": {"$ref": "#/definitions/URLtype"},
        "minItems": 1},
      "HashData": {"$ref": "#/definitions/HashData"},
      "Signature": {
        "type": "array",
        "items": {"$ref": "#/definitions/BYTE"},
        "minItems": 1},
      "AssociatedSoftware": {"$ref": "#/definitions/SoftwareType"},
      "FileProperties": {
        "type":"array",
        "items":{"$ref":"#/definitions/ExtensionType"},
        "minItems": 1}},
    "required": [],
    "additionalProperties": false},
  "HashData": {
    "type": "object",
    "properties": {
      "scope": {"enum": ["file-contents","file-pe-section",
        "file-pe-iat","file-pe-resource","file-pdf-object",
        "email-hash","email-headers-hash","email-body-hash",
        "ext-value"]},
      "HashTargetID": {"type": "string"},
      "Hash": {
        "type": "array",
        "items": {"$ref": "#/definitions/Hash"},
        "minItems": 1},
      "FuzzyHash": {
        "type": "array",
        "items": {"$ref": "#/definitions/FuzzyHash"},
        "minItems": 1}},
    "required": ["scope"],
    "additionalProperties": false},
  "Hash": {
```

```
      "type": "object",
      "properties": {
        "DigestMethod": {"$ref": "#/definitions/BYTE"},
        "DigestValue": {"$ref": "#/definitions/BYTE"},
        "CanonicalizationMethod": {"$ref": "#/definitions/BYTE"},
        "Application": {"$ref": "#/definitions/SoftwareType"}},
      "required": ["DigestMethod","DigestValue"],
      "additionalProperties": false},
    "FuzzyHash": {
      "type": "object",
      "properties": {
        "FuzzyHashValue": {
          "type": "array",
          "items": {"$ref": "#/definitions/ExtensionType"},
          "minItems": 1},
        "Application": {"$ref": "#/definitions/SoftwareType"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["FuzzyHashValue"],
      "additionalProperties": false},
    "Indicator": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "IndicatorID": {"$ref": "#/definitions/IndicatorID"},
        "AlternativeIndicatorID": {
          "type": "array",
          "items": {"$ref": "#/definitions/AlternativeIndicatorID"},
          "minItems": 1},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "StartTime": {"$ref": "#/definitions/DATETIME"},
        "EndTime": {"$ref": "#/definitions/DATETIME"},
        "Confidence": {"$ref": "#/definitions/Confidence"},
        "Contact": {
          "type": "array",
          "items": {"$ref": "#/definitions/Contact"},
          "minItems": 1},
        "Observable": {"$ref": "#/definitions/Observable"},
        "uid-ref": {"$ref": "#/definitions/IDREFType"},
        "IndicatorExpression":{
         "$ref":"#/definitions/IndicatorExpression"},
        "IndicatorReference":{
         "$ref": "#/definitions/IndicatorReference"},
        "NodeRole": {
```

```
            "type": "array",
            "items": {"$ref": "#/definitions/NodeRole"},
            "minItems": 1},
        "AttackPhase": {
            "type": "array",
            "items": {"$ref": "#/definitions/AttackPhase"},
            "minItems": 1},
        "Reference": {
            "type": "array",
            "items": {"$ref": "#/definitions/Reference"},
            "minItems": 1},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "allOf": [
        {"required": ["IndicatorID"]},
        {"oneOf": [
          {"required":["Observable"]},
          {"required":["uid-ref"]},
          {"required":["IndicatorExpression"]},
          {"required":["IndicatorReference"]}]}],
      "additionalProperties": false},
    "IndicatorID": {
      "type": "object",
      "properties": {
        "id": {"type": "string"},
        "name": {"type": "string"},
        "version": {"type": "string"}},
      "required": ["id","name","version"],
      "additionalProperties": false},
    "AlternativeIndicatorID": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
          "default": "private"},
        "ext-restriction": {"type": "string"},
        "IndicatorID": {
          "type": "array",
          "items": {"$ref": "#/definitions/IndicatorID"},
          "minItems": 1}},
      "required": ["IndicatorID"],
      "additionalProperties": false},
    "Observable": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "System": {"$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": {"$ref": "#/definitions/RegistryHandle"},
      "RecordData": {"$ref": "#/definitions/RecordData"},
      "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"}},
      "oneOf": [
        {"required":["System"]},
        {"required":["Address"]},
        {"required":["DomainData"]},
        {"required":["EmailData"]},
        {"required":["Service"]},
        {"required":["WindowsRegistryKeysModified"]},
        {"required":["FileData"]},
        {"required":["CertificateData"]},
        {"required":["RegistryHandle"]},
        {"required":["RecordData"]},
        {"required":["EventData"]},
        {"required":["Incident"]},
        {"required":["Expectation"]},
        {"required":["Reference"]},
        {"required":["Assessment"]},
        {"required":["DetectionPattern"]},
        {"required":["HistoryItem"]},
        {"required":["BulkObservable"]},
        {"required":["AdditionalData"]}],
    "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-uri","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"},
      "BulkObservableFormat":{
        "$ref": "#/definitions/BulkObservableFormat"},
      "BulkObservableList": {"type": "string"},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
    "required": ["BulkObservableList"],
    "additionalProperties": false},
  "BulkObservableFormat": {
    "type": "object",
    "properties": {
      "Hash": {"$ref": "#/definitions/Hash"},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
    "oneOf": [
      {"required": ["Hash"]},
      {"required": ["AdditionalData"]}
    ],
    "additionalProperties": false},
  "IndicatorExpression": {
    "type": "object",
    "properties": {
      "operator": {"enum": ["not","and","or","xor"],"default": "and"},
      "ext-operator": {"type": "string"},
      "IndicatorExpression": {
        "type": "array",
        "items": {"$ref": "#/definitions/IndicatorExpression"},
        "minItems": 1},
      "Observable": {
        "type": "array",
        "items": {"$ref": "#/definitions/Observable"},
        "minItems": 1},
      "uid-ref": {
        "type": "array",
        "items": {"$ref": "#/definitions/IDREFType"},
        "minItems": 1},
      "IndicatorReference": {
        "type": "array",
        "items": {"$ref": "#/definitions/IndicatorReference"},
        "minItems": 1},
      "Confidence": {"$ref":"#/definitions/Confidence"},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
    "required": [],
    "additionalProperties": false},
  "IndicatorReference": {
    "type": "object",
    "properties": {
      "uid-ref": {"$ref":"#/definitions/IDREFType"},
```

```
            "euid-ref": {"type": "string"},
            "version": {"type": "string"}},
         "oneOf": [
            {"required": ["uid-ref"]},
            {"required": ["euid-ref"]}
         ],
         "additionalProperties": false},
      "AttackPhase": {
         "type": "object",
         "properties": {
            "AttackPhaseID": {
               "type": "array",
               "items": {"type": "string"},
               "minItems": 1},
            "URL": {
               "type": "array",
               "items": {"$ref": "#/definitions/URLtype"},
               "minItems": 1},
            "Description": {
               "type": "array",
               "items": {"$ref": "#/definitions/MLStringType"},
               "minItems": 1},
            "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": {"$ref": "#/definitions/Incident"},
         "minItems": 1},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
   "required": ["version","Incident"],
   "additionalProperties": false}
```

                        Figure 10: 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