MILE
Internet-Draft
Intended status: Standards Track
Expires: May 14, 2018

T. Takahashi
M. Suzuki
NICT

November 10, 2017

JSON binding of IODEF
draft-ietf-mile-jsoniodef-01

Abstract

RFC 7970 [RFC7970] provides XML-based data representation on incident information, but the use of the IODEF data model is not limited to XML. JSON representation is sometimes preferred since it is easy to handle from certain programming environments. This draft represents the IODEF data model in JSON.

Status of This Memo

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

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

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

This Internet-Draft will expire on May 14, 2018.

Copyright Notice

Table of Contents

1. Introduction

RFC 7970 [RFC7970] defines an data model for sharing incident information. It facilitates automated exchange of information among parties over networks. The data model can be implemented in a form of XML, but it is not always suitable for implementation. JSON-based representation is often useful.

Therefore, in this document, we provide a means to represent IODEF data model in JSON.

1.1. Requirements Language

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

2. IODEF Data Types

The IODEF Data Types, defined in RFC 7970 [RFC7970]are used for the JSON IODEF, with some syntax changes for some of the types.

2.1. Integers

An integer is represented in the information model by the INTEGER data type. Integer data MUST be encoded in Base 10, and is implemented as an "integer" type per JSON schema [jsonschema].

2.2. Real Numbers

A real (floating-point) number is represented in the information model by the REAL data type. Real data MUST be encoded in Base 10, and is implemented in the data model as an "number" type per JSON schema [jsonschema].

2.3. Characters and Strings

A single character is represented in the information model by the CHARACTER data type. A string is represented by the STRING data type. Special characters MUST be encoded using entity references.The CHARACTER and STRING data types are implemented in the data model as an "string" type per JSON schema [jsonschema].

2.4. Multilingual Strings

A string that needs to be represented in a human-readable language different than the default encoding of the document is represented in the information model by the ML_STRING data type. This data type is implemented as an object with "value", "lang", and "translation-id" elements as defined in Section 6. Examples are shown below.

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

2.5. Binary Strings

2.5.1. Base64 Bytes

A binary octet encoded with base64 is represented in the information model by the BYTE data type. A sequence of these octets is of the BYTE[] data type. The BYTE and BYTE[] data types are implemented in the data model as an "string" type per JSON schema [jsonschema].

2.5.2. Hexadecimal Bytes

A binary octet encoded as a character tuple consistent of two hexadecimal digits is represented in the information model by the HEXBIN data type. A sequence of these octets is of the HEXBIN[] data type. The HEXBIN and HEXBIN[] data types are implemented in the data model as an "string" type per JSON schema [jsonschema].

2.6. Enumerated Types

An enumerated type is represented in the information model by the ENUM data type. It is an ordered list of acceptable string values. Each value has a representative keyword. The ENUM data type is implemented in the data model as values of an enum array per JSON schema [jsonschema].

2.7. Date-Time String

A date-time string that describes a particular instant in time is represented in the information model by the DATETIME data type. Ranges are not supported. The DATETIME data type is implemented in the data model as an "string" type per JSON schema [jsonschema].

2.8. Timezone String

A timezone offset from UTC is represented in the information model by the TIMEZONE data type. It is formatted according to the following regular expression: "Z|[\+\-](0[0-9]|1[0-4]):[0-5][0-9]". The TIMEZONE data type is implemented in the data model as an "string" type per JSON schema [jsonschema].

2.9. Port Lists

A list of network ports is represented in the information model by the PORTLIST data type. A PORTLIST consists of a comma-separated list of numbers and ranges (N-M means ports N through M, inclusive). It is formatted according to the following regular expression: "\d+(\-\d+)?(,\d+(\-\d+)?)*". For example, "2,5-15,30,32,40-50,55-60". The PORTLIST data type is implemented in the data model as an "string" type per JSON schema [jsonschema]

2.10. Postal Address

A postal address is represented in the information model by the POSTAL data type. The format of the POSTAL data type is documented in Section 2.23 of [RFC4519] as a free-form multi-line string separated by the "$" character. The POSTAL data type is implemented in the data model as the aforementioned ML_STRING type.

2.11. Telephone Number

A telephone number is represented in the information model by the PHONE data type. The format of the PHONE data type is documented in [E.164]. The PHONE data type is implemented in the data model as an "string" type per JSON schema [jsonschema].

2.12. Email String

An email address is represented in the information model by the EMAIL data type. The format of the EMAIL data type is documented in Section 3.4.1 of [RFC5322] and Section 3.3 of [RFC6531]. The EMAIL data type is implemented in the data model as an "string" type per JSON schema [jsonschema].

2.13. Uniform Resource Locator Strings

A uniform resource locator (URL) is represented in the information model by the URL data type. The format of the URL data type is documented in [RFC3986].

The URL data type is implemented as an "string" type per JSON schema [jsonschema].

2.14. Identifiers and Identifier References

An identifier unique to the IODEF document is represented in the information model by the ID data type. A reference to this identifier is represented by the IDREF data type. These data types are implemented in the model as an "string" type per JSON schema [jsonschema].

2.15. Software

A particular version of software is represented in the information model by the SOFTWARE data type. This software can be described by using a reference, a URL, or with free-form text. The SOFTWARE data type is implemented as an object with "SoftwareReference", "URL", and "Description" elements as defined in Section 6. Examples are shown below.

```
"SoftwareType": {
  "SoftwareReference": {...},                  //SoftwareReference
  "Description": {"value":"MS Windows"},       //ML_STRING
}
```

2.16. StructuredInfo

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

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

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

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

3. The IODEF Information Model in JSON

The data model of IODEF is defined in RFC 7970 [RFC7970], and this section illustrates their representations in JSON. Note that the complete JSON schema is defined in Section 6.

3.1. IODEF-Document Class

This class is the top level class in the IODEF data model. Its class elements and an example are shown below. See Section 3.1 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

version, lang?, format-id?, private-enum-name?, private-enum-id?, Incident+, AdditionalData*

Example:

```
 "IODEF-Document": {
   "version": "2.1",                                    //STRING
   "lang": "en",                                          //ENUM
   "format-id": "RFC7970-json",                              //STRING
   "Incident": [ ... ]                                 //Incident
 }
```

3.2. Incident Class

The Incident class describes commonly exchanged information when reporting or sharing derived analysis from security incidents. Its class elements and an example are shown below. See Section 3.2 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

purpose, ext-purpose?, status?, ext-status?, lang?, restriction?, ext-restriction?, observable-id?, IncidentID, AlternativeID?, RelatedActivity*, DetectTime?, StartTime?, EndTime?, RecoveryTime?, ReportTime?, GenrationTime?, Description*, Discovery*, Assessment*, Method*, Contact+, EventData*, IndicatorData?, History?, AdditionalData*

Example:

```
   "Incident": {
     "purpose": "reporting",                                    //ENUM
     "lang": "en",                                             //STRING
     "restriction": "green",                                    //ENUM
     "IncidentID": { ... },                        //IncidentID Class
     "RelatedActivity": [ ... ],                //RelatedActivity Class
     "GenerationTime": "2015-10-02T11:18:00-05:00",         //DateTime
     "Description": [{"value":"Incident in the HQ"}],      //ML_STRING
     "Assessment": [ ... ],                                //Assessment
     "Method": [ ... ],                                        //Method
     "Contact": [ ... ]                                        //Contact
     "EventData": [ ... ],                                  //EventData
     "IndicatorData": { ... }                            //IndicatorData
     "History": { ... },                                       //History
     "AdditionalData": [ ... ],                        //AdditionalData
   }
```

3.3. Common Attributes

There are a number of recurring attributes used in the information model. They are documented in this section.

3.3.1. restriction Attribute

RFC 7970 [RFC7970] defines the restriction Attribute as one of common attributes. It is defined as below:

```
"restriction":{"enum": ["public", "partner", "need-to-know", "private",
              "default", "white", "green", "amber", "red", "ext-value"]}
```

Note that you must use "ext-restriction" field (STRING type) when the value of "restriction" field is set to "ext-value".

3.3.2. observable-id Attribute

RFC 7970 [RFC7970] defines the observable-id attribute as one of common attributes. The value of this attribute is a unique identifier, in string type, in the scope of the document.It is defined as below:

3.4. IncidentID Class

The class elements and an example are shown below. See Section 3.4 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

id, name, instance?, restriction?, ext-restriction?

Example:

```
"IncidentID": {
  "id": "nict20150518-0001",                          // STRING
  "name": "NICT_cert",                                // STRING
  "instance": "cyberlab"                              // STRING
  "restriction": "ext-value"                            // ENUM
  "ext-restriction": "registration required"          // STRING
}
```

3.5. AlternativeID Class

The class elements and an example are shown below. See Section 3.5 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

restriction?, ext-restriction?, IncidentID+

Example:

```
"AltervativeID": {
  "restriction": "private",                                 //ENUM
  "IncidentID": [<<<omitted>>>]                          //IncidentID
}
```

3.6. RelatedActivity Class

The class elements and an example are shown below. See Section 3.6 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

restriction?, ext-restriction?, IncidentID*, URL*, ThreatActor*, Campaign*, IndicatorID*, Confidence?, Description*, AdditionalData*

Example:

```
"RelatedActivity": {
  "restriction": "private",                                 //ENUM
  "ThreatActor": [{...}],                       //ThreatActor class
  "Campaign": [{...}]                              //Campaign class
}
```

3.7. ThreatActor Class

The class elements and an example are shown below. See Section 3.7 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

restriction?, ext-restriction?, ThreatActorID*, URL*, Description*, AdditionalData*

Example:

```
"ThreatActor": {
  "ThreatActorID": "TA-12-AGGRESSIVE-BUTTERFLY",          //STRING
  "Description": {"value":"Aggressive Butterfly"}      //ML_STRING
}
```

3.8. Campaign Class

The class elements and an example are shown below. See Section 3.8 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

restriction?, ext-restriction?, CampaignID*, URL*, Description*, AdditionalData*

Example:

```
"Campaign": {
  "CampaignID": "C-2015-59405",                           //STRING
  "Description": {"value":"Orange Giraffe"}            //ML_STRING
}
```

3.9. Contact Class

The class elements and an example are shown below. See Section 3.9 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

role, ext-role?, type, ext-type?, restriction?, ext-restriction?, ContactName*, ContactTitle*, Description*, RegistryHandle*, PostalAddress*, Email*, Telephone*, Timezone?, Contact*, AdditionalData*

Example:

```
"Contact": {
  "role": "creator",                                          //ENUM
  "type": "organization",                                     //ENUM
  "ContactName": {"value":"CSIRT for example.com"},    //ML_STRING
  "ContactTitle": {"value":"Senior Research Engineer"} //ML_STRING
  "email": {...},                                     //Email Class
  "Telephone": {...},                              //Telephone Class
  "Timezone": "+09:00"                                 //TIMEZONE
}
```

3.9.1. RegistryHandle Class

The class elements and an example are shown below. See Section 3.9.1 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

handle, registry, ext-registry?

Example:

```
"RegistryHandle": {
  "handle": "MyAPNIC",                                      //STRING
  "registry": "apnic",                                        //ENUM
}
```

3.9.2. PostalAddress Class

The class elements and an example are shown below. See Section 3.9.2 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

type?, ext-type?, PAddress, Description*

Example:

```
"PostalAddress": {
  "type": "mailing",                                          //ENUM
  "PAddress": "1-2-3 Kitamachi Koganei Tokyo, Japan",      //POSTAL
  "Description": {"value":"Office address"}             //ML_STRING
},
```

3.9.3. Email Class

The class elements and an example are shown below. See Section 3.9.3 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

type?, ext-type?, EmailTo, Description*

Example:

```
"Email": {
  "type": "direct",                                          //ENUM
  "emailTo": "contact@csirt.example.com",                   //EMAIL
  "Description": {"value":"Administrator's address"}   //ML_STRING
},
```

3.9.4. Telephone Class

The class elements and an example are shown below. See Section 3.9.4 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

type?, ext-type?, TelephoneNumber, Description*

Example:

```
"Telephone": {
  "type": "wired",                                           //ENUM
  "TelephoneNumber": "+818012345678",                       //PHONE
  "Description": {"value":"Admin's moble"}             //ML_STRING
},
```

3.10. Discovery Class

The class elements and an example are shown below. See Section 3.10 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

source?, ext-source?, restriction?, ext-restriction?, Description*, Contact*, DetectionPattern*

Example:

```
"Discovery": {
  "source": "nidps",                                          //ENUM
  "restriction": "need-to-know"                               //ENUM
  "Contact": {...},                                 //Contact class
  "DetectionPattern": {...},                //DetectionPattern class
  "Description":{"value":"IDS provided an alert"}      //ML_STRING
  }
}
```

3.10.1. DetectionPattern Class

The class elements and an example are shown below. See Section 3.10.1 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

restriction?, ext-restriction?, observable-id?, Application, Description*, DetectionConfiguration*

Example:

```
"DetectionPattern": {
  "Application": {...},                                  //SOFTWARE
  "Description": {"value":"The specified application
                  needs to be reviewed"},               //ML_STRING
  }
}
```

3.11. Method Class

The class elements and an example are shown below. See Section 3.11 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

restriction?, ext-restriction?, Reference*, Description*, AttackPattern*, Vulnerability*, Weakness*

Example:

```
"Method": {
  "AttackPattern": {...}                          //StructuredInfo
  "Vulnerability": {...}                          //StructuredInfo
}
```

3.11.1. Reference Class

The class elements and an example are shown below. See Section 3.11.1 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

observable-id?, ReferenceName?, URL*, Description*

Example:

```
"Reference":{
  "URL":"http://www.nict.go.jp"                              //URL
}
```

3.12. Assessment Class

The class elements and an example are shown below. See Section 3.12 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

occurence?, restriction?, ext-restriction?, observable-id?, IncidentCategory*, SystemImpact*, BusinessImpact*, TimeImpact*, MonetaryImpact*, IntendedImpact*, Counter*, MitigationFactor*, Cause*, Confidence?, AdditionalData*

Example:

```
"Assessment": {
  "SystemImpact": {...},                      //SystemImpact class
  "BusinessImpact": {...},                  //BusinessImpact class
  "TimeImpact": {...},                         //TimeImpact class
  "MonetaryImpact": {...},                  //MonetaryImpact class
  "IntendedImpact": {...},                  //IntendedImpact class
  "Counter": "5",                                  //Counter class
  "MitigationFactor": {"value":"Rebooting is required"}//ML_STRING
  "Cause": {"value":"Malware Infection"}              //ML_STRING
  }
}
```

3.12.1. SystemImpact Class

The class elements and an example are shown below. See Section 3.12.1 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

severity?, completion?, type, ext-type?, Description*

Example:

```
"SystemImpact":{
  "severity":"high",                                          //ENUM
  "completion": "successful"                                  //ENUM
  "type":"integrity-data"                                     //ENUM
  "Description":{"value":"The web page was falsified"} //ML_STRING
},
```

3.12.2. BusinessImpact Class

The class elements and an example are shown below. See Section 3.12.2 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

severity?, ext-severity?, type, ext-type?, Description*

Example:

```
"BusinessImpact": {
  "severity":"medium",                                        //ENUM
  "completion": "successful"                                  //ENUM
  "type": "degraded-reputation"                               //ENUM
  "Description":{"value":"The web page was falsified"} //ML_STRING
}
```

3.12.3. TimeImpact Class

The class elements and an example are shown below. See Section 3.12.3 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

value, severity?, metric, ext-metric?, duration?, ext-duration?

Example:

```
"TimeImpact":{
  "time": "240"                                          //REAL
  "metric": "elapsed"                                    //ENUM
  "duration": "minutes"                                  //ENUM
}
```

3.12.4. MonetaryImpact Class

The class elements and an example are shown below. See Section 3.12.4 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

value, severity?, currency?

Example:

```
"MonetaryImpact":{
  "money": "10000",                                      //REAL
  "severity": "medium",                                  //ENUM
  "currency": "USD",                                    //STRING
}
```

3.12.5. Confidence Class

The class elements and an example are shown below. See Section 3.12.5 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

value, rating, ext-rating?

Example:

```
"Confidence": {
  "value": "5"                                           //REAL
  "rating": "medium"                                     //ENUM
}
```

3.13. History Class

The class elements and an example are shown below. See Section 3.13 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

restriction?, ext-restriction?, HistoryItem+

Example:

```
"History": {
  "restriction": "need-to-know"                          //ENUM
  "HistoryItem": { ... }                      //HistoryItem class
},
```

3.13.1. HistoryItem Class

The class elements and an example are shown below. See Section 3.13.1 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

action, ext-action?, restriction?, ext-restriction?, observable-id?, DateTime, IncidentID?, Contact?, Description*, DefinedCOA*, AdditionalData*

Example:

```
"HistoryItem": {
  "action": "investigate"                                  //ENUM
  "restriction": "need-to-know"                            //ENUM
  "DateTime": "2015-10-15T11:18:00-05:00",               //DateTime
  "IncidentID" { ...},                        //IncidentID class
}
```

3.14. EventData Class

The class elements and an example are shown below. See Section 3.14 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

restriction?, ext-restriction?, observable-id?, Description*, DetectTime?, StartTime?, EndTime?, RecoveryTime?, ReportTime?, Contact*, Discovery*, Assessment?, Method*, Flow*, Expectation*, Record?, EventData*, AdditionalData*

Example:

```
"EventData": {
  "ReportTime": "2016-06-01 18:05:33",
  "Contact": { ...},                              //Contact class
  "Assessment": { ...},                         //Assessment class
  "Method": { ...},                                 //Method class
  "System": { ... },                                //System class
  "Expectation": { ...},                       //Expectation class
```

3.15. Expectation Class

The class elements and an example are shown below. See Section 3.15 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

action?, ext-action?, severity?, restriction?, ext-restriction?, Description*, DefinedCOA*, StartTime?, EndTime?, Contact?

Example:

```
"Expectation": {
  "action": "investigate"                                  //ENUM
  "severity": "medium"                                     //ENUM
  "restriction": "need-to-know"                            //ENUM
},
```

3.16. System Class

The class elements and an example are shown below. See Section 3.17 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

category?, ext-category?, interface?, spoofed?, virtual?, ownership?, ext-ownership?, restriction?, ext-restriction?, Node, NodeRole*, Service*, OperatingSystem*, Counter*, AssetID*, Description*, AdditionalData*

Example:

```
"System": {
  "category": "source",                                    //ENUM
  "Node": { ... },                                       //Node class
  "Service": { ... },                                  //Service class
},
```

3.17. Node Class

The class elements and an example are shown below. See Section 3.18 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

DomainData*, Address*, PostalAddress?, Location*, Counter*

Example:

```
"Node": {
  "Address": { ... },                                  //Address class
  "Location": {"value":"OrgID=7"}                          //ML_STRING
}
```

3.17.1. Address Class

The class elements and an example are shown below. See Section 3.18.1 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

value, category, ext-category?, vlan-name?, vlan-num?, observable-id?

Example:

```
"Address": {
  "value": """192.228.139.118",                              //STRING
  "category": "ipv4-addr",                                     //ENUM
},
```

3.17.2. NodeRole Class

The class elements and an example are shown below. See Section 3.18.2 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

category, ext-category?, Description*

Example:

```
"NodeRole": {
  "category": "client"                                    //ENUM
  "Description": {"value":"The computer at room A"}    //ML_STRING
},
```

3.17.3. Counter Class

The class elements and an example are shown below. See Section 3.18.3 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

value, type, ext-type?, unit, ext-unit?, meaning?, duration?, ext-duration?

Example:

```
"Counter": {
  "value": "3",                                           //REAL
  "type": "count",                                        //ENUM
  "unit": "packet"                                        //ENUM
  "meaning": {"value":"The number of scan packets
              are counted"},                           //ML_STRING
}
```

3.18. DomainData Class

The class elements and an example are shown below. See Section 3.19 of RFC 7970 [RFC7970] for the intended meanings of these elements.

Class elements:

system-status, ext-system-status?, domain-status, ext-domain-status?, observable-id?, Name, DateDomainWasChecked?, RegistrationDate?, ExpirationDate?, RelatedDNS*, Nameservers*, DomainContacts?

Example:

```
"DomainData": {
  "system-status": "innocent-hacked",                      //ENUM
  "domain-status": "assignedAndInactive",                //STRING
  "Name": "temp1.nict.go.jp"                             //STRING
},
```

3.18.1. Nameserver Class

This class is defined in Section 3.19.1 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

Server, Address*

Example:

```
"NameServers": {
  "Server": "vgw.nict.go.jp",                          //STRING
  "Address": {
    "AddressValue": "133.243.18.5",                    //STRING
    "category": "ipv4-addr"                              //ENUM
  }
}
```

3.18.2. DomainContacts Class

This class is defined in Section 3.19.2 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

SameDomainContact?, Contact+

Example:

```
"DomainContacts": {
  "Contact": {
    "role": "user",                                      //ENUM
    "type": "organization"                               //ENUM
  }
}
```

3.19. Service Class

This class is defined in Section 3.20 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

ip-protocol?, observable-id?, ServiceName?, Port?, Portlist?, ProtoCode?, ProtoType?, ProtoField?, ApplicationHeader?, EmailData?, Application?

Example:

```
"Service": {
  "ServiceName": {
    "Description": "It seems to be a scan from an infected machine."
  },
  "ip-protocol": 6,                                        //INTEGER
  "Port": 49183                                            //INTEGER
}
```

3.19.1. ServiceName Class

This class is defined in Section 3.20.1 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

IANAService?, URL*, Description*

Example:

```
"ServiceName": {
  "IANAService": "telnet"                                          //STRING
  "URL": "https://en.wikipedia.org/wiki/Telnet"                    //STRING
  "Description": "It seems to be a scan from an infected machine." //STRING
},
```

3.19.2. ApplicationHeader Class

This class is defined in Section 3.20.2 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

ApplicationHeaderField+

Example:

```
"ApplicationHeader": {
  "ApplicationHeaderField": {}
}
```

3.20. EmailData Class

This class is defined in Section 3.21 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

observable-id?, EmailTo*, EmailFrom?, EmailSubject?, EmailX-Mailer?, EmailHeaderField*, EmailHeaders?, EmailBody?, EmailMessage?, HashData*, SignatureData*

Example:

```
"EmailData":{
  "EmailTo": "user1@example.org"                                  //EMAIL
  "EmailFrom": "user2@example.com"                                //EMAIL
  "EmailSubject": "example email"                                //STRING
  "EmailX-Mailer": "example mailer v1.1.0"                       //STRING
  "EmailBody": "example email"                                   //STRING
}
```

3.21. Record Class

This class is defined in Section 3.22 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

restriction?, ext-restriction?, RecordData+

Example:

```
"Record": {
  "RecordData": {
    "RecordPattern": {
      "type": "regex",                                             //ENUM
      "value": "[0-9][A-Z]"
    }
  },
  "RecordItem": {}
},
```

3.21.1. RecordData Class

This class is defined in Section 3.22.1 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

restriction?, ext-restriction?, observable-id?, DateTime?, Description*, Application?, RecordPattern*, RecordItem*, URL*, FileData*, WindowsRegistryKeysModified*, CertificateData*, AdditionalData*

Example:

```
   "RecordData": {
     "RecordPattern": {
       "type": "regex",
       "value": "[0-9][A-Z]"
     }
   },
```

3.21.2. RecordPattern Class

This class is defined in Section 3.22.2 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

type, ext-type?, offset?, offsetunit?, ext-offsetunit?, instance?, value

Example:

```
   "RecordPattern": {
     "type": "regex",
     "value": "[0-9][A-Z]"
   },
```

3.22. WindowsRegistryKeysModified Class

This class is defined in Section 3.23 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

observable-id?, Key+

Example:

```
"WindowsRegistryKeysModified": {
  "Key": {
    "KeyValue": "xxxxxxxxxxxxxxxxxxxxxxx",                    //STRING
    "KeyName":"HKEY_LOCAL_MACHINExxxxxxx",                    //STRING
  }
}
```

3.22.1. Key Class

This class is defined in Section 3.23.1 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

registryaction?, ext-registryaction?, observable-id?, KeyName, KeyValue?

Example:

```
"Key": {
  "KeyValue": "xxxxxxxxxxxxxxxxxxxxxx",              //STRING
  "KeyName":"HKEY_LOCAL_MACHINExxxxxxx",             //STRING
}
```

3.23. CertificateData Class

This class is defined in Section 3.24 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

restriction?, ext-restriction?, observable-id?, Certificate+

Example:

```
"CertificateData": {
  "Certificate": {
    "X509Data": "xxxxxxxx"                          //STRING
  }
}
```

3.23.1. Certificate Class

This class is defined in Section 3.24.1 of RFC 7970 [RFC7970]. The X509Data class contains base64 encoded form of X.509 certificate or chain as described in Section 4.4.4 of [W3C.XMLSIG]. The example below represents how to describe this class in JSON.

Class elements:

observable-id?, X509Data, Description*

Example:

```
"Certificate": {
  "X509Data": "xxxxxxxx"                          //STRING
}
```

3.24. FileData Class

This class is defined in Section 3.25 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

restriction?, ext-restriction?, observable-id?, File+

Example:

```
"FileData": {
  "File": {
    "FileName": "dummy.exe"                          //STRING
  }
},
```

3.24.1. File Class

This class is defined in Section 3.25.1 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

observable-id?, FileName?, FileSize?, FileType?, URL*, HashData?, SignatureData?, AssociatedSoftware?, FileProperties*

Example:

```
"File": {
  "FileName": "dummy.exe"                          //STRING
}
```

3.25. HashData Class

This class is defined in Section 3.26 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

scope, HashTargetID?, Hash*, FuzzyHash*

Example:

```
  "HashData": {
    "scope": "file-contents",                       //ENUM
    "Hash": {
      "DigestMethod": "http://www.w3.org/2000/09/xmldsig#sha1", //STRING
      "DigestValue": "xxxxxxxxxxx"                //STRING
    }
  }
```

3.25.1. Hash Class

This class is defined in Section 3.26.1 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

DigestMethod, DigestValue, CanonicalizationMethod?, Application?

Example:

```
"Hash": {
  "DigestMethod": "http://www.w3.org/2000/09/xmldsig#sha1", //STRING
  "DigestValue": "xxxxxxxxxxx"                //STRING
}
```

3.25.2. FuzzyHash Class

This class is defined in Section 3.26.2 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

FuzzyHashValue+, Application?, AdditionalData?

Example:

```
"FuzzyHash": {
  "FuzzyHashValue": {}
}
```

3.26. SignatureData Class

This class is defined in Section 3.27 of RFC 7970 [RFC7970]. The Signature class contains base64 encoded form of signature as described in Section 4.2 of [W3C.XMLSIG]. The example below represents how to describe this class in JSON.

Class elements:

Signature+

Example:

```
"SignatureData": {
  "Signature": "xxxxxxxx"                        //STRING
}
```

3.27. Indicator Class

This class is defined in Section 3.29 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

restriction?, ext-restriction?, IndicatorID, AlternativeIndicatorID*, Description*, StartTime?, EndTime?, Confidence?, Contact*, Observable?, ObservableReference?, IndicatorExpression?, IndicatorReference?, NodeRole*, AttackPhase*, Reference*, AdditionalData*

Example:

```
"Indicator": {
  "IndicatorID": {
    "id": "G90823490",                                  //STRING
    "name": "csirt.example.com",                        //STRING
    "version": "1"                                      //STRING
  },
  "Description": "C2 domains",                         //ML_STRING
  "StartTime": "2014-12-02T11:18:00-05:00",             //Datetime
  "Observable": {
    "BulkObservable": {
      "type": "fqdn"                                      //ENUM
    },
    "BulkObservableList": [
      "kj290023j09r34.example.com",                     //STRING
      "09ijk23jfj0k8.example.net",                      //STRING
      "klknjwfjiowjefr923.example.org",                 //STRING
      "oimireik79msd.example.org"                       //STRIN
    ]
  }
}
```

3.27.1. IndicatorID Class

This class is defined in Section 3.29.1 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

id, name, version

Example:

```
"IndicatorID": {
  "id": "G90823490",                                  //STRING
  "name": "csirt.example.com",                        //STRING
  "version": "1"                                      //STRING
}
```

3.27.2. AlternativeIndicatorID Class

This class is defined in Section 3.29.2 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

restriction?, ext-restriction?, IndicatorReference+

Example:

```
"AlternativeIndicatorID": {
  "IndicatorReference": {
    "uid-ref": "xxxxx"
  }
},
```

3.27.3. Observable Class

This class is defined in Section 3.29.3 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

restriction?, ext-restriction?, System?, Address?, DomainData?, Service?, EmailData?, WindowsRegistryKeysModified?, FileData?, CertificateData?, RegistryHandle?, RecordData?, EventData?, Incident?, Expectation?, Reference?, Assessment?, DetectionPattern?, HistoryItem?, BulkObservable?, AdditionalData*

Example:

```
"Observable": {
  "BulkObservable": {
    "type": "fqdn"                                        //ENUM
  },
  "BulkObservableList": [
    "kj290023j09r34.example.com",                         //STRING
    "09ijk23jfj0k8.example.net",                          //STRING
    "klknjwfjiowjefr923.example.org",                     //STRING
    "oimireik79msd.example.org"                           //STRING
  ]
}
```

3.27.4. BulkObservable Class

This class is defined in Section 3.29.3.1 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

type?, ext-type?, BulkObservableFormat?, BulkObservableList, AdditionalData*

Example:

```
"BulkObservable": {
  "type": "fqdn"                                          //ENUM
},
"BulkObservableList": [
  "kj290023j09r34.example.com",                         //STRING
  "09ijk23jfj0k8.example.net",                          //STRING
  "klknjwfjiowjefr923.example.org",                     //STRING
  "oimireik79msd.example.org"                           //STRING
]
```

3.27.5. BulkObservableFormat Class

This class is defined in Section 3.29.3.1.1 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

Hash?, AdditionalData*

Example:

```
  "BulkObservableFormat": {
    "Hash": {
      "DigestMethod": "http://www.w3.org/2000/09/xmldsig#sha1", //STRING
      "DigestValue": "xxxxxxxxxxx"                  //STRING
    }
  }
```

3.27.6. IndicatorExpression Class

This class is defined in Section 3.29.4 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

operator?, ext-operator?, IndicatorExpression*, Observable*, ObservableReference*, IndicatorReference*, Confidence?, AdditionalData*

Example:

```
"IndicatorExpression": {
  "ObservableReference": {
    "uid-ref": "xxxxx"
  }
}
```

3.27.7. ObservableReference Class

This class is defined in Section 3.29.6 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

uid-ref

Example:

```
"ObservableReference": {
  "uid-ref": "xxxxx"
},
```

3.27.8. IndicatorReference Class

This class is defined in Section 3.29.7 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

uid-ref?, euid-ref?, version?

Example:

```
"IndicatorReference": {
  "uid-ref": "xxxxx"
}
```

3.27.9. AttackPhase Class

This class is defined in Section 3.29.8 of RFC 7970 [RFC7970]. The example below represents how to describe this class in JSON.

Class elements:

AttackPhaseID*, URL*, Description*, AdditionalData*

Example:

```
"AttackPhase": {
  "Description": "Currently, the infected host is scanning arbitrary hosts to fi
nd next targets." //ML_STRING
}
```

4. Notable differences from RFC 7970 (to be deleted)

- This document treats attributes and elements of each class defined in RFC 7970 [RFC7970] equally and is agnostic on the order of their appearances.
- Flow class is deleted, and EventData class now has the instance of System class.
- Record class is deleted, and the link to the Record class are directly connected to RecordData class, which is then renamed to Record class.

5. Examples

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

5.1. Minimal Example

A document containing only the mandatory elements and attributes.

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

5.2. Indicators from a Campaign

An example of C2 domains from a given campaign.

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

```
          "Campaign": [
            {
              "CampaignID": "C-2015-59405",
              "Description": "Orange Giraffe"
            }
          ]
        }
      ],
      "GenerationTime": "2015-10-02T11:18:00-05:00",
      "Description": [
        "Summarizes the Indicators of Compromise for the Orange Giraffe campaign
 of the Aggressive Butterfly crime gang."
      ],
      "Assessment": [
        {
          "BusinessImpact": {
            "type": "breach-proprietary"
          }
        }
      ],
      "Contacts": [
        {
          "type": "organization",
          "role": "creator",
          "ContactName": "CSIRT for example.com",
          "Email": {
            "emailTo": "contact@csirt.example.com"
          }
        }
      ],
      "IndicatorList": [
        {
          "IndicatorID": {
            "id": "G90823490",
            "name": "csirt.example.com",
            "version": "1"
          },
          "Description": "C2 domains",
          "StartTime": "2014-12-02T11:18:00-05:00",
          "Observable": {
            "BulkObservable": {
              "type": "fqdn"
            },
            "BulkObservableList": [
              "kj290023j09r34.example.com",
              "09ijk23jfj0k8.example.net",
              "klknjwfjiowjefr923.example.org",
              "oimireik79msd.example.org"
            ]
```

```
          }
        }
      ]
    }
  ]
}
```

6. The IODEF Data Model (JSON Schema)

```
{ "$schema": "http://json-schema.org/draft-04/schema#",
  "definitions": {
    "action": {"enum": ["nothing","contact-source-site","contact-target-site",
               "contact-sender", "investigate","block-host","block-network",
               "block-port","rate-limit-host","rate-limit-network",
               "rate-limit-port","redirect-traffic","honeypot",
               "upgrade-software","rebuild-asset","harden-asset",
               "remediate-other","status-triage","status-new-info",
               "watch-and-report","training","defined-coa","ext-value"]},
    "duration": {"enum": ["second","minute","hour","day","month","quarter",
                 "year","ext-value"]},
    "lang": {"enum": ["en","jp"]},
    "purpose": {"enum": ["traceback","mitigation","reporting","watch","other",
               "ext-value"]},
    "restriction": {"enum": ["public","partner","need-to-know","private",
                   "default","white","green","amber","red","ext-value"]},
    "status": {"enum": ["new","in-progress","forwarded","resolved","future",
              "ext-value"]},
    "DATETIME": {"type": "string"},
    "PORTLIST": {"type": "string"},
    "URLtype": {"type": "string"},
    "IDtype": {"type": "string"},
    "ExtensionType": {
      "type": "object",
      "properties": {
        "name": {"type": "string"},
        "dtype": {"enum": ["boolean","byte","bytes","character","date-time",
                  "ntpstamp","integer","portlist","real","string","file",
                  "path","frame","packet","ipv4-packet","ipv6-packet","url",
                  "csv","winreg","xml","ext-value"]},
        "ext-dtype": {"type": "string"},
        "meaning": {"type": "string"},
        "formatid": {"type": "string"},
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"}}},
    "ExtensionTypeList": {
      "type": "array",
      "items": {"$ref": "#/definitions/ExtensionType"}},
```

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

```
        "RecoveryTime": {"type": "string"},
        "ReportTime": {"type": "string"},
        "GenerationTime": {"type": "string"},
        "Description": {"type": "array","items": {"type": "string"}},
        "Discovery": {
          "type": "array","items": {"$ref": "#/definitions/Discovery"}},
        "Assessment": {
          "type": "array","items": {"$ref": "#/definitions/Assessment"}},
        "Methods": {
          "type": "array","items": {"$ref": "#/definitions/Method"}},
        "Contacts": {
          "type": "array","items": {"$ref": "#/definitions/Contact"}},
        "EventData": {
          "type": "array","items": {"$ref": "#/definitions/EventData"}},
        "IndicatorList": {
          "type": "array","items": {"$ref": "#/definitions/Indicator"}},
        "History": {"$ref": "#/definitions/History"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["IncidentID","GenerationTime","Contacts","purpose"],
      "additionalProperties": false},
    "IncidentID": {
      "title": "IncidentID",
      "description": "JSON schema for IncidentID class",
      "type": "object",
      "properties": {
        "id": {"type": "string"},
        "name": {"type": "string"},
        "instance": {"type": "string"},
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"}},
      "required": ["name"],
      "additionalProperties": false},
    "AlternativeID": {
      "title": "AlternativeID",
      "description": "JSON schema for AlternativeID class",
      "type": "object",
      "properties": {
        "IncidentID": {
          "type": "array","items":{"$ref": "#/definitions/IncidentID"}},
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"}},
      "required": ["IncidentID"],
      "additionalProperties": false},
    "RelatedActivity": {
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "IncidentID": {
```

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

```
        "PostalAddress": {
          "type": "array", "items": {"$ref": "#/definitions/PostalAddress"}},
        "Email": {"type": "array", "items": {"$ref": "#/definitions/Email"}},
        "Telephone": {
          "type": "array", "items": {"$ref": "#/definitions/Telephone"}},
        "Timezone": {"type": "string"},
        "Contact": {
          "type": "array", "items": {"$ref": "#/definitions/Contact"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["role","type"],
      "additionalProperties": false},
    "RegistryHandle": {
      "type": "object",
      "properties": {
        "handle": {"type": "string"},
        "registry": {
          "enum": ["internic","apnic","arin","lacnic","ripe","afrinic","local",
                   "ext-value"]},
        "ext-registry": {"type": "string"}},
      "required": ["registry"],
      "additionalProperties": false},
    "PostalAddress": {
      "type": "object",
      "properties": {
        "type": {"type": "string"},
        "ext-type": {"type": "string"},
        "PAddress": {"type": "string"},
        "Description": {"type": "array", "items": {"type": "string"}}},
      "required": ["PAddress"],
      "additionalProperties": false},
    "Email": {
      "type": "object",
      "properties": {
        "type": {
          "enum":["direct","hotline","ext-value"]},
        "ext-type": {"type": "string"},
        "EmailTo": {"type": "string"},
        "Description": {"type": "array", "items": {"type": "string"}}},
      "required": ["EmailTo"],
      "additionalProperties": false},
    "Telephone": {
      "type": "object",
      "properties": {
        "type": {
          "enum":["wired","mobile","fax","hotline","ext-value"]},
        "ext-type": {"type": "string"},
        "TelephoneNumber": {"type": "string"},
        "Description": {"type": "array", "items": {"type": "string"}}},
```

```
      "required": ["TelephoneNumber"],
      "additionalProperties": false},
    "Discovery": {
      "type": "object",
      "properties": {
        "source": {
          "enum":["nidps","hips","siem","av","third-party-monitoring",
                  "incident","os-log","application-log","device-log",
                  "network-flow","passive-dns","investigation","audit",
                  "internal-notification","external-notification","leo",
                  "partner","actor","unknown","ext-value"]},
        "ext-source": {"type": "string"},
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "Description": {"type": "array", "items": {"type": "string"}},
        "Contact": {
          "type": "array", "items": {"$ref": "#/definitions/Contact"}},
        "DetectionPattern": {
          "type": "array", "items":{"$ref":"#/definitions/DetectionPattern"}}},
      "required": [],
      "additionalProperties": false},
    "DetectionPattern": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Application": {"$ref": "#/definitions/SoftwareType"},
        "Description": {"type": "array", "items": {"type": "string"}},
        "DetectionConfiguration": {
          "type": "array", "items": {"type": "string"}}},
      "required": ["Application"],
      "additionalProperties": false},
    "Method": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "References": {
          "type": "array","items": {"$ref": "#/definitions/Reference"}},
        "Description": {"type": "array", "items": {"type": "string"}},
        "AttackPattern": {
          "type": "array", "items": {"$ref": "#/definitions/StructuredInfo"}},
        "Vulnerability": {
          "type": "array", "items": {"$ref": "#/definitions/StructuredInfo"}},
        "Weakness": {
          "type": "array", "items": {"$ref": "#/definitions/StructuredInfo"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
```

```
      "required": [],
      "additionalProperties": false},
    "Reference": {
      "type": "object",
      "properties": {
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "ReferenceName": {"type": "string"},
        "URL": {"type": "array", "items": {"$ref": "#/definitions/URLtype"}},
        "Description": {"type": "array", "items": {"type": "string"}}},
      "required": [],
      "additionalProperties": false},
    "Assessment": {
      "type": "object",
      "properties": {
        "occurrence": {"enum":["actual","potential"]},
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "IncidentCategory": {"type": "array", "items": {"type": "string"}},
        "SystemImpact": {
          "type": "array", "items": {"$ref": "#/definitions/SystemImpact"}},
        "BusinessImpact": {
          "type": "array", "items": {"$ref": "#/definitions/BusinessImpact"}},
        "TimeImpact": {
          "type": "array", "items": {"$ref": "#/definitions/TimeImpact"}},
        "MonetaryImpact": {
          "type": "array", "items": {"$ref": "#/definitions/MonetaryImpact"}},
        "IntendedImpact": {
          "type": "array", "items": {"$ref": "#/definitions/BusinessImpact"}},
        "Counter": {
          "type": "array", "items": {"$ref": "#/definitions/Counter"}},
        "MitigatingFactor": {
          "type": "array", "items": {"$type": "string"}},
        "Cause": {"type": "array", "items": {"$type": "string"}},
        "Confidence": {"$ref": "#/definitions/Confidence"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "SystemImpact": {
      "type": "object",
      "properties": {
        "severity": {
          "enum":["low","medium","high"]},
        "completion": {"enum":["failed","succeeded"]},
        "type": {
          "enum":["takeover-account","takeover-service","takeover-system",
                  "cps-manipulation","cps-damage","availability-data",
                  "availability-account","availability-service",
```

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

```
        "value": {"type": "number"},
        "rating": {
          "enum": ["low","medium","high","numeric","unknown","ext-value"]},
        "ext-rating": {"type":"string"}},
      "required": ["rating"],
      "additionalProperties": false},
    "History": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "HistoryItem": {
          "type": "array","items": {"$ref": "#/definitions/HistoryItem"}}},
      "required": ["HistoryItem"],
      "additionalProperties": false},
    "HistoryItem": {
      "type": "object",
      "properties": {
        "action": {"$ref": "#/definitions/action"},
        "ext-action": {"type": "string"},
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "DateTime": {"$ref": "#/definitions/DATETIME"},
        "IncidentID": {"$ref": "#/definitions/IncidentID"},
        "Contact": {"$ref": "#/definitions/Contact"},
        "Description": {"type": "array","items": {"type": "string"}},
        "DefinedCOA": {"type": "array","items": {"type": "string"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["DateTime","action"],
      "additionalProperties": false},
    "EventData": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Description": {"type": "array","items": {"type": "string"}},
        "DetectTime": {"type": "string"},
        "StartTime": {"type": "string"},
        "EndTime": {"type": "string"},
        "RecoveryTime": {"type": "string"},
        "ReportTime": {"type": "string"},
        "Contact": {
          "type": "array","items": {"$ref": "#/definitions/Contact"}},
        "Discovery": {
          "type": "array","items": {"$ref": "#/definitions/Discovery"}},
        "Assessment": {"$ref": "#/definitions/Assessment"},
```

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

```
        "Service": {
          "type": "array","items": {"$ref": "#/definitions/Service"}},
        "OperatingSystem": {
          "type": "array","items": {"$ref": "#/definitions/SoftwareType"}},
        "Counter": {
          "type": "array","items": {"$ref": "#/definitions/Counter"}},
        "AssetID": {"type": "array","items": {"type": "string"}},
        "Description": {"type": "array","items": {"type": "string"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["Node"],
      "additionalProperties": false},
    "Node": {
      "type": "object",
      "properties": {
        "DomainData": {
          "type": "array","items": {"$ref": "#/definitions/DomainData"}},
        "Address": {
          "type": "array","items": {"$ref": "#/definitions/Address"}},
        "PostalAddress": {"type": "string"},
        "Location": {"type": "array","items": {"type": "string"}},
        "Counter": {"type": "array","items":{"$ref":"#/definitions/Counter"}}},
      "required": [],
      "additionalProperties": false},
    "Address": {
      "type": "object",
      "properties": {
        "value": {"type": "string"},
        "category": {
           "enum": ["asn","atm","e-mail","ipv4-addr","ipv4-net",
                    "ipv4-net-masked","ipv4-net-mask","ipv6-addr","ipv6-net",
                    "ipv6-net-masked","mac","site-url","ext-value"]},
        "ext-category": {"type": "string"},
        "vlan-name": {"type": "string"},
        "vlan-num": {"type": "integer"},
        "observable-id": {"$ref": "#/definitions/IDtype"}},
      "required": ["category"],
      "additionalProperties": false},
    "NodeRole": {
      "type": "object",
      "properties": {
        "category": {
          "enum":["client","client-enterprise","clent-partner","client-remote",
                  "client-kiosk","client-mobile","server-internal",
                  "server-public","www","mail","webmail","messaging",
                  "streaming","voice","file","ftp","p2p","name","directory",
                  "credential","print","application","database","backup",
                  "dhcp","assessment","source-control","config-management",
                  "monitoring","infra","infra-firewall","infra-router",
```

```
                  "infra-switch","camera","proxy","remote-access","log",
                  "virtualization","pos", "scada", "scada-supervisory",
                  "sinkhole","honeypot","anomyzation","c2-server",
                  "malware-distribution","drop-server","hot-point","reflector",
                  "phishing-site","spear-phishing-site","recruiting-site",
                  "fraudulent-site","ext-value"]},
        "ext-category": {"type": "string"},
        "Description": {"type": "array","items": {"type": "string"}}},
      "required": ["category"],
      "additionalProperties": false},
    "Counter": {
      "type": "object",
      "properties": {
        "value": {"type": "string"},
        "type": {"enum": ["count","peak","average","ext-value"]},
        "ext-type": {"type": "string"},
        "unit": {"enum": ["byte","mbit","packet","flow","session","alert",
                 "message","event","host","site","organization","ext-value"]},
        "ext-unit": {"type": "string"},
        "meaning": {"type": "string"},
        "duration": {"$ref":"#/definitions/duration"},
        "ext-duration": {"type": "string"}},
      "required": ["type","unit"],
      "additionalProperties": false},
    "DomainData": {
      "type": "object",
      "properties": {
        "system-status": {
          "enum": ["spoofed","fraudulent","innocent-hacked",
                   "innocent-hijacked","unknown","ext-value"]},
        "ext-system-status": {"type": "string"},
        "domain-status": {
          "enum": [
            "reservedDelegation","assignedAndActive","assignedAndInactive",
            "assignedAndOnHold","revoked","transferPending","registryLock",
            "registrarLock","other","unknown","ext-value"]},
        "ext-domain-status": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Name": {"type": "string"},
        "DateDomainWasChecked": {"$ref": "#/definitions/DATETIME"},
        "RegistrationDate": {"$ref": "#/definitions/DATETIME"},
        "ExpirationDate": {"$ref": "#/definitions/DATETIME"},
        "RelatedDNS": {
          "type": "array","items": {"$ref": "#/definitions/ExtensionType"}},
        "NameServers": {
          "type": "array","items": {"$ref": "#/definitions/NameServers"}},
        "DomainContacts": {
          "type": "array","items": {"$ref": "#/definitions/DomainContacts"}}},
```

```
      "required": ["Name","system-status","domain-status"],
      "additionalProperties": false},
    "NameServers": {
      "type": "object",
      "properties": {
        "Server": {"type": "string"},
        "Address": {"type": "array","items":{"$ref":"#/definitions/Address"}}},
      "required": ["Server","Address"],
      "additionalProperties": false},
    "DomainContacts": {
      "type": "object",
      "properties": {
        "SameDomainContact": {"type": "string"},
        "Contact": {"type": "array","items":{"$ref":"#/definitions/Contact"}}},
      "required": ["Contact"],
      "additionalProperties": false},
    "Service": {
      "type": "object",
      "properties": {
        "ip-protocol": {"type": "integer"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "ServiceName": {"$ref": "#/definitions/ServiceName"},
        "Port": {"type": "integer"},
        "Portlist": {"$ref": "#/definitions/PORTLIST"},
        "ProtoCode": {"type": "integer"},
        "ProtoType": {"type": "integer"},
        "ProtoField": {"type": "integer"},
        "ApplicationHeader": {"$ref": "#/definitions/ApplicationHeader"},
        "EmailData": {"$ref": "#/definitions/EmailData"},
        "Application": {"$ref": "#/definitions/SoftwareType"}},
      "required": [],
      "additionalProperties": false},
    "ServiceName": {
      "type": "object",
      "properties": {
        "IANAService": {"type": "string"},
        "URL": {"type": "array","items": {"$ref": "#/definitions/URLtype"}},
        "Description": {"type": "array","items": {"type": "string"}}},
      "required": [],
      "additionalProperties": false},
    "ApplicationHeader": {
      "type": "object",
      "properties": {
        "ApplicationHeaderField": {
          "type": "array","items": {"$ref": "#/definitions/ExtensionType"}}},
      "required": ["ApplicationHeaderField"],
      "additionalProperties": false},
    "EmailData": {
```

```
      "type": "object",
      "properties": {
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "EmailTo": {"type": "array","items": {"type": "string"}},
        "EmailFrom": {"type": "string"},
        "EmailSubject": {"type": "string"},
        "EmailX-Mailer": {"type": "string"},
        "EmailHeaderField": {
          "type": "array","items": {"$ref": "#/definitions/ExtensionType"}},
        "EmailHeaders": {"type": "string"},
        "EmailBody": {"type": "string"},
        "EmailMessage": {"type": "string"},
        "HashData": {
          "type": "array","items": {"$ref": "#/definitions/HashData"}},
        "SignatureData": {
          "type": "array","items": {"$ref": "#/definitions/SignatureData"}}},
      "required": [],
      "additionalProperties": false},
    "Record":{
      "type": "object",
      "properties":{
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "RecordData": {
          "type": "array","items": {"$ref": "#/definitions/RecordData"}}},
      "required":["RecordData"],
      "additionalProperties": false},
    "RecordData": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "DateTime": {"$ref": "#/definitions/DATETIME"},
        "Description": {"type": "array","items": {"type": "string"}},
        "Applicadtion": {"$ref": "#/definitions/SoftwareType"},
        "RecordPattern": {
          "type": "array","items": {"$ref": "#/definitions/RecordPattern"}},
        "RecordItem": {
          "type": "array","items": {"$ref": "#/definitions/ExtensionType"}},
        "URL": {
          "type": "array","items": {"$ref": "#/definitions/URLtype"}},
        "FileData": {
          "type": "array","items": {"$ref": "#/definitions/FileData"}},
        "WindowsRegistryKeysModified": {
          "type": "array",
          "items": {"$ref": "#/definitions/WindowsRegistryKeysModified"}},
        "CertificateData": {
```

```
          "type": "array","items": {"$ref": "#/definitions/CertificateData"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false
    },
    "RecordPattern": {
      "type": "object",
      "properties": {
        "value": {"type": "string"},
        "type": {"enum": ["regex","binary","xpath","ext-value"]},
        "ext-type": {"type": "string"},
        "offset": {"type": "integer"},
        "offsetunit": {"enum":["line","byte","ext-value"]},
        "ext-offsetunit": {"type": "string"},
        "instance": {"type": "integer"}},
      "required": ["type"],
      "additionalProperties": false},
    "WindowsRegistryKeysModified": {
      "type": "object",
      "properties": {
        "observabile-id": {"$ref": "#/definitions/IDtype"},
        "Key": {"type": "array","items": {"$ref": "#/definitions/Key"}}},
      "required": ["Key"],
      "additionalProperties": false},
    "Key": {
      "type": "object",
      "properties": {
        "registryaction": {"enum": ["add-key","add-value","delete-key",
                           "delete-value","modify-key","modify-value",
                           "ext-value"]},
        "ext-registryaction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "KeyName": {"type":"string"},
        "KeyValue": {"type": "string"}},
      "required": ["KeyName"],
      "additionalProperties": false},
    "CertificateData": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Certificate": {
          "type": "array","items": {"$ref": "#/definitions/Certificate"}}},
      "required": ["Certificate"],
      "additionalProperties": false},
    "Certificate": {
      "type": "object",
```

```
      "properties": {
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "X509Data": {type: "string"},
        "Description": {"type": "array","items": {"type": "string"}}},
      "required": ["X509Data"],
      "additionalProperties": false},
    "FileData": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "File": {"type": "array","items": {"$ref": "#/definitions/File"}}},
      "required": ["File"],
      "additionalProperties": false},
    "File": {
      "type": "object",
      "properties": {
        "FileName": {"type": "string"},
        "FileSize": {"type": "integer"},
        "FileType": {"type": "string"},
        "URL": {"type": "array","items": {"$ref": "#/definitions/URLtype"}},
        "HashData": {"$ref": "#/definitions/HashData"},
        "SignatureData": {"$ref": "#/definitions/SignatureData"},
        "AssociatedSoftware": {"$ref": "#/definitions/SoftwareType"},
        "FileProperties": {
          "type": "array","items": {"$ref": "#/definitions/ExtensionType"}}},
      "required": [],
      "additionalProperties": false},
    "HashData": {
      "type": "object",
      "properties": {
        "scope": {"enum": ["file-contents","file-pe-section","file-pe-iat",
                  "file-pe-resource","file-pdf-object","email-hash",
                  "email-hash-header","email-hash-body"]},
        "HashTargetID": {"type": "string"},
        "Hash": {"type": "array","items": {"$ref": "#/definitions/Hash"}},
        "FuzzyHash": {
          "type": "array","items": {"$ref": "#/definitions/FuzzyHash"}}},
      "required": ["scope"],
      "additionalProperties": false},
    "Hash": {
      "type": "object",
      "properties": {
        "DigestMethod": {"type": "string"},
        "DigestValue": {"type": "string"},
        "CanonicalizationMethod": {},
        "Application": {"$ref": "#/definitions/SoftwareType"}},
```

```
      "required": ["DigestMethod","DigestValue"],
      "additionalProperties": false},
    "FuzzyHash": {
      "type": "object",
      "properties": {
        "FuzzyHashValue": {
          "type": "array","items": {"$ref": "#/definitions/ExtensionType"}},
        "Application": {"$ref": "#/definitions/SoftwareType"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["FuzzyHashValue"],
      "additionalProperties": false},
    "SignatureData": {
      "type": "object",
      "properties": {
        "Signature": {"type": "array","items": {"type": "string"}}},
      "required": ["Signature"],
      "additionalProperties": false},
    "Indicator": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "IndicatorID": {"$ref": "#/definitions/IndicatorID"},
        "AlternativeIndicatorID": {
          "type": "array",
          "items": {"$ref": "#/definitions/AlternativeIndicatorID"}},
        "Description": {"type": "array","items": {"type": "string"}},
        "StartTime": {"$ref": "#/definitions/DATETIME"},
        "EndTime": {"$ref": "#/definitions/DATETIME"},
        "Confidence": {"$ref": "#/definitions/Confidence"},
        "Contact": {
          "type": "array","items": {"$ref": "#/definitions/Contact"}},
        "Observable": {"$ref": "#/definitions/Observable"},
        "ObservableReference": {"$ref": "#/definitions/ObservableReference"},
        "IndicatorExpression": {"$ref": "#/definitions/IndicatorExpression"},
        "IndicatorReference": {"$ref": "#/definitions/IndicatorReference"},
        "NodeRole": {
          "type": "array","items": {"$ref": "#/definitions/NodeRole"}},
        "AttackPhase": {
          "type": "array","items": {"$ref": "#/definitions/AttackPhase"}},
        "Reference": {
          "type": "array","items": {"$ref": "#/definitions/Reference"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["IndicatorID"],
      "additionalProperties": false},
    "IndicatorID": {
      "type": "object",
      "properties": {
```

```
        "id": {"type": "string"},
        "name": {"type": "string"},
        "version": {"type": "string"}},
      "required": ["name","version"],
      "additionalProperties": false},
    "AlternativeIndicatorID": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "IndicatorReference": {
          "type": "array",
          "items": {"$ref": "#/definitions/IndicatorReference"}}},
      "required": ["IndicatorReference"],
      "additionalProperties": false},
    "Observable": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "System": {"$ref": "#/definitions/System"},
        "Address": {"$ref": "#/definitions/Address"},
        "DomainData": {"$ref": "#/definitions/DomainData"},
        "EmailData": {"$ref": "#/definitions/EmailData"},
        "Service": {"$ref": "#/definitions/Service"},
        "WindowsRegistryKeysModified": {
          "$ref": "#/definitions/WindowsRegistryKeysModified"},
        "FileData": {"$ref": "#/definitions/FileData"},
        "CertificateData": {"$ref": "#/definitions/CertificateData"},
        "RegistryHandle": {"$ref": "#/definitions/RegistryHandle"},
        "Record": {"$ref": "#/definitions/Record"},
        "EventData": {"$ref": "#/definitions/EventData"},
        "Incident": {"$ref": "#/definitions/Incident"},
        "Expectation": {"$ref": "#/definitions/Expectation"},
        "Reference": {"$ref": "#/definitions/Reference"},
        "Assessment": {"$ref": "#/definitions/Assessment"},
        "DetectionPattern": {"$ref": "#/definitions/DetectionPattern"},
        "HistoryItem": {"$ref": "#/definitions/HistoryItem"},
        "BulkObservable": {"type": "string"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "BulkObservable": {
      "type": "object",
      "properties": {
        "type": {"enum": ["asn","atm","e-mail","ipv4-addr","ipv4-net",
                  "ipv4-net-mask","ipv6-addr","ipv6-net","ipv6-net-mask","mac",
                  "site-url","domain-name","domain-to-ipv4","domain-to-ipv6",
```

```
                "domain-to-ipv4-timestamp","domain-to-ipv6-timestamp",
                "ipv4-port","ipv6-port","windows-reg-key","file-hash",
                "email-x-mailer","email-subject","http-user-agent",
                "http-request-url","mutex","file-path","user-name",
                "ext-value"]},
        "ext-type": {"type": "string"},
        "BulkObservableFormant":{"$ref": "#/definitions/BulkObservableFormat"},
        "BulkObservableList": {"type": "string"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "BulkObservableFormat": {
      "type": "object",
      "properties": {
        "Hash": {"$ref": "#/definitions/Hash"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "IndicatorExpression": {
      "type": "object",
      "properties": {
        "operator": {"enum": ["not","and","or","xor"]},
        "ext-operator": {"type": "string"},
        "IndicatorExpression": {
          "type": "array",
          "items": {"$ref": "#/definitions/IndicatorExpression"}},
        "Observable": {
          "type": "array","items": {"$ref": "#/definitions/Observable"}},
        "ObservableReference": {
          "type": "array",
          "items": {"$ref": "#/definitions/ObservableReference"}},
        "IndicatorReference": {
          "type": "array",
         "items": {"$ref": "#/definitions/IndicatorReference"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "ObservableReference": {
      "type": "object",
      "properties": {"uid-ref": {"type": "string"}},
      "required": ["uid-ref"],
      "additionalProperties": false},
    "IndicatorReference": {
      "type": "object",
      "properties": {
        "uid-ref": {"type": "string"},
        "euid-ref": {"type": "string"},
        "version": {"type": "string"}},
```

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

Figure 1: JSON schema

7. Acknowledgements

TBD.

8. IANA Considerations

This memo includes no request to IANA.

9. Security Considerations

This memo does not provide any further security considerations than the one described in RFC 7970 [RFC7970].

10. References

10.1. Normative References

[jsonschema]
"JSON Schema", 2006.

http://json-schema.org/

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

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

10.2. Informative References

[DOMINATION] Mad Dominators, Inc., "Ultimate Plan for Taking Over the World", 1984, <http://www.example.com/dominator.html>.

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, DOI 10.17487/RFC2629, June 1999, <https://www.rfc-editor.org/info/rfc2629>.

[RFC3552] Rescorla, E. and B. Korver, "Guidelines for Writing RFC Text on Security Considerations", BCP 72, RFC 3552, DOI 10.17487/RFC3552, July 2003, <https://www.rfc-editor.org/info/rfc3552>.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", RFC 5226, DOI 10.17487/RFC5226, May 2008, <https://www.rfc-editor.org/info/rfc5226>.

Authors' Addresses

Takeshi Takahashi
NICT
4-2-1 Nukui-Kitamachi
Koganei, Tokyo 184-8795
Japan

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

Mio Suzuki
NICT
4-2-1 Nukui-Kitamachi
Koganei, Tokyo 184-8795
Japan

Email: mio@nict.go.jp