

MILE
Internet-Draft
Intended status: Standards Track
Expires: January 9, 2020

T. Takahashi
NICT
R. Danyliw
CERT
M. Suzuki
NICT
July 8, 2019

CBOR/JSON binding of IODEF
draft-ietf-mile-jsoniodef-09

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 January 9, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

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	2
1.1. Requirements Language	3
2. IODEF Data Types	3
2.1. Abstract Data Type to JSON Data Type Mapping	3
2.2. Complex JSON Types	5
2.2.1. Integer	5
2.2.2. Multilingual Strings	5
2.2.3. Enum	6
2.2.4. Software and Software Reference	6
2.2.5. Structured Information	6
2.2.6. EXTENSION	7
3. IODEF JSON Data Model	7
3.1. Classes and Elements	7
3.2. Mapping between CBOR/JSON and XML IODEF	17
4. Examples	18
4.1. Minimal Example	18
4.2. Indicators from a Campaign	20
5. The IODEF Data Model (CDDL)	25
6. IANA Considerations	40
7. Security Considerations	40
8. Acknowledgments	40
9. References	41
9.1. Normative References	41
9.2. Informative References	41
Appendix A. Data Types used in this document	42
Appendix B. The IODEF Data Model (JSON Schema)	42
Authors' Addresses	70

1. Introduction

The Incident Object Description Exchange Format (IODEF) [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.

IODEF documents are structured and thus suitable for machine processing. They will streamline incident response operations. Another well-used and structured format that is suitable for machine processing is JSON. To facilitate the automation of incident response operations, IODEF documents should support JSON representation.

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, see Section 2.2.1
REAL	Section 2.2	"number" per [RFC8259]
CHARACTER	Section 2.3	"string" per [RFC8259]
STRING	Section 2.3	"string" per [RFC8259]
ML_STRING	Section 2.4	see Section 2.2.2
BYTE	Section 2.5.1	"string" per [RFC8259]
BYTE[]	Section 2.5.1	"string" per [RFC8259]
HEXBIN	Section 2.5.2	"string" per [RFC8259]
HEXBIN[]	Section 2.5.2	"string" per [RFC8259]
ENUM	Section 2.6	see Section 2.2.3
DATETIME	Section 2.7	"string" per [RFC8259]
TIMEZONE	Section 2.8	"string" per [RFC8259]
PORTLIST	Section 2.9	"string" per [RFC8259]
POSTAL	Section 2.10	ML_STRING, Section 2.2.2
PHONE	Section 2.11	"string" per [RFC8259]
EMAIL	Section 2.12	"string" per [RFC8259]
URL	Section 2.13	"string" per [RFC8259]
ID	Section 2.14	"string" per [RFC8259]
IDREF	Section 2.14	"string" per [RFC8259]
SOFTWARE	Section 2.15	see Section 2.2.4
STRUCTUREDINFO	[RFC 7203]	see Section 2.2.5
EXTENSION	Section 2.16	see Section 2.2.6

Figure 1: JSON Data Types

IODEF Data Type	CBOR Data Type	CDDL prelude [RFC8610]
INTEGER	0, 1, 6 tag 2, 6 tag 3	integer
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. Integer

An integer is a subset of "number" type of JSON, which represents signed digits encoded in Base 10. The definition of this integer is "[minus] int" in [RFC7159] Section 6 manner.

2.2.2. 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  
}
```

2.2.3. Enum

Enum is an ordered list of acceptable string values. Each value has a representative keyword. Within the data model, the enumerated type keywords are used as attribute values.

2.2.4. 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  
}
```

2.2.5. 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
}

```

2.2.6. 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?	3.1

	Incident+ AdditionalData*	
Incident	purpose ext-purpose? status? ext-status? lang? restriction? ext-restriction? observable-id? IncidentID AlternativeID? RelatedActivity* DetectTime? StartTime? EndTime? RecoveryTime? ReportTime? GenerationTime Description* Discovery* Assessment* Method* Contact+ EventData* Indicator* History? AdditionalData*	3.2
IncidentID	id name instance? restriction? ext-restriction?	3.4
AlternativeID	restriction? ext-restriction? IncidentID+	3.5
RelatedActivity	restriction? ext-restriction? IncidentID* URL* ThreatActor* Campaign* IndicatorID* Confidence?	3.6

	Description* AdditionalData*	
ThreatActor	restriction? ext-restriction? ThreatActorID* URL* Description* AdditionalData*	3.7
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? ext-restriction? observable-id? Application Description* DetectionConfiguration*	3.10.1
Method	restriction? ext-restriction? Reference* Description* AttackPattern* Vulnerability* Weakness* AdditionalData*	3.11
Reference	observable-id? ReferenceName? URL* Description*	3.11.1
Assessment	occurrence? 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? Key+	3.23

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.
- o EmailBody represents an whole message body including MIME structure in the same manner defined in [RFC7970]. In case of an email composed of MIME multipart, the EmailBody contains multiple body parts separated by boundary strings.

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)
        52656C617465644163746976697479 # "RelatedActivity"
81          # array(1)
      A2          # map(2)
        6B          # text(11)
        5468726561744163746F72   # "ThreatActor"
      81          # array(1)
        A2          # map(2)
          6D          # text(13)
          5468726561744163746F724944 # "ThreatActorID"
          81          # array(1)
          78 1A        # text(26)
          54412D31322D414747524553534956452D425554544552464
          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)
                    4F72616E67652047697261666665 # "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)

```

```

      436F6E74616374          # "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: "nids" / "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" /
    "anonymization" / "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|\\+\\-([0-9]|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": {"$ref": "#/definitions/MLStringType"},
    "minItems": 1}},
  "required": ["TelephoneNumber"],
  "additionalProperties": false},
"Discovery": {
  "type": "object",
  "properties": {
    "source": {
      "enum": ["nids", "hips", "siem", "av", "third-party-monitoring",
        "incident", "os-log", "application-log", "device-log",
        "network-flow", "passive-dns", "investigation", "audit",
        "internal-notification", "external-notification", "leo",
        "partner", "actor", "unknown", "ext-value"]},
    "ext-source": {"type": "string"},
    "restriction": {"$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": {"$ref": "#/definitions/IDtype"}},
    "required": ["value", "category"],
    "additionalProperties": false},
  "NodeRole": {
    "type": "object",
    "properties": {
      "category": {
        "enum": ["client", "client-enterprise", "client-partner",
          "client-remote", "client-kiosk", "client-mobile",
          "server-internal", "server-public", "www", "mail", "webmail",
          "messaging", "streaming", "voice", "file", "ftp", "p2p", "name",
          "directory", "credential", "print", "application", "database",
          "backup", "dhcp", "assessment", "source-control",
          "config-management", "monitoring", "infra", "infra-firewall",
          "infra-router", "infra-switch", "camera", "proxy",
          "remote-access", "log", "virtualization", "pos", "scada",
          "scada-supervisory", "sinkhole", "honeypot", "anonymization",
          "c2-server", "malware-distribution", "drop-server",
          "hop-point", "reflector", "phishing-site",
          "spear-phishing-site", "recruiting-site", "fraudulent-site",
          "ext-value"]},
      "ext-category": {"type": "string"},
      "Description": {
        "type": "array",
        "items": {"$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

MILE
Internet-Draft
Intended status: Standards Track
Expires: September 2, 2020

T. Takahashi
NICT
R. Danyliw
CERT
M. Suzuki
NICT
March 1, 2020

JSON binding of IODEF
draft-ietf-mile-jsoniodef-14

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 JSON and its encoding in CBOR.

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 September 2, 2020.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

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	2
1.1. Requirements Language	3
2. IODEF Data Types	3
2.1. Abstract Data Type to JSON Data Type Mapping	3
2.2. Complex JSON Types	5
2.2.1. Integer	5
2.2.2. Multilingual Strings	5
2.2.3. Enum	6
2.2.4. Software and Software Reference	6
2.2.5. Structured Information	6
2.2.6. EXTENSION	7
3. IODEF JSON Data Model	7
3.1. Classes and Elements	8
3.2. Mapping between JSON and XML IODEF	18
4. Examples	19
4.1. Minimal Example	19
4.2. Indicators from a Campaign	22
5. Mapkeys	26
6. The IODEF Data Model (CDDL)	30
7. IANA Considerations	50
8. Security Considerations	50
9. Acknowledgments	50
10. References	50
10.1. Normative References	50
10.2. Informative References	51
Appendix A. Data Types used in this document	51
Appendix B. The IODEF Data Model (JSON Schema)	52
Authors' Addresses	80

1. Introduction

The Incident Object Description Exchange Format (IODEF) [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.

IODEF documents are structured and thus suitable for machine processing. They will streamline incident response operations. Another well-used and structured format that is suitable for machine processing is JavaScript Object Notation (JSON) [RFC8259]. To facilitate the automation of incident response operations, IODEF documents and implementations should support JSON representation and its encoding in Concise Binary Object Representation (CBOR) [RFC7049].

This document defines an alternate implementation of the IODEF UML information model by specifying a JavaScript Object Notation (JSON) data model using Concise Data Definition Language (CDDL) [RFC8610] and JSON Schema [I-D.handrews-json-schema-validation]. 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 6. 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

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, see Section 2.2.1
REAL	Section 2.2	"number" per [RFC8259]
CHARACTER	Section 2.3	"string" per [RFC8259]
STRING	Section 2.3	"string" per [RFC8259]
ML_STRING	Section 2.4	see Section 2.2.2
BYTE	Section 2.5.1	"string" per [RFC8259]
BYTE[]	Section 2.5.1	"string" per [RFC8259]
HEXBIN	Section 2.5.2	"string" per [RFC8259]
HEXBIN[]	Section 2.5.2	"string" per [RFC8259]
ENUM	Section 2.6	see Section 2.2.3
DATETIME	Section 2.7	"string" per [RFC8259]
TIMEZONE	Section 2.8	"string" per [RFC8259]
PORTLIST	Section 2.9	"string" per [RFC8259]
POSTAL	Section 2.10	ML_STRING, Section 2.2.2
PHONE	Section 2.11	"string" per [RFC8259]
EMAIL	Section 2.12	"string" per [RFC8259]
URL	Section 2.13	"string" per [RFC8259]
ID	Section 2.14	"string" per [RFC8259]
IDREF	Section 2.14	"string" per [RFC8259]
SOFTWARE	Section 2.15	see Section 2.2.4
STRUCTUREDINFO	[RFC 7203]	see Section 2.2.5
EXTENSION	Section 2.16	see Section 2.2.6

Figure 1: JSON Data Types

IODEF Data Type	CBOR Data Type	CDDL prelude [RFC8610]
INTEGER	0, 1, 6 tag 2, 6 tag 3	integer
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	6 tag 23	eb16
HEXBIN[]	6 tag 23	eb16
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. Integer

An integer is a subset of "number" type of JSON, which represents signed digits encoded in Base 10. The definition of this integer is "[minus] int" in [RFC8259] Section 6 manner.

2.2.2. 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 6. An example is shown below.

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

Note that in figures throughout this document, some supplementary information follows "#", but these are not valid syntax in JSON, but are intended to facilitate reader understanding.

2.2.3. Enum

Enum is an ordered list of acceptable string values. Each value has a representative keyword. Within the data model, the enumerated type keywords are used as attribute values.

2.2.4. 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 6. 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  
}
```

2.2.5. 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 Section 4.4 of [RFC7203] as a basic structure of its extension classes. The STRUCTUREDINFO data type is implemented as an object with "SpecID", "ext-SpecID", "ContentID",

"RawData", and "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, it should be encoded as a BYTE type object, as shown below.

```
"StructuredInfo": {
  "SpecID": "urn:ietf:params:xml:ns:mile:mmdef:1.2",    # ENUM
  "RawData": "<<< encoded structured data >>>"        # BYTE
}
```

When embedding the raw data, base64 encoding defined in Section 4 of [RFC4648] MUST be used for JSON IODEF while binary representation MUST be used for CBOR IODEF.

2.2.6. 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
}
```

Note that this data type is specified in [RFC7970] as its generic extension mechanism. If a data item has internal structure that is intended to be processed outside of the IODEF framework, one may consider using StructuredInfo data type mentioned in Section 2.2.5.

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 6 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? RelatedActivity* DetectTime? StartTime? EndTime? RecoveryTime? ReportTime? GenerationTime Description* Discovery* Assessment* Method* Contact+ EventData* Indicator* History? AdditionalData*	3.2
IncidentID	id name	3.4

	instance? restriction? ext-restriction?	
AlternativeID	restriction? ext-restriction? IncidentID+	3.5
RelatedActivity	restriction? ext-restriction? IncidentID* URL* ThreatActor* Campaign* IndicatorID* Confidence? Description* AdditionalData*	3.6
ThreatActor	restriction? ext-restriction? ThreatActorID* URL* Description* AdditionalData*	3.7
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? ext-restriction? observable-id? Application Description* DetectionConfiguration*	3.10.1
Method	restriction? ext-restriction? Reference* Description* AttackPattern* Vulnerability* Weakness* AdditionalData*	3.11
Weakness (TBD)	restriction? ext-restriction?	

Reference	observable-id? ReferenceName? URL* Description*	3.11.1
Assessment	occurrence? 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? Key+	3.23
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 JSON and XML IODEF

- o Attributes and elements of each class in XML IODEF document are both presented as JSON attributes in JSON IODEF document, and the order of their appearances is ignored.
- 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 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. Implementations need to be capable of parsing MLStringType that could take form of both text and object.
- o The elements of ML_STRING type in XML IODEF document are presented as either STRING type or ML_STRING type in JSON IODEF document. When converting from XML IODEF document to JSON one or vice versa, the information contained in the original data of ML_STRING type must be preserved. When STRING is used instead of ML_STRING, parsers can assume that its "xml:lang" is set to "en".
- 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 using base64 encoding for JSON IODEF and binary representation for CBOR IODEF to represent them as BYTE object.
- o EmailBody represents an whole message body including MIME structure in the same manner defined in [RFC7970]. In case of an email composed of MIME multipart, the EmailBody contains multiple body parts separated by boundary strings.
- o The "ipv6-net-mask" type attribute of BulkObservable class remains available for the backward compatibility purpose, but the use of this attribute is not recommended because IPV6 does not use netmask any more.
- o ENUM values in this document is extensible and is managed by IANA, as with [RFC7970]. The values in the table are used both by [RFC7970] implementations and by their JSON (and CBOR) bindings as specified by this document.
- o This document uses JSON's "number" type to represent integers that only has full precision for integer values between -2^{53} and 2^{53} . When dealing with integers outside the range, this issue needs to be considered.
- o Binaries are encoded in bytes. Note that XML IODEF in [RFC7970] uses HEXBIN due to the incapability of XML for embedding binaries as they are.

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)
  37                                 # negative(23)
  63                                 # text(3)
    322E30                          # "2.0"
  36                                 # negative(22)
  62                                 # text(2)
    656E                            # "en"
  32                                 # negative(18)
  81                                 # array(1)
    A5                              # map(5)
      21                            # negative(1)
      69                            # text(9)
        7265706F7274696E67         # "reporting"
      29                            # negative(9)
      67                            # text(7)
        70726976617465             # "private"
      02                            # unsigned(2)
      A2                            # map(2)
        12                          # unsigned(18)
        66                          # text(6)
          343932333832              # "492382"
        2E                          # negative(14)
        71                          # text(17)
          63736972742E6578616D706C652E636F6D # "csirt.example.com"
      0A                            # unsigned(10)
      78 19                         # text(25)
        323031352D30372D31385430393A30303A30302D30353A3030
          # "2015-07-18T09:00:00-05:00"
      0E                            # unsigned(14)
      81                            # array(1)
        A3                          # map(3)
          18 1C                      # unsigned(28)
          6C                          # text(12)
            6F7267616E697A6174696F6E # "organization"
          18 1A                      # unsigned(26)
          67                          # text(7)
            63726561746F72           # "creator"
          18 22                      # unsigned(34)
          81                          # array(1)
            A1                        # map(1)
              18 29                  # unsigned(41)
              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": "domain-name",
    "BulkObservableList": "kj290023j09r34.example.com"}
  }
}]]
}]]
}

```

Figure 6: Indicators from a Campaign in JSON

```

A3                                     # map(3)
37                                     # negative(23)
63                                     # text(3)
    322E30                             # "2.0"
36                                     # negative(22)
62                                     # text(2)
    656E                               # "en"
32                                     # negative(18)
81                                     # array(1)
    A9                                 # map(9)
        21                             # negative(1)
        65                             # text(5)
            7761746368                 # "watch"
        29                             # negative(9)
        65                             # text(5)
            677265656E                 # "green"
        02                             # unsigned(2)
        A2                             # map(2)
            12                         # unsigned(18)
            66                         # text(6)
                383937393233           # "897923"
            2E                         # negative(14)
            71                         # text(17)
                63736972742E6578616D706C652E636F6D
                    # "csirt.example.com"
        04                             # unsigned(4)
        81                             # array(1)
            A2                         # map(2)
                14                     # unsigned(20)
                81                     # array(1)
                    A2                 # map(2)
                        18 18           # unsigned(24)
                        81               # array(1)
                            78 1A       # text(26)
                                54412D31322D414747524553534956452D425554544552464C59
                                    # "TA-12-AGGRESSIVE-BUTTERFLY"
                                    24   # negative(4)
                                    81   # array(1)
                                        74   # text(20)

```

```

4167677265737369766520427574746572666C79
# "Aggressive Butterfly"
15 # unsigned(21)
81 # array(1)
A2 # map(2)
18 19 # unsigned(25)
81 # array(1)
6C # text(12)
432D323031352D3539343035
# "C-2015-59405"
24 # negative(4)
81 # array(1)
6E # text(14)
4F72616E67652047697261666665
# "Orange Giraffe"
0A # unsigned(10)
78 19 # text(25)
323031352D31302D30325431313A31383A30302D30353A3030
# "2015-10-02T11:18:00-05:00"
24 # negative(4)
81 # array(1)
78 6F # text(111)
53756D6D6172697A65732074686520496E64696361746F7273206F6620436F6D70
726F6D69736520666F7220746865204F72616E676520476972616666652063616D706169676E206F6
620746865204167677265737369766520427574746572666C79206372696D652067616E672E
# "Summarizes the Indicators of
# Compromise for the Orange Giraffe
# campaign of the Aggressive
# Butterfly crime gang."
0C # unsigned(12)
81 # array(1)
A1 # map(1)
18 3F # unsigned(63)
81 # array(1)
A1 # map(1)
18 41 # unsigned(65)
A1 # map(1)
18 1C # unsigned(28)
72 # text(18)
6272656163682D70726F7072696574617279
# "breach-proprietary"
0E # unsigned(14)
81 # array(1)
A4 # map(4)
18 1C # unsigned(28)
6C # text(12)
6F7267616E697A6174696F6E
# "organization"
18 1A # unsigned(26)
67 # text(7)

```

```

        63726561746F72      # "creator"
18 1E      # unsigned(30)
81      # array(1)
        75      # text(21)
        435349525420666F72206578616D706C652E636F6D
        # "CSIRT for example.com"
18 22      # unsigned(34)
81      # array(1)
        A1      # map(1)
            18 29      # unsigned(41)
            78 19      # text(25)
            636F6E746163744063736972742E6578616D706C652E636F6D
            # "contact@csirt.example.com"
10      # unsigned(16)
81      # array(1)
        A4      # map(4)
            16      # unsigned(22)
            A3      # map(3)
                12      # unsigned(18)
                69      # text(9)
                473930383233343930 # "G90823490"
                2E      # negative(14)
                71      # text(17)
                63736972742E6578616D706C652E636F6D
                # "csirt.example.com"
            37      # negative(23)
            61      # text(1)
            31      # "1"
            24      # negative(4)
            81      # array(1)
            6A      # text(10)
            433220646F6D61696E73 # "C2 domains"
            06      # unsigned(6)
            78 19      # text(25)
            323031342D31322D30325431313A31383A30302D30353A3030
            # "2014-12-02T11:18:00-05:00"
18 AB      # unsigned(171)
        A1      # map(1)
            18 B0      # unsigned(176)
            A2      # map(2)
                18 1C      # unsigned(28)
                6B      # text(11)
                646F6D61696E2D6E616D65
                # "domain-name"
            18 B2      # unsigned(178)
            78 1A      # text(26)
            6B6A3239303032336A30397233342E6578616D706C652E636F6D
            # "kj290023j09r34.example.com"

```


Figure 7: Indicators from a Campaign in CBOR

5. Mapkeys

The mapkeys are provided in Table Figure 8 for minimizing the CBOR size.

mapkey	cborkey
iodef-version	-24
iodef-lang	-23
iodef-format-id	-22
iodef-private-enum-name	-21
iodef-private-enum-id	-20
iodef-Incident	-19
iodef-AdditionalData	-18
iodef-value	-17
iodef-translation-id	-16
iodef-name	-15
iodef-dtype	-14
iodef-ext-dtype	-13
iodef-meaning	-12
iodef-formatid	-11
iodef-restriction	-10
iodef-ext-restriction	-9
iodef-observable-id	-8
iodef-SoftwareReference	-7
iodef-URL	-6
iodef-Description	-5
iodef-spec-name	-4
iodef-ext-spec-name	-3
iodef-purpose	-2
iodef-ext-purpose	-1
iodef-status	0
iodef-ext-status	1
iodef-IncidentID	2
iodef-AlternativeID	3
iodef-RelatedActivity	4
iodef-DetectTime	5
iodef-StartTime	6
iodef-EndTime	7
iodef-RecoveryTime	8
iodef-ReportTime	9
iodef-GenerationTime	10
iodef-Discovery	11
iodef-Assessment	12
iodef-Method	13

iodef-Contact	14
iodef-EventData	15
iodef-Indicator	16
iodef-History	17
iodef-id	18
iodef-instance	19
iodef-ThreatActor	20
iodef-Campaign	21
iodef-IndicatorID	22
iodef-Confidence	23
iodef-ThreatActorID	24
iodef-CampaignID	25
iodef-role	26
iodef-ext-role	27
iodef-type	28
iodef-ext-type	29
iodef-ContactName	30
iodef-ContactTitle	31
iodef-RegistryHandle	32
iodef-PostalAddress	33
iodef-Email	34
iodef-Telephone	35
iodef-Timezone	36
iodef-handle	37
iodef-registry	38
iodef-ext-registry	39
iodef-PAddress	40
iodef-EmailTo	41
iodef-TelephoneNumber	42
iodef-source	43
iodef-ext-source	44
iodef-DetectionPattern	45
iodef-DetectionConfiguration	46
iodef-Application	47
iodef-Reference	48
iodef-AttackPattern	49
iodef-Vulnerability	50
iodef-Weakness	51
iodef-SpecID	52
iodef-ext-SpecID	53
iodef-ContentID	54
iodef-RawData	55
iodef-Platform	56
iodef-Scoring	57
iodef-ReferenceName	58
iodef-specIndex	59
iodef-ID	60
iodef-occurrence	61

iodef-IncidentCategory	62
iodef-Impact	63
iodef-SystemImpact	64
iodef-BusinessImpact	65
iodef-TimeImpact	66
iodef-MonetaryImpact	67
iodef-IntendedImpact	68
iodef-Counter	69
iodef-MitigatingFactor	70
iodef-Cause	71
iodef-severity	72
iodef-completion	73
iodef-ext-severity	74
iodef-metric	75
iodef-ext-metric	76
iodef-duration	77
iodef-ext-duration	78
iodef-currency	79
iodef-rating	80
iodef-ext-rating	81
iodef-HistoryItem	82
iodef-action	83
iodef-ext-action	84
iodef-DateTime	85
iodef-DefinedCOA	86
iodef-System	87
iodef-Expectation	88
iodef-RecordData	89
iodef-category	90
iodef-ext-category	91
iodef-interface	92
iodef-spoofed	93
iodef-virtual	94
iodef-ownership	95
iodef-ext-ownership	96
iodef-Node	97
iodef-NodeRole	98
iodef-Service	99
iodef-OperatingSystem	100
iodef-AssetID	101
iodef-DomainData	102
iodef-Address	103
iodef-Location	104
iodef-vlan-name	105
iodef-vlan-num	106
iodef-unit	107
iodef-ext-unit	108
iodef-system-status	109

iodef-ext-system-status	110
iodef-domain-status	111
iodef-ext-domain-status	112
iodef-Name	113
iodef-DateDomainWasChecked	114
iodef-RegistrationDate	115
iodef-ExpirationDate	116
iodef-RelatedDNS	117
iodef-NameServers	118
iodef-DomainContacts	119
iodef-Server	120
iodef-SameDomainContact	121
iodef-ip-protocol	122
iodef-ServiceName	123
iodef-Port	124
iodef-Portlist	125
iodef-ProtoCode	126
iodef-ProtoType	127
iodef-ProtoField	128
iodef-ApplicationHeaderField	129
iodef-EmailData	130
iodef-IANAService	131
iodef-EmailFrom	132
iodef-EmailSubject	133
iodef-EmailX-Mailer	134
iodef-EmailHeaderField	135
iodef-EmailHeaders	136
iodef-EmailBody	137
iodef-EmailMessage	138
iodef-HashData	139
iodef-Signature	140
iodef-RecordPattern	141
iodef-RecordItem	142
iodef-FileData	143
iodef-WindowsRegistryKeysModified	169
iodef-CertificateData	145
iodef-offset	146
iodef-offsetunit	147
iodef-ext-offsetunit	148
iodef-Key	149
iodef-registryaction	150
iodef-ext-registryaction	151
iodef-KeyName	152
iodef-KeyValue	153
iodef-Certificate	154
iodef-X509Data	155
iodef-File	156
iodef-FileName	157

iodef-FileSize	158
iodef-FileType	159
iodef-AssociatedSoftware	160
iodef-FileProperties	161
iodef-scope	162
iodef-HashTargetID	163
iodef-Hash	164
iodef-FuzzyHash	165
iodef-DigestMethod	166
iodef-DigestValue	167
iodef-CanonicalizationMethod	168
iodef-FuzzyHashValue	169
iodef-AlternativeIndicatorID	170
iodef-Observable	171
iodef-uid-ref	172
iodef-IndicatorExpression	173
iodef-IndicatorReference	174
iodef-AttackPhase	175
iodef-BulkObservable	176
iodef-BulkObservableFormat	177
iodef-BulkObservableList	178
iodef-operator	179
iodef-ext-operator	180
iodef-euid-ref	181
iodef-AttackPhaseID	182

Figure 8: Mapkeys

6. The IODEF Data Model (CDDL)

This section provides the IODEF data model. Note that mapkeys are described at the beginning of the CDDL data model for better readability.

```
start = iodef
```

```
;;; iodef.json: IODEF-Document
```

```
iodef-version = -24
iodef-lang = -23
iodef-format-id = -22
iodef-private-enum-name = -21
iodef-private-enum-id = -20
iodef-Incident = -19
iodef-AdditionalData = -18
iodef-value = -17
iodef-translation-id = -16
```

```
iodef-name = -15
iodef-dtype = -14
iodef-ext-dtype = -13
iodef-meaning = -12
iodef-formatid = -11
iodef-restriction = -10
iodef-ext-restriction = -9
iodef-observable-id = -8
iodef-SoftwareReference = -7
iodef-URL = -6
iodef-Description = -5
iodef-spec-name = -4
iodef-ext-spec-name = -3
iodef-purpose = -2
iodef-ext-purpose = -1
iodef-status = 0
iodef-ext-status = 1
iodef-IncidentID = 2
iodef-AlternativeID = 3
iodef-RelatedActivity = 4
iodef-DetectTime = 5
iodef-StartTime = 6
iodef-EndTime = 7
iodef-RecoveryTime = 8
iodef-ReportTime = 9
iodef-GenerationTime = 10
iodef-Discovery = 11
iodef-Assessment = 12
iodef-Method = 13
iodef-Contact = 14
iodef-EventData = 15
iodef-Indicator = 16
iodef-History = 17
iodef-id = 18
iodef-instance = 19
iodef-ThreatActor = 20
iodef-Campaign = 21
iodef-IndicatorID = 22
iodef-Confidence = 23
iodef-ThreatActorID = 24
iodef-CampaignID = 25
iodef-role = 26
iodef-ext-role = 27
iodef-type = 28
iodef-ext-type = 29
iodef-ContactName = 30
iodef-ContactTitle = 31
iodef-RegistryHandle = 32
```

iodef-PostalAddress = 33
iodef-Email = 34
iodef-Telephone = 35
iodef-Timezone = 36
iodef-handle = 37
iodef-registry = 38
iodef-ext-registry = 39
iodef-PAddress = 40
iodef-EmailTo = 41
iodef-TelephoneNumber = 42
iodef-source = 43
iodef-ext-source = 44
iodef-DetectionPattern = 45
iodef-DetectionConfiguration = 46
iodef-Application = 47
iodef-Reference = 48
iodef-AttackPattern = 49
iodef-Vulnerability = 50
iodef-Weakness = 51
iodef-SpecID = 52
iodef-ext-SpecID = 53
iodef-ContentID = 54
iodef-RawData = 55
iodef-Platform = 56
iodef-Scoring = 57
iodef-ReferenceName = 58
iodef-specIndex = 59
iodef-ID = 60
iodef-occurrence = 61
iodef-IncidentCategory = 62
iodef-Impact = 63
iodef-SystemImpact = 64
iodef-BusinessImpact = 65
iodef-TimeImpact = 66
iodef-MonetaryImpact = 67
iodef-IntendedImpact = 68
iodef-Counter = 69
iodef-MitigatingFactor = 70
iodef-Cause = 71
iodef-severity = 72
iodef-completion = 73
iodef-ext-severity = 74
iodef-metric = 75
iodef-ext-metric = 76
iodef-duration = 77
iodef-ext-duration = 78
iodef-currency = 79
iodef-rating = 80

iodef-ext-rating = 81
iodef-HistoryItem = 82
iodef-action = 83
iodef-ext-action = 84
iodef-DateTime = 85
iodef-DefinedCOA = 86
iodef-System = 87
iodef-Expectation = 88
iodef-RecordData = 89
iodef-category = 90
iodef-ext-category = 91
iodef-interface = 92
iodef-spoofed = 93
iodef-virtual = 94
iodef-ownership = 95
iodef-ext-ownership = 96
iodef-Node = 97
iodef-NodeRole = 98
iodef-Service = 99
iodef-OperatingSystem = 100
iodef-AssetID = 101
iodef-DomainData = 102
iodef-Address = 103
iodef-Location = 104
iodef-vlan-name = 105
iodef-vlan-num = 106
iodef-unit = 107
iodef-ext-unit = 108
iodef-system-status = 109
iodef-ext-system-status = 110
iodef-domain-status = 111
iodef-ext-domain-status = 112
iodef-Name = 113
iodef-DateDomainWasChecked = 114
iodef-RegistrationDate = 115
iodef-ExpirationDate = 116
iodef-RelatedDNS = 117
iodef-NameServers = 118
iodef-DomainContacts = 119
iodef-Server = 120
iodef-SameDomainContact = 121
iodef-ip-protocol = 122
iodef-ServiceName = 123
iodef-Port = 124
iodef-Portlist = 125
iodef-ProtoCode = 126
iodef-ProtoType = 127
iodef-ProtoField = 128

iodef-ApplicationHeaderField = 129
iodef-EmailData = 130
iodef-IANAService = 131
iodef-EmailFrom = 132
iodef-EmailSubject = 133
iodef-EmailX-Mailer = 134
iodef-EmailHeaderField = 135
iodef-EmailHeaders = 136
iodef-EmailBody = 137
iodef-EmailMessage = 138
iodef-HashData = 139
iodef-Signature = 140
iodef-RecordPattern = 141
iodef-RecordItem = 142
iodef-FileData = 143
iodef-WindowsRegistryKeysModified = 169
iodef-CertificateData = 145
iodef-offset = 146
iodef-offsetunit = 147
iodef-ext-offsetunit = 148
iodef-Key = 149
iodef-registryaction = 150
iodef-ext-registryaction = 151
iodef-KeyName = 152
iodef-KeyValue = 153
iodef-Certificate = 154
iodef-X509Data = 155
iodef-File = 156
iodef-FileName = 157
iodef-FileSize = 158
iodef-FileType = 159
iodef-AssociatedSoftware = 160
iodef-FileProperties = 161
iodef-scope = 162
iodef-HashTargetID = 163
iodef-Hash = 164
iodef-FuzzyHash = 165
iodef-DigestMethod = 166
iodef-DigestValue = 167
iodef-CanonicalizationMethod = 168
iodef-FuzzyHashValue = 169
iodef-AlternativeIndicatorID = 170
iodef-Observable = 171
iodef-uid-ref = 172
iodef-IndicatorExpression = 173
iodef-IndicatorReference = 174
iodef-AttackPhase = 175
iodef-BulkObservable = 176

```
iodef-BulkObservableFormat = 177
iodef-BulkObservableList = 178
iodef-operator = 179
iodef-ext-operator = 180
iodef-euid-ref = 181
iodef-AttackPhaseID = 182

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

duration = "second" / "minute" / "hour" / "day" / "month" / "quarter" /
"year" / "ext-value"
lang = "" / text .regex "[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 .regex "[a-zA-Z_][a-zA-Z0-9_.-]*"
IDREFType = IDtype
URLtype = uri
TimeZonetype = text .regex "Z|([\\+\\-])(0[0-9]|1[0-4]):[0-5][0-9]"
PortlistType = text .regex "[0-9]+(\\-[0-9]+)?(,[0-9]+(\\-[0-9]+)?)*"
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 = {
  iodef-value => text,
  ? iodef-lang => lang,
  ? iodef-translation-id => text
} / text
```

```
PositiveFloatType = float32 .gt 0
```

```
PAddressType = MLStringType
```

```
ExtensionType = {  
  iodef-value => text,  
  ? iodef-name => text,  
  iodef-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"  
  ? iodef-ext-dtype => text,  
  ? iodef-meaning => text,  
  ? iodef-formatid => text,  
  ? iodef-restriction => restriction .default "private",  
  ? iodef-ext-restriction => text,  
  ? iodef-observable-id => IDtype,  
}
```

```
SoftwareType = {  
  ? iodef-SoftwareReference => SoftwareReference,  
  ? iodef-URL => [+ URLtype],  
  ? iodef-Description => [+ MLStringType]  
}
```

```
SoftwareReference = {  
  ? iodef-value => text,  
  iodef-spec-name => "custom" / "cpe" / "swid" / "ext-value",  
  ? iodef-ext-spec-name => text,  
  ? iodef-dtype => "bytes" / "integer" / "real" / "string" / "xml" /  
  "ext-value" .default "string",  
  ? iodef-ext-dtype => text  
}
```

```
Incident = {  
  iodef-purpose => "traceback" / "mitigation" / "reporting" / "watch" /  
  "other" / "ext-value",  
  ? iodef-ext-purpose => text,  
  ? iodef-status => "new" / "in-progress" / "forwarded" / "resolved" /  
  "future" / "ext-value",  
  ? iodef-ext-status => text,  
  ? iodef-lang => lang,  
  ? iodef-restriction => restriction .default "private",  
  ? iodef-ext-restriction => text,  
  ? iodef-observable-id => IDtype,  
  iodef-IncidentID => IncidentID,  
  ? iodef-AlternativeID => AlternativeID,
```

```
? iodef-RelatedActivity => [+ RelatedActivity],
? iodef-DetectTime => DATETIME,
? iodef-StartTime => DATETIME,
? iodef-EndTime => DATETIME,
? iodef-RecoveryTime => DATETIME,
? iodef-ReportTime => DATETIME,
iodef-GenerationTime => DATETIME,
? iodef-Description => [+ MLStringType],
? iodef-Discovery => [+ Discovery],
? iodef-Assessment => [+ Assessment],
? iodef-Method => [+ Method],
iodef-Contact => [+ Contact],
? iodef-EventData => [+ EventData],
? iodef-Indicator f=> [+ Indicator],
? iodef-History => History,
? iodef-AdditionalData => [+ ExtensionType]
}

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

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

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

ThreatActor = {
  ? iodef-restriction => restriction .default "private",
  ? iodef-ext-restriction => text,
```

```
? iodef-ThreatActorID => [+ text],
? iodef-URL => [+ URLtype],
? iodef-Description => [+ MLStringType],
? iodef-AdditionalData => [+ ExtensionType]
}
```

```
Campaign = {
  ? iodef-restriction => restriction .default "private",
  ? iodef-ext-restriction => text,
  ? iodef-CampaignID => [+ text],
  ? iodef-URL => [+ URLtype],
  ? iodef-Description => [+ MLStringType],
  ? iodef-AdditionalData => [+ ExtensionType]
}
```

```
Contact = {
  iodef-role => "creator" / "reporter" / "admin" / "tech" / "provider" / "user" /,
  "billing" / "legal" / "irt" / "abuse" / "cc" / "cc-irt" / "leo" /
  "vendor" / "vendor-support" / "victim" / "victim-notified" /
  "ext-value",
  ? iodef-ext-role => text,
  iodef-type => "person" / "organization" / "ext-value",
  ? iodef-ext-type => text,
  ? iodef-restriction => restriction .default "private",
  ? iodef-ext-restriction => text,
  ? iodef-ContactName => [+ MLStringType],
  ? iodef-ContactTitle => [+ MLStringType],
  ? iodef-Description => [+ MLStringType],
  ? iodef-RegistryHandle => [+ RegistryHandle],
  ? iodef-PostalAddress => [+ PostalAddress],
  ? iodef-Email => [+ Email],
  ? iodef-Telephone => [+ Telephone],
  ? iodef-Timezone => TimeZonetype,
  ? iodef-Contact => [+ Contact],
  ? iodef-AdditionalData => [+ ExtensionType]
}
```

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

```
PostalAddress = {
  ? iodef-type => "street" / "mailing" / "ext-value",
  ? iodef-ext-type => text,
  iodef-PAddress => PAddressType,
}
```

```
? iodef-Description => [+ MLStringType]
}

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

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

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

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

Method = {
  ? iodef-restriction => restriction .default "private",
  ? iodef-ext-restriction => text,
  ? iodef-Reference => [+ Reference],
  ? iodef-Description => [+ MLStringType],
  ? iodef-AttackPattern => [+ StructuredInfo],
  ? iodef-Vulnerability => [+ StructuredInfo],
  ? iodef-Weakness => [+ StructuredInfo],
  ? iodef-AdditionalData => [+ ExtensionType]
```

```
}

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

Platform = {
  iodef-SpecID => SpecID,
  ? iodef-ext-SpecID => text,
  ? iodef-ContentID => text,
  ? iodef-RawData => [+ BYTE],
  ? iodef-Reference => [+ Reference]
}

Scoring = {
  iodef-SpecID => SpecID,
  ? iodef-ext-SpecID => text,
  ? iodef-ContentID => text,
  ? iodef-RawData => [+ BYTE],
  ? iodef-Reference => [+ Reference]
}

Reference = {
  ? iodef-observable-id => IDtype,
  ? iodef-ReferenceName => ReferenceName,
  ? iodef-URL => [+ URLtype],
  ? iodef-Description => [+ MLStringType]
}

ReferenceName = {
  iodef-specIndex => integer,
  iodef-ID => IDtype
}

Assessment = {
  ? iodef-occurrence => "actual" / "potential",
  ? iodef-restriction => restriction .default "private",
  ? iodef-ext-restriction => text,
  ? iodef-observable-id => IDtype,
  ? iodef-IncidentCategory => [+ MLStringType],
  iodef-Impact => [+ {iodef-SystemImpact => SystemImpact} /
    {iodef-BusinessImpact => BusinessImpact} /
    {iodef-TimeImpact => TimeImpact} /
    {iodef-MonetaryImpact => MonetaryImpact} /
    {iodef-IntendedImpact => BusinessImpact}],

```

```
? iodef-Counter => [+ Counter],
? iodef-MitigatingFactor => [+ MLStringType],
? iodef-Cause => [+ MLStringType],
? iodef-Confidence => Confidence,
? iodef-AdditionalData => [+ ExtensionType]
}
```

```
SystemImpact = {
  ? iodef-severity => "low" / "medium" / "high",
  ? iodef-completion => "failed" / "succeeded",
  iodef-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",
  ? iodef-ext-type => text,
  ? iodef-Description => [+ MLStringType]
}
```

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

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

```
MonetaryImpact = {
  iodef-value => PositiveFloatType,
  ? iodef-severity => "low" / "medium" / "high",
}
```



```
? iodef-currency => text
}

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

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

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

EventData = {
  ? iodef-restriction => restriction .default "default",
  ? iodef-ext-restriction => text,
  ? iodef-observable-id => IDtype,
  ? iodef-Description => [+ MLStringType],
  ? iodef-DetectTime => DATETIME,
  ? iodef-StartTime => DATETIME,
  ? iodef-EndTime => DATETIME,
  ? iodef-RecoveryTime => DATETIME,
  ? iodef-ReportTime => DATETIME,
  ? iodef-Contact => [+ Contact],
  ? iodef-Discovery => [+ Discovery],
  ? iodef-Assessment => Assessment,
  ? iodef-Method => [+ Method],
  ? iodef-System => [+ System],
  ? iodef-Expectation => [+ Expectation],
  ? iodef-RecordData => [+ RecordData],
  ? iodef-EventData => [+ EventData],
  ? iodef-AdditionalData => [+ ExtensionType]
```

```
}

Expectation = {
  ? iodef-action => action .default "other",
  ? iodef-ext-action => text,
  ? iodef-severity => "low" / "medium" / "high",
  ? iodef-restriction => restriction .default "default",
  ? iodef-ext-restriction => text,
  ? iodef-observable-id => IDtype,
  ? iodef-Description => [+ MLStringType],
  ? iodef-DefinedCOA => [+ text],
  ? iodef-StartTime => DATETIME,
  ? iodef-EndTime => DATETIME,
  ? iodef-Contact => Contact
}

System = {
  ? iodef-category => "source" / "target" / "intermediate" / "sensor" /
  "infrastructure" / "ext-value",
  ? iodef-ext-category => text,
  ? iodef-interface => text,
  ? iodef-spoofed => "unknown" / "yes" / "no" .default "unknown",
  ? iodef-virtual => "yes" / "no" / "unknown" .default "unknown",
  ? iodef-ownership => "organization" / "personal" / "partner" / "customer" /
  "no-relationship" / "unknown" / "ext-value",
  ? iodef-ext-ownership => text,
  ? iodef-restriction => restriction .default "private",
  ? iodef-ext-restriction => text,
  ? iodef-observable-id => IDtype,
  iodef-Node => Node,
  ? iodef-NodeRole => [+ NodeRole],
  ? iodef-Service => [+ Service],
  ? iodef-OperatingSystem => [+ SoftwareType],
  ? iodef-Counter => [+ Counter],
  ? iodef-AssetID => [+ text],
  ? iodef-Description => [+ MLStringType],
  ? iodef-AdditionalData => [+ ExtensionType]
}

Node = {
  (iodef-DomainData => [+ DomainData] // iodef-Address => [+ Address]),
  ? iodef-PostalAddress => PostalAddress,
  ? iodef-Location => [+ MLStringType],
  ? iodef-Counter => [+ Counter]
}

Address = {
  iodef-value => text,
```

```
iodef-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",  
? iodef-ext-category => text,  
? iodef-vlan-name => text,  
? iodef-vlan-num => integer,  
? iodef-observable-id => IDtype  
}
```

```
NodeRole = {  
  iodef-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" /  
"anonymization" / "c2-server" / "malware-distribution" /  
"drop-server" / "hop-point" / "reflector" /  
"phishing-site" / "spear-phishing-site" / "recruiting-site" /  
"fraudulent-site" / "ext-value",  
  ? iodef-ext-category => text,  
  ? iodef-Description => [+ MLStringType]  
}
```

```
Counter = {  
  iodef-value => float32,  
  iodef-type => "count" / "peak" / "average" / "ext-value",  
  ? iodef-ext-type => text,  
  iodef-unit => "byte" / "mbit" / "packet" / "flow" / "session" / "alert" /  
"message" / "event" / "host" / "site" / "organization" /  
"ext-value",  
  ? iodef-ext-unit => text,  
  ? iodef-meaning => text,  
  ? iodef-duration => duration .default "hour",  
  ? iodef-ext-duration => text  
}
```

```
DomainData = {  
  iodef-system-status => "spoofed" / "fraudulent" / "innocent-hacked" /  
"innocent-hijacked" / "unknown" / "ext-value",  
  ? iodef-ext-system-status => text,  
  iodef-domain-status => "reservedDelegation" / "assignedAndActive" /
```

```
"assignedAndInactive" / "assignedAndOnHold" /
"revoked" / "transferPending" / "registryLock" /
"registrarLock" / "other" / "unknown" / "ext-value",
? iodef-ext-domain-status => text,
? iodef-observable-id => IDtype,
iodef-Name => text,
? iodef-DateDomainWasChecked => DATETIME,
? iodef-RegistrationDate => DATETIME,
? iodef-ExpirationDate => DATETIME,
? iodef-RelatedDNS => [+ ExtensionType],
? iodef-NameServers => [+ NameServers],
? iodef-DomainContacts => DomainContacts
}

NameServers = {
  iodef-Server => text,
  iodef-Address => [+ Address]
}

DomainContacts = {
  (iodef-SameDomainContact => text // iodef-Contact => [+ Contact])
}

Service = {
  ? iodef-ip-protocol => integer,
  ? iodef-observable-id => IDtype,
  ? iodef-ServiceName => ServiceName,
  ? iodef-Port => integer,
  ? iodef-Portlist => PortlistType,
  ? iodef-ProtoCode => integer,
  ? iodef-ProtoType => integer,
  ? iodef-ProtoField => integer,
  ? iodef-ApplicationHeaderField => [+ ExtensionType],
  ? iodef-EmailData => EmailData,
  ? iodef-Application => SoftwareType
}

ServiceName = {
  ? iodef-IANAService => text,
  ? iodef-URL => [+ URLtype],
  ? iodef-Description => [+ MLStringType]
}

EmailData = {
  ? iodef-observable-id => IDtype,
  ? iodef-EmailTo => [+ text],
  ? iodef-EmailFrom => text,
  ? iodef-EmailSubject => text,
```

```
? iodef-EmailX-Mailer => text,  
? iodef-EmailHeaderField => [+ ExtensionType],  
? iodef-EmailHeaders => text,  
? iodef-EmailBody => text,  
? iodef-EmailMessage => text,  
? iodef-HashData => [+ HashData],  
? iodef-Signature => [+ BYTE]  
}
```

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

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

```
WindowsRegistryKeysModified = {  
  ? iodef-observable-id => IDtype,  
  iodef-Key => [+ Key]  
}
```

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

```
}

CertificateData = {
  ? iodef-restriction => restriction .default "private",
  ? iodef-ext-restriction => text,
  ? iodef-observable-id => IDtype,
  iodef-Certificate => [+ Certificate]
}

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

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

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

HashData = {
  iodef-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",
  ? iodef-HashTargetID => text,
  ? iodef-Hash => [+ Hash],
  ? iodef-FuzzyHash => [+ FuzzyHash]
}

Hash = {
  iodef-DigestMethod => BYTE,
  iodef-DigestValue => BYTE,
  ? iodef-CanonicalizationMethod => BYTE,
  ? iodef-Application => SoftwareType
}
```

```
}

FuzzyHash = {
  iodef-FuzzyHashValue => [+ ExtensionType],
  ? iodef-Application => SoftwareType,
  ? iodef-AdditionalData => [+ ExtensionType]
}

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

IndicatorID = {
  iodef-id => IDtype,
  iodef-name => text,
  iodef-version => text
}

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

Observable = {
  ? iodef-restriction => restriction .default "private",
  ? iodef-ext-restriction => text,
  ? (iodef-System => System // iodef-Address => Address //
     iodef-DomainData => DomainData // iodef-EmailData => EmailData //
     iodef-Service => Service //
     iodef-WindowsRegistryKeysModified => WindowsRegistryKeysModified //
     iodef-FileData => FileData // iodef-CertificateData => CertificateData //
     iodef-RegistryHandle => RegistryHandle // iodef-RecordData => RecordData //
```

```
    iodef-EventData => EventData // iodef-Incident => Incident //
    iodef-Expectation => Expectation // iodef-Reference => Reference //
    iodef-Assessment => Assessment //
    iodef-DetectionPattern => DetectionPattern //
    iodef-HistoryItem => HistoryItem //
    iodef-BulkObservable => BulkObservable //
    iodef-AdditionalData => [+ ExtensionType]
  }

BulkObservable = {
  ? iodef-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",
  ? iodef-ext-type => text,
  ? iodef-BulkObservableFormat => BulkObservableFormat,
  iodef-BulkObservableList => text,
  ? iodef-AdditionalData => [+ ExtensionType]
}

BulkObservableFormat = {
  (iodef-Hash => Hash // iodef-AdditionalData => [+ ExtensionType])
}

IndicatorExpression = {
  ? iodef-operator => "not" / "and" / "or" / "xor" .default "and",
  ? iodef-ext-operator => text,
  ? iodef-IndicatorExpression => [+ IndicatorExpression],
  ? iodef-Observable => [+ Observable],
  ? iodef-uid-ref => [+ IDREFType],
  ? iodef-IndicatorReference => [+ IndicatorReference],
  ? iodef-Confidence => Confidence,
  ? iodef-AdditionalData => [+ ExtensionType]
}

IndicatorReference = {
  (iodef-uid-ref => IDREFType // iodef-euid-ref => text),
  ? iodef-version => text
}

AttackPhase = {
  ? iodef-AttackPhaseID => [+ text],
  ? iodef-URL => [+ URLtype],
  ? iodef-Description => [+ MLStringType],
```



```
? iodef-AdditionalData => [+ ExtensionType]
}
```

Figure 9: Data Model in CDDL

7. IANA Considerations

This document does not require any IANA actions.

8. Security Considerations

This document provides a mapping from XML IODEF defined in [RFC7970] to JSON, and Section 3.2 describes several issues that arise when converting XML IODEF and JSON IODEF. Though it does not provide any further security considerations than the one described in [RFC7970], implementers of this document should be aware of those issues to avoid any unintended outcome.

9. Acknowledgments

We would like to thank Henk Birkholz, Carsten Bormann, Benjamin Kaduk, Alexey Melnikov, Yasuaki Morita, and Takahiko Nagata for their insightful comments on this document and CDDL.

10. References

10.1. 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>>.
- [RFC7049] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", RFC 7049, DOI 10.17487/RFC7049, October 2013, <<https://www.rfc-editor.org/info/rfc7049>>.

- [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>>.
- [RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <<https://www.rfc-editor.org/info/rfc8259>>.
- [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>>.

10.2. Informative References

- [I-D.handrews-json-schema-validation] Wright, A., Andrews, H., and B. Hutton, "JSON Schema Validation: A Vocabulary for Structural Validation of JSON", draft-handrews-json-schema-validation-02 (work in progress), September 2019.

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 10: CDDL Prelude mapping in JSON

Appendix B. The IODEF Data Model (JSON Schema)

This section provides a JSON schema [I-D.handrews-json-schema-validation] 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": "[0-9]+(\\-[0-9]+)?(,[0-9]+(\\-[0-9]+)?)*"},
    "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": ["nids", "hids", "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": {"$ref": "#/definitions/IDtype"}},
  "required": ["value", "category"],
  "additionalProperties": false},
"NodeRole": {
  "type": "object",
  "properties": {
    "category": {
      "enum": ["client", "client-enterprise", "client-partner",
        "client-remote", "client-kiosk", "client-mobile",
        "server-internal", "server-public", "www", "mail", "webmail",
        "messaging", "streaming", "voice", "file", "ftp", "p2p", "name",
        "directory", "credential", "print", "application", "database",
        "backup", "dhcp", "assessment", "source-control",
        "config-management", "monitoring", "infra", "infra-firewall",
        "infra-router", "infra-switch", "camera", "proxy",
        "remote-access", "log", "virtualization", "pos", "scada",
        "scada-supervisory", "sinkhole", "honeypot", "anonymization",
        "c2-server", "malware-distribution", "drop-server",
        "hop-point", "reflector", "phishing-site",
        "spear-phishing-site", "recruiting-site", "fraudulent-site",
        "ext-value"]},
    "ext-category": {"type": "string"},
    "Description": {
      "type": "array",
      "items": {"$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 11: 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

MILE Working Group
Internet-Draft
Intended status: Informational
Expires: September 27, 2019

S. Banghart
NIST
J. Field
Pivotal
March 26, 2019

Definition of ROLIE CSIRT Extension
draft-ietf-mile-rolie-csirt-02

Abstract

This document extends the Resource-Oriented Lightweight Information Exchange (ROLIE) core to add the information type categories and related requirements needed to support Computer Security Incident Response Team (CSIRT) use cases. The indicator and incident information types are defined as ROLIE extensions. Additional supporting requirements are also defined that describe the use of specific formats and link relations pertaining to the new information types.

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 September 27, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

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	3
2. Terminology	4
3. Additional Requirements for the Atom Publishing Protocol . .	4
3.1. Use of HTTP requests	4
3.1.1. / (forward slash) Resource URL	4
4. Information-type Extensions	4
4.1. The "incident" information type	4
4.2. The "indicator" information type	5
5. Data format requirements	5
5.1. Incident Object Description Exchange Format	6
5.1.1. Description	6
5.1.2. Requirements	6
5.2. Structured Threat Information eXpression (STIX) Format .	7
5.2.1. Description	7
5.2.2. Requirements	7
5.3. Malware Information Sharing Platform (MISP) Format . . .	7
5.3.1. Creating MISP Event Entries	8
5.3.2. MISP Feeds and Manifests	8
6. atom:link Extensions	9
6.1. Link relations for the 'incident'	
information-type	9
6.2. Link relations for the 'indicator'	
information-type	10
6.3. Link relations for both information-types	11
7. atom:category Extensions	11
7.1. Newly registered category values	12
7.2. Expectation and Impact Classes	12
8. IANA Considerations	12
8.1. information-type registrations	12
8.1.1. incident information-type	13
8.1.2. indicator information-type	13
8.2. atom:category scheme registrations	13
8.2.1. category:csirt:iodef:purpose	13
8.2.2. category:csirt:iodef:restriction	13
8.3. rolie:property name registrations	14
8.3.1. property:csirt:id	14
9. Security Considerations	14
10. Normative References	14
Appendix A. Examples of Use	15
Authors' Addresses	17

1. Introduction

Threats to computer security are evolving ever more rapidly as time goes on. As software increases in complexity, the number of vulnerabilities in systems and networks can increase exponentially. Threat actors looking to exploit these vulnerabilities are making more frequent and more widely distributed attacks across a large variety of systems. The adoption of liberal information sharing amongst attackers allows a discovered vulnerability to be shared and used to attack a vulnerable system within a narrow window of time. As the skills and knowledge required to identify and combat these attacks become more and more specialized, even a well established and secure system may find itself unable to quickly respond to an incident. Effective identification of and response to a sophisticated attack requires open cooperation and collaboration between defending operators, software vendors, and end-users. To improve the timeliness of responses, automation must be used to acquire, contextualize, and put to use shared computer security information.

CSIRTs share two primary forms of information: incidents and indicators. Using these forms of information, analysts are able to perform a wide range of activities both proactive and reactive to ensure the security of their systems.

Incident information describes a cyber security incident. Such information may include attack characteristics, information about the attacker, and attack vector data. Sharing this information helps analysts within the sharing community to inoculate their systems against similar attacks, providing proactive protection.

Indicator information describes the symptoms or necessary pre-conditions of an attack. Everything from system vulnerabilities to unexpected network traffic can help analysts secure systems and prepare for an attack. Making this information available for sharing aids in the proactive defense of systems both within an operating unit but also for any CSIRTs that are part of a sharing consortium.

As a means to bring automation of content discovery and dissemination into the CSIRT domain, this specification provides an extension to the Resource-Oriented Lightweight Information Exchange (ROLIE) core [RFC8322] designed to address CSIRT use cases. The primary purpose of this extension is to define two new information types: incident, and indicator, along with formats and link relations that support these information-types.

2. Terminology

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 [RFC2119].

Definitions for some of the common computer security-related terminology used in this document can be found in Section 2 of [RFC5070].

3. Additional Requirements for the Atom Publishing Protocol

This document specifies the following additional requirements for use of the Atom Publishing Protocol.[RFC5023]

3.1. Use of HTTP requests

This document defines the following requirements on HTTP request behavior:

3.1.1. / (forward slash) Resource URL

The forward slash resource URL SHOULD be supported as defined in Section 5.5 [RFC8322]. Note that this is a stricter requirement than [RFC8322].

4. Information-type Extensions

4.1. The "incident" information type

When an "atom:category" element has a "scheme" attribute equal to "urn:ietf:params:rolie:category:information-type", the "term" attribute defines the information type of the associated resource. A new valid "term" value for this "scheme": "incident", is described in this section, and registered in Section 8.1.1.

The "incident" information type represents any information describing or pertaining to a computer security incident. This document uses the definition of incident provided by [RFC4949]. Provided below is a non-exhaustive list of information that may be considered to be an incident information type.

- o Timing information: start and end times for the incident and/or the response.
- o Descriptive information: plain text or machine readable data that provides some degree of description of the incident itself.

- o Response information: the methods and results of a response to the incident.
- o Meta and contact information: data about the CSIRT that recorded the information, or the operator that enacted the response.
- o Effect and result information: data that describes the effects of an incident, or what the final results of the incident are.

Note again that this list is not exhaustive, any information that in is the abstract realm of an incident should be classified under this information-type.

4.2. The "indicator" information type

When an "atom:category" element has a "scheme" attribute equal to "urn:ietf:params:rolie:category:information-type", the "term" attribute defines the information type of the associated resource. A new valid "term" value for this "scheme": "indicator", is described in this section, and registered in Section 8.1.2.

The "indicator" information type represents computer security indicators or any information surrounding them. This document uses the definition of indicator provided by [RFC4949]. Some examples of indicator information is provided below, but note that indicator is defined in an abstract sense, to be understood as a flexible and widely-applicable definition.

- o Specific vulnerabilities that indicate a vector for attack.
- o Signs of malicious reconnaissance.
- o Definitions of patterns of other indicators.
- o Events that may indicate an attack and information regarding those events.
- o Meta information about the collecting agent.

This list is intended to provide examples of the indicator information-type, not to define it.

5. Data format requirements

This section defines usage guidance and additional requirements related to data formats above and beyond those specified in [RFC8322]. The following formats are expected to be commonly used to express software descriptor information. For this reason, this

document specifies additional requirements to ensure interoperability.

5.1. Incident Object Description Exchange Format

5.1.1. Description

The Incident Object Description Exchange Format (IODEF) is a format for representing computer security information commonly exchanged between Computer Security Incident Response Teams (CSIRTs) or other operational security teams.

IODEF conveys indicators, incident reports, response activities, and related meta-data in an XML serialization. This information is formally structured in order to support and encourage automated machine-to-machine security communication, as well as enhanced processing at the endpoint.

The full IODEF specification [RFC7970] provides further high-level discussion and technical details.

5.1.2. Requirements

For an Entry to be considered as a "IODEF Entry", it MUST fulfill the following conditions:

- o The information-type of the Entry is "indicator" or "incident". For a typical Entry, this is derived from the information type of the Feed it is contained in. For a standalone Entry, this is provided by an "atom:category" element.

o

- o The document linked to by the "href" attribute of the "atom:content" element is an IODEF document as per [RFC7970]

A "IODEF Entry" MUST conform to the following requirements:

- o The value of the "type" attribute of the "atom:content" element MUST be "application/xml".
- o There MUST be at least one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "<Indicator-ID>" or the "<Incident-ID>" element in the attached IODEF document. This allows for ROLIE consumers to more easily search for IODEF documents without needing to download the document itself.

5.2. Structured Threat Information eXpression (STIX) Format

5.2.1. Description

STIX is a structured language for describing a wide range of security resources. STIX approaches the problem with a focus on flexibility, automation, readability, and extensibility.

The full STIX specification [stix2] provides further high-level discussion and technical details.

5.2.2. Requirements

For an Entry to be considered as a "STIX Entry", it MUST fulfill the following conditions:

- o The information-type of the Entry is "indicator" or "incident". For a typical Entry, this is derived from the information type of the Feed it is contained in. For a standalone Entry, this is provided by an "atom:category" element.

o

- o The document linked to by the "href" attribute of the "atom:content" element is a STIX object as per [stix2]

A "STIX Entry" MUST conform to the following requirements:

- o The value of the "type" attribute of the "atom:content" element MUST be "application/xml" or "application/json".
- o There MUST be at least one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "<id>" element in the attached STIX object. This allows for ROLIE consumers to more easily search for STIX objects without needing to download the document itself.

5.3. Malware Information Sharing Platform (MISP) Format

MISP involves documentation, utilities, and formats designed to facilitate the day-to-day duties of security operators. MISP includes its own data format that is used to share between MISP features. While MISP has Feed features that can share and distribute events, it has support for linking to other sharing methods like ROLIE.

MISP is defined by a family of internet drafts and are actively being worked on. With that in mind, this extension will provide non-

normative guidance on using MISP format data in ROLIE. In the future, when the MISP format is formally published, this document will be updated to normative requirements around MISP content.

5.3.1. Creating MISP Event Entries

MISP content should be syndicated in ROLIE using the following guidance:

- o The information-type of the Entry is "indicator". For a typical Entry, this is derived from the information type of the Feed it is contained in. For a standalone Entry, this is provided by an "atom:category" element.
- o The document linked to by the "href" attribute of the "atom:content" element is a MISP Event object as per [I-D.dulaunoy-misp-core-format]
- o The value of the "type" attribute of the "atom:content" element should be "application/xml".
- o There should be at least one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "<uuid>" element in the attached MISP Event. This allows for ROLIE consumers to more easily search for MISP Events without needing to download the document itself.
- o It is also recommended to expose information in the ROLIE Entry that is required and recommended to expose in the MISP Manifest format. This ensures better compatibility between a ROLIE Feed and a MISP Manifest
 - * The following fields are required by the MISP draft: info, Orgc, timestamp, date
 - * The following fields are recommended by the MISP draft: analysis, threat_level_id

5.3.2. MISP Feeds and Manifests

MISP Feeds are hosted lists of MISP events, each event represented by its uuid. Users request Events on a one-by-one basis and are served the full Event on each request.

MISP Manifest files list MISP events by their uuids as well, but provide a variety of metadata for each Event inline. After examining the minimized and stripped Event in the manifest, a user could search

for the Event uuid of interest in a locally located folder of Event files where the file name is the uuid of the Event.

ROLIE hosting MISP data would operate as a combination of these approaches. Each ROLIE Feed would contain a list of Event Entries, each with metadata and identifying information about a given Event. Should the user be interested in the Event, the Event Entry provides a direct link to download the full Event. In short, a ROLIE MISP Feed is minimally mappable to a MISP Manifest file where a resolvable link to the MISP Event was injected into each Event described in the Manifest.

With that in mind, a MISP Feed as well as a MISP Manifest with attached local file list could be fully converted and hosted as a ROLIE repository. As a lower overhead alternative, a ROLIE server could simply provide a view into MISP data.

6. atom:link Extensions

This section defines additional link relationships that implementations MUST support. These relationships are not registered in the Link Relation IANA table as their use case is too narrow. Each relationship is named and described.

These relations come in related pairs. The first of each pair is expected to be more common, as they can be determined at the time that the Entry is created. The second of each pair will often need to be added retroactively to an Entry.

6.1. Link relations for the 'incident' information-type

If a ROLIE server supports either the incident information-types, then these link relations MUST be supported

Name	Description	Conformance
indicators	Provides a link to a collection of zero or more instances of cyber security indicators that are associated with the resource. attacker	evidence
Provides a link to a collection of zero or more resources that provides some proof of attribution for an incident. The evidence may or may not have any identified chain of custody. vector	Provides a link to a collection of zero or more resources that provides a representation of the method used by the attacker.	Provides a link to a collection of zero or more resources that provides a representation of the attacker.

Table 1: Link Relations for Resource-Oriented Lightweight Indicator Exchange

6.2. Link relations for the 'indicator' information-type

If a ROLIE server supports the indicator information-types, then these link relations MUST be supported.

Name	Description	Conformance
incidents	Provides a link to a collection of zero or more instances of incident representations associated with the resource.	

Table 2: Link Relations for Resource-Oriented Lightweight Indicator Exchange

6.3. Link relations for both information-types

If a ROLIE server supports either the incident or the indicator information-types, then these link relations MUST be supported.

Name	Description	Conformance
assessments	Provides a link to a collection of zero or more resources that represent the results of executing a benchmark.	reports
Provides a link to a collection of zero or more resources that represent RID reports.	traceRequests	Provides a link to a collection of zero or more resources that represent RID traceRequests.
investigationRequests	Provides a link to a collection of zero or more resources that represent RID investigationRequests.	

Table 3: Link Relations for Resource-Oriented Lightweight Indicator Exchange

7. atom:category Extensions

7.1. Newly registered category values

This document registers two additional registered atom:category names: 'urn:ietf:params:rolie:category:csirt:iodef:purpose' and 'urn:ietf:params:rolie:category:csirt:iodef:restriction'. These categories IODEF content exposure provides valuable metadata for the searching and organization of IODEF documents.

When the name attribute of the category is 'urn:ietf:params:rolie:category:csirt:iodef:purpose', the value attribute SHOULD be constrained as per section 3.2 of IODEF [RFC7970], e.g. traceback, mitigation, reporting, or other.

When the name attribute of the category is 'urn:ietf:params:rolie:category:csirt:iodef:restriction', the value attribute SHOULD be constrained as per section 3.2 of IODEF [RFC7970], e.g. public, need-to-know, private, default.

7.2. Expectation and Impact Classes

It is frequently the case that an organization will need to triage their investigation and response activities based upon, e.g., the state of the current threat environment, or simply as a result of having limited resources.

In order to enable operators to effectively prioritize their response activity, it is RECOMMENDED that feed implementers provide Atom categories that correspond to the IODEF Expectation and Impact classes. The availability of these feed categories will enable clients to more easily retrieve and prioritize cyber security information that has already been identified as having a specific potential impact, or having a specific expectation.

Support for these categories may also enable efficiencies for organizations that already have established (or plan to establish) operational processes and workflows that are based on these IODEF classes.

8. IANA Considerations

8.1. information-type registrations

IANA has added the following entries to the "ROLIE Security Resource Information Type Sub-Registry" registry located at <<https://www.iana.org/assignments/rolie/category/information-type>> .

8.1.1. incident information-type

The entry is as follows:

name: incident

index: TBD

reference: This document, Section 4.1

8.1.2. indicator information-type

The entry is as follows:

name: indicator

index: TBD

reference: This document, Section 4.2

8.2. atom:category scheme registrations

IANA has added the following entries to the "ROLIE URN Parameters" registry located in <https://www.iana.org/assignments/rolie/>.

8.2.1. category:csirt:iodef:purpose

The entry is as follows:

name: category:csirt:iodef:purpose

Extension IRI: urn:ietf:params:rolie:category:csirt:iodef:purpose

Reference: This document, Section 7.1

Subregistry: None

8.2.2. category:csirt:iodef:restriction

The entry is as follows:

name: category:csirt:iodef:restriction

Extension IRI:

urn:ietf:params:rolie:category:csirt:iodef:restriction

Reference: This document, Section 7.1

Subregistry: None

8.3. rolie:property name registrations

IANA has added the following entries to the "ROLIE URN Parameters" registry located in <<https://www.iana.org/assignments/rolie/>>.

8.3.1. property:csirt:id

The entry is as follows:

name: property:csirt:id

Extension IRI: urn:ietf:params:rolie:property:csirt:id

Reference: This document, section 6.3.1

Subregistry: None

9. Security Considerations

This document implies the use of ROLIE in high-security use cases, as such, added care should be taken to fortify and secure ROLIE repositories and clients using this extension. The guidance in the ROLIE core specification is strongly recommended, and implementers should consider adding additional security measures as they see fit.

When providing a private workspace for closed sharing, it is recommended that the ROLIE repository checks user authorization when the user sends a GET request to the service document. If the user is not authorized to send any requests to a given workspace or collection, that workspace or collection should be truncated from the service document in the response. In this way the existence of unauthorized content remains unknown to potential attackers, hopefully reducing attack surface.

10. Normative References

[I-D.dulaunoy-misp-core-format]

Dulaunoy, A. and A. Iklody, "MISP core format", draft-dulaunoy-misp-core-format-07 (work in progress), February 2019.

[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>>.

- [RFC4287] Nottingham, M., Ed. and R. Sayre, Ed., "The Atom Syndication Format", RFC 4287, DOI 10.17487/RFC4287, December 2005, <<https://www.rfc-editor.org/info/rfc4287>>.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/info/rfc4949>>.
- [RFC5023] Gregorio, J., Ed. and B. de hOra, Ed., "The Atom Publishing Protocol", RFC 5023, DOI 10.17487/RFC5023, October 2007, <<https://www.rfc-editor.org/info/rfc5023>>.
- [RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, DOI 10.17487/RFC5070, December 2007, <<https://www.rfc-editor.org/info/rfc5070>>.
- [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>>.
- [RFC8322] Field, J., Banghart, S., and D. Waltermire, "Resource-Oriented Lightweight Information Exchange (ROLIE)", RFC 8322, DOI 10.17487/RFC8322, February 2018, <<https://www.rfc-editor.org/info/rfc8322>>.
- [stix2] "Structured Threat Information Expression 2.0", July 2017.

Appendix A. Examples of Use

Use of this extension in a ROLIE repository will not typically change that repository's operation. As such, the general examples provided by the ROLIE core document would serve as examples. Provided below is a sample incident ROLIE entry containing an IODEF document:

```
<?xml version="1.0" encoding="UTF-8"?>
<entry xmlns="http://www.w3.org/2005/Atom"
  xmlns:rolie="urn:ietf:params:xml:ns:rolie-1.0">
  <id>f762c77c-057d-45c9-b805-677ab89aaf7c</id>
  <title>Sample Incident</title>
  <published>2018-09-04T18:13:51.0Z</published>
  <updated>2019-08-05T18:13:51.0Z</updated>
  <summary>A document containing an indicator of compromise. </summary>
  <link rel="self" href="http://www.example.org/rolie/CSIRT/123456"/>
  <link rel="feed" href="http://www.example.org/rolie/CSIRT/">
  <rolie:property name=urn:ietf:params:rolie:property:content-id
    value="id847201"/>
  <category
    scheme="urn:ietf:params:rolie:category:information-type"
    term="incident"/>
  <rolie:format
    ns="urn:ietf:params:xml:ns:iodef-2.0"/>
  <content type="application/xml"
    src="http://www.example.org/rolie/csirt/123456/data"/>
</entry>
```

Below is a sample indicator ROLIE entry containing a STIX document:

```
<?xml version="1.0" encoding="UTF-8"?>
<entry xmlns="http://www.w3.org/2005/Atom"
  xmlns:rolie="urn:ietf:params:xml:ns:rolie-1.0">
  <id>0c99df51-767f-4940-8a09-c4b607b6fe21</id>
  <title>Sample Indicator</title>
  <published>2018-09-04T18:13:51.0Z</published>
  <updated>2019-08-05T18:13:51.0Z</updated>
  <summary>A document containing an incident report. </summary>
  <link rel="self" href="http://www.example.org/rolie/CSIRT/654321"/>
  <link rel="feed" href="http://www.example.org/rolie/CSIRT/">
  <rolie:property name=urn:ietf:params:rolie:property:content-id
    value="exmaple:indicator:654321"/>
  <category
    scheme="urn:ietf:params:rolie:category:information-type"
    term="indicator"/>
  <rolie:format
    ns=http://stix.mitre.org/XMLSchema/core/1.2/stix_core.xsd"/>
  <content type="application/xml"
    src="http://www.example.org/rolie/csirt/654321/data"/>
</entry>
```


Authors' Addresses

Stephen A. Banghart
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland
USA

Phone: (301)975-4288
Email: sab3@nist.gov

John P. Field
Pivotal Software, Inc.
625 Avenue of the Americas
New York, New York
USA

Phone: (646)792-5770
Email: jfield@pivotal.io

MILE Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 30, 2020

S. Banghart
NIST
J. Field
Pivotal
October 28, 2019

Definition of ROLIE CSIRT Extension
draft-ietf-mile-rolie-csirt-06

Abstract

This document extends the Resource-Oriented Lightweight Information Exchange (ROLIE) core to add the Indicator and Incident information types, relevant categories, and related requirements needed to support Computer Security Incident Response Team (CSIRT) use cases. Additional supporting requirements are also defined that describe the use of specific formats and link relations pertaining to the new information types.

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 April 30, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect 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	3
2. Terminology	4
3. Information-type Extensions	4
3.1. The "incident" information type	4
3.2. The "indicator" information type	5
4. Data format requirements	5
4.1. Incident Object Description Exchange Format	6
4.1.1. Description	6
4.1.2. Requirements	6
4.2. Structured Threat Information eXpression (STIX) Format	6
4.2.1. Description	7
4.2.2. Requirements	7
4.3. Malware Information Sharing Platform (MISP) Format	7
4.3.1. Creating MISP Event Entries	8
4.3.2. MISP Feeds and Manifests	8
5. atom:link Extensions	9
5.1. Link relations for the 'incident' information-type	9
5.2. Link relations for the 'indicator' information-type	10
5.3. Link relations for both information-types	10
6. atom:category Extensions	11
6.1. Newly registered category values	11
6.2. Expectation and Impact Classes	11
7. IANA Considerations	12
7.1. information-type registrations	12
7.1.1. incident information-type	12
7.1.2. indicator information-type	12
7.2. atom:category scheme registrations	12
7.2.1. category:csirt:iodef:purpose	13
7.2.2. category:csirt:iodef:restriction	13
8. Security Considerations	13
9. References	14
9.1. Normative References	14
9.2. Informative References	15
Appendix A. Examples of Use	15
Authors' Addresses	16

1. Introduction

Threats to computer security are evolving ever more rapidly as time goes on. As software increases in complexity, the number of vulnerabilities in systems and networks can increase exponentially. Threat actors looking to exploit these vulnerabilities are making more frequent and more widely distributed attacks across a large variety of systems. The adoption of liberal information sharing amongst attackers allows a discovered vulnerability to be shared and used to attack a vulnerable system within a narrow window of time. As the skills and knowledge required to identify and combat these attacks become more and more specialized, even a well established and secure system may find itself unable to quickly respond to an incident. Effective identification of and response to a sophisticated attack requires open cooperation and collaboration between defending operators, software vendors, and end-users. To improve the timeliness of responses, automation must be used to acquire, contextualize, and put to use shared computer security information.

Computer Security Incident Response Teams (CSIRTs) share two primary forms of information: incidents and indicators. Using these forms of information, analysts are able to perform a wide range of activities both proactive and reactive to improve the security of their systems.

Incident information describes a cyber security incident. Such information may include attack characteristics, information about the attacker, and attack vector data. Sharing this information helps analysts within the sharing community to inoculate their systems against similar attacks, providing proactive protection.

Indicator information describes the symptoms or necessary pre-conditions of an attack. Everything from system vulnerabilities to unexpected network traffic can help analysts secure systems and prepare for an attack. Making this information available for sharing aids in the proactive defense of systems both within an operating unit but also for any CSIRTs that are part of a sharing consortium.

As a means to bring automation of content discovery and dissemination into the CSIRT domain, this specification provides an extension to the Resource-Oriented Lightweight Information Exchange (ROLIE) core [RFC8322] designed to address CSIRT use cases. The primary purpose of this extension is to define two new information types: incident, and indicator, along with formats and link relations that support these information-types.

2. Terminology

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 [RFC8174].

Definitions for some of the common computer security-related terminology used in this document can be found in Section 2 of [RFC5070].

As an extension of [RFC8322], this document refers to many terms defined in that document. In particular, the use of "Entry" and "Feed" are aligned with the definitions presented there.

Several places in this document refer to the "information-type" of a Resource (Entry or Feed). This refers to the "term" attribute of an "atom:category" element whose scheme is "urn:ietf:params:rolie:category:information-type". For an Entry, this value can be inherited from its containing Feed as per [RFC8322].

3. Information-type Extensions

3.1. The "incident" information type

When an "atom:category" element has a "scheme" attribute equal to "urn:ietf:params:rolie:category:information-type", the "term" attribute defines the information type of the associated resource. A new valid "term" value for this "scheme": "incident", is described in this section, and registered in Section 7.1.1.

The "incident" information type represents any information describing or pertaining to a computer security incident. This document uses the definition of incident provided by [RFC4949]. Provided below is a non-exhaustive list of information that may be considered to be an incident information type.

- o Timing information: start and end times for the incident and/or the response.
- o Descriptive information: plain text or machine readable data that provides some degree of description of the incident itself.
- o Response information: the methods and results of a response to the incident.
- o Meta and contact information: data about the CSIRT that recorded the information, or the operator that enacted the response.

- o Effect and result information: data that describes the effects of an incident, or what the final results of the incident are.

Note again that this list is not exhaustive, any information that is in the abstract realm of an incident should be classified under this information-type.

3.2. The "indicator" information type

When an "atom:category" element has a "scheme" attribute equal to "urn:ietf:params:rolie:category:information-type", the "term" attribute defines the information type of the associated resource. A new valid "term" value for this "scheme": "indicator", is described in this section, and registered in Section 7.1.2.

The "indicator" information type represents computer security indicators or any information surrounding them. This document uses the definition of indicator provided by [RFC4949]. Some examples of indicator information are provided below, but note that indicator is defined in an abstract sense, to be understood as a flexible and widely-applicable definition.

- o Specific vulnerabilities that indicate a vector for attack.
- o Signs of malicious reconnaissance.
- o Definitions of patterns of other indicators.
- o Events that may indicate an attack and information regarding those events.
- o Meta information about the collecting agent.

This list is intended to provide examples of the indicator information-type, not to define it.

4. Data format requirements

This section defines usage guidance and additional requirements related to data formats above and beyond those specified in [RFC8322]. The following formats are expected to be commonly used to express software descriptor information. For this reason, this document specifies additional requirements to ensure interoperability.

4.1. Incident Object Description Exchange Format

4.1.1. Description

The Incident Object Description Exchange Format (IODEF) is a format for representing computer security information commonly exchanged between Computer Security Incident Response Teams (CSIRTs) or other operational security teams.

IODEF conveys indicators, incident reports, response activities, and related meta-data in an XML serialization. This information is formally structured in order to support and encourage automated machine-to-machine security communication, as well as enhanced processing at the endpoint.

The full IODEF specification [RFC7970] provides further high-level discussion and technical details.

4.1.2. Requirements

For an Entry to be considered as a "IODEF Entry", it MUST fulfill the following conditions:

- o The information-type of the Entry is "indicator" or "incident". For a typical Entry, this is derived from the information type of the Feed it is contained in. For a standalone Entry, this is provided by an "atom:category" element.
- o The document linked to by the "href" attribute of the "atom:content" element is an IODEF document as per [RFC7970]

A "IODEF Entry" MUST conform to the following requirements:

- o The value of the "type" attribute of the "atom:content" element MUST be "application/xml".
- o There MUST be at least one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "<Indicator-ID>" or the "<Incident-ID>" element in the attached IODEF document. This allows for ROLIE consumers to more easily search for IODEF documents without needing to download the document itself.

4.2. Structured Threat Information eXpression (STIX) Format

4.2.1. Description

STIX is a structured language for describing a wide range of security resources. STIX approaches the problem with a focus on flexibility, automation, readability, and extensibility.

The full STIX specification [stix2] provides further high-level discussion and technical details.

4.2.2. Requirements

For an Entry to be considered as a "STIX Entry", it MUST fulfill the following conditions:

- o The information-type of the Entry is "indicator" or "incident". For a typical Entry, this is derived from the information type of the Feed it is contained in. For a standalone Entry, this is provided by an "atom:category" element.
- o The document linked to by the "href" attribute of the "atom:content" element is a STIX object as per [stix2]

A "STIX Entry" MUST conform to the following requirements:

- o The value of the "type" attribute of the "atom:content" element MUST be "application/xml" or "application/json".
- o There MUST be at least one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "<id>" element in the attached STIX object. This allows for ROLIE consumers to more easily search for STIX objects without needing to download the document itself.

4.3. Malware Information Sharing Platform (MISP) Format

MISP involves documentation, utilities, and formats designed to facilitate the day-to-day duties of security operators. MISP includes it's own data format that is used to share between MISP features. While MISP has Feed features that can share and distribute events, it has support for linking to other sharing methods like ROLIE.

MISP is defined by a family of internet drafts currently being developed in the IETF. With that in mind, this extension will provide non-normative guidance on using MISP format data in ROLIE. In the future, when the MISP format is formally published, this

document will be updated to normative requirements around MISP content.

4.3.1. Creating MISP Event Entries

MISP content should be syndicated in ROLIE using the following guidance:

- o The information-type of the Entry is "indicator". For a typical Entry, this is derived from the information type of the Feed it is contained in. For a standalone Entry, this is provided by an "atom:category" element.
- o The document linked to by the "href" attribute of the "atom:content" element is a MISP Event object as per [I-D.dulaunoy-misp-core-format]
- o The value of the "type" attribute of the "atom:content" element should be "application/xml".
- o There should be at least one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "<uuid>" element in the attached MISP Event. This allows for ROLIE consumers to more easily search for MISP Events without needing to download the document itself.
- o It is also recommended to expose information in the ROLIE Entry that is required and recommended to expose in the MISP Manifest format. This ensures better compatibility between a ROLIE Feed and a MISP Manifest.
 - * The following fields are required by the MISP draft: info, Orgc, timestamp, date
 - * The following fields are recommended by the MISP draft: analysis, threat_level_id

4.3.2. MISP Feeds and Manifests

MISP Feeds are hosted lists of MISP events, each event represented by its UUID. Users request Events on a one-by-one basis and are served the full Event on each request.

MISP Manifest files list MISP events by their UUIDs as well, but provide a variety of metadata for each Event inline. After examining the minimized and stripped Event in the manifest, a user could search

for the Event UUID of interest in a locally located folder of Event files where the file name is the UUID of the Event.

ROLIE hosting MISP data would operate as a combination of these approaches. Each ROLIE Feed would contain a list of Event Entries, each with metadata and identifying information about a given Event. Should the user be interested in the Event, the Event Entry provides a direct link to download the full Event. In short, a ROLIE MISP Feed is minimally mappable to a MISP Manifest file where a resolvable link to the MISP Event was injected into each Event described in the Manifest.

With that in mind, a MISP Feed as well as a MISP Manifest with attached local file list could be fully converted and hosted as a ROLIE repository. As a lower overhead alternative, a ROLIE server could simply provide a view into MISP data.

5. atom:link Extensions

This section defines additional link relationships that implementations MUST support. These relationships are not registered in the Link Relation IANA table as their use case is too narrow. Each relationship is named and described.

These relations come in related pairs. The first of each pair is expected to be more common, as they can be determined at the time that the Entry is created. The second of each pair will often need to be added retroactively to an Entry.

5.1. Link relations for the 'incident' information-type

If a ROLIE server supports the incident information-type, then these link relations MUST be supported.

Name	Description
indicators	Provides a link to a collection of zero or more instances of cyber security indicators that are associated with the resource.
evidence	Provides a link to a collection of zero or more resources that provides some proof of attribution for an incident. The evidence may or may not have any identified chain of custody.
attacker	Provides a link to a collection of zero or more resources that provides a representation of the attacker.
vector	Provides a link to a collection of zero or more resources that provides a representation of the method used by the attacker.

Table 1: Link Relations for Resource-Oriented Lightweight Indicator Exchange

5.2. Link relations for the 'indicator' information-type

If a ROLIE server supports the indicator information-type, then these link relations MUST be supported.

Name	Description
incidents	Provides a link to a collection of zero or more instances of incident representations associated with the resource.

Table 2: Link Relations for Resource-Oriented Lightweight Indicator Exchange

5.3. Link relations for both information-types

If a ROLIE server supports either the incident or the indicator information-types, then these link relations MUST be supported.

Name	Description
assessments	Provides a link to a collection of zero or more resources that represent the results of executing a benchmark.
reports	Provides a link to a collection of zero or more resources that represent RID reports.
traceRequests	Provides a link to a collection of zero or more resources that represent RID traceRequests.
investigationRequests	Provides a link to a collection of zero or more resources that represent RID investigationRequests.

Table 3: Link Relations for Resource-Oriented Lightweight Indicator Exchange

6. atom:category Extensions

6.1. Newly registered category values

This document registers two additional registered atom:category names: 'urn:ietf:params:rolie:category:csirt:iodef:purpose' and 'urn:ietf:params:rolie:category:csirt:iodef:restriction'. These categories expose important information from inside the attached IODEF document. The Purpose and Restriction elements are often used to sort or categorize IODEF documents, and in some use cases, determine the security and access permissions of the document.

When the name attribute of the category is 'urn:ietf:params:rolie:category:csirt:iodef:purpose', the value attribute SHOULD be constrained as per section 3.2 of IODEF [RFC7970], e.g. traceback, mitigation, reporting, or other.

When the name attribute of the category is 'urn:ietf:params:rolie:category:csirt:iodef:restriction', the value attribute SHOULD be constrained as per section 3.2 of IODEF [RFC7970], e.g. public, need-to-know, private, default.

6.2. Expectation and Impact Classes

It is frequently the case that an organization will need to triage their investigation and response activities based upon, e.g., the state of the current threat environment, or simply as a result of having limited resources.

In order to enable operators to effectively prioritize their response activity, it is RECOMMENDED that feed implementers provide Atom categories that correspond to the IODEF Expectation and Impact classes. The availability of these feed categories will enable clients to more easily retrieve and prioritize cyber security information that has already been identified as having a specific potential impact, or having a specific expectation.

Support for these categories may also enable efficiencies for organizations that already have established (or plan to establish) operational processes and workflows that are based on these IODEF classes.

7. IANA Considerations

7.1. information-type registrations

IANA has added the following entries to the "ROLIE Security Resource Information Type Sub-Registry" registry located at <https://www.iana.org/assignments/rolie/category/information-type> .

7.1.1. incident information-type

The entry is as follows:

name: incident

index: TBD

reference: This document, Section 3.1

7.1.2. indicator information-type

The entry is as follows:

name: indicator

index: TBD

reference: This document, Section 3.2

7.2. atom:category scheme registrations

IANA has added the following entries to the "ROLIE URN Parameters" registry located in <https://www.iana.org/assignments/rolie/>.

7.2.1. category:csirt:iodef:purpose

The entry is as follows:

name: category:csirt:iodef:purpose

Extension IRI: urn:ietf:params:rolie:category:csirt:iodef:purpose

Reference: This document, Section 6.1

Subregistry: None

7.2.2. category:csirt:iodef:restriction

The entry is as follows:

name: category:csirt:iodef:restriction

Extension IRI:

urn:ietf:params:rolie:category:csirt:iodef:restriction

Reference: This document, Section 6.1

Subregistry: None

8. Security Considerations

This document implies the use of ROLIE in high-security use cases; as such, added care should be taken to fortify and secure ROLIE repositories and clients using this extension. The guidance in the ROLIE core specification is strongly recommended, and implementers should consider adding additional security measures as they see fit.

When providing a private workspace for closed sharing, it is recommended that the ROLIE repository checks user authorization when the user sends a GET request to the service document. If the user is not authorized to send any requests to a given workspace or collection, that workspace or collection should be truncated from the service document in the response. In this way the existence of unauthorized content remains unknown to potential attackers, hopefully reducing attack surface.

When sharing IODEF Version 2 documents using a ROLIE server, care should be taken to separate IODEF Entries into different workspaces based on the "restriction" attribute of the IODEF Document (and therefore the restriction property in ROLIE). Security and access controls are most effectively deployed at the workspace level, as

such, keeping private and need-to-know IODEF documents in their own workspace helps prevent unintended information leakage.

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>>.
- [RFC4287] Nottingham, M., Ed. and R. Sayre, Ed., "The Atom Syndication Format", RFC 4287, DOI 10.17487/RFC4287, December 2005, <<https://www.rfc-editor.org/info/rfc4287>>.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/info/rfc4949>>.
- [RFC5023] Gregorio, J., Ed. and B. de hOra, Ed., "The Atom Publishing Protocol", RFC 5023, DOI 10.17487/RFC5023, October 2007, <<https://www.rfc-editor.org/info/rfc5023>>.
- [RFC5070] Danyliw, R., Meijer, J., and Y. Demchenko, "The Incident Object Description Exchange Format", RFC 5070, DOI 10.17487/RFC5070, December 2007, <<https://www.rfc-editor.org/info/rfc5070>>.
- [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>>.
- [RFC8322] Field, J., Banghart, S., and D. Waltermire, "Resource-Oriented Lightweight Information Exchange (ROLIE)", RFC 8322, DOI 10.17487/RFC8322, February 2018, <<https://www.rfc-editor.org/info/rfc8322>>.
- [stix2] Organization for the Advancement of Structured Information Standards (OASIS) Cyber Threat Intelligence (CTI) Technical Committee, "Structured Threat Information Expression 2.0", July 2017, <<https://oasis-open.github.io/cti-documentation/resources#stix-20-specification>>.

9.2. Informative References

[I-D.dulaunoy-misp-core-format]

Dulaunoy, A. and A. Iklody, "MISP core format", draft-dulaunoy-misp-core-format-07 (work in progress), February 2019.

Appendix A. Examples of Use

Use of this extension in a ROLIE repository will not typically change that repository's operation. As such, the general examples provided by the ROLIE core document would serve as examples. Provided below is a sample incident ROLIE entry containing an IODEF document:

```
<?xml version="1.0" encoding="UTF-8"?>
<entry xmlns="http://www.w3.org/2005/Atom"
  xmlns:rolie="urn:ietf:params:xml:ns:rolie-1.0">
  <id>f762c77c-057d-45c9-b805-677ab89aaf7c</id>
  <title>Sample Incident</title>
  <published>2018-09-04T18:13:51.0Z</published>
  <updated>2019-08-05T18:13:51.0Z</updated>
  <summary>A document containing an indicator of compromise. </summary>
  <link rel="self" href="http://www.example.org/rolie/CSIRT/123456"/>
  <link rel="feed" href="http://www.example.org/rolie/CSIRT/">
  <rolie:property name="urn:ietf:params:rolie:property:content-id"
    value="id847201"/>
  <category
    scheme="urn:ietf:params:rolie:category:information-type"
    term="incident"/>
  <rolie:format
    ns="urn:ietf:params:xml:ns:iodef-2.0"/>
  <content type="application/xml"
    src="http://www.example.org/rolie/csirt/123456/data"/>
</entry>
```

Below is a sample indicator ROLIE entry containing a STIX document:


```
<?xml version="1.0" encoding="UTF-8"?>
<entry xmlns="http://www.w3.org/2005/Atom"
  xmlns:rolie="urn:ietf:params:xml:ns:rolie-1.0">
  <id>0c99df51-767f-4940-8a09-c4b607b6fe21</id>
  <title>Sample Indicator</title>
  <published>2018-09-04T18:13:51.0Z</published>
  <updated>2019-08-05T18:13:51.0Z</updated>
  <summary>A document containing an incident report. </summary>
  <link rel="self" href="http://www.example.org/rolie/CSIRT/654321"/>
  <link rel="feed" href="http://www.example.org/rolie/CSIRT/" />
  <rolie:property name="urn:ietf:params:rolie:property:content-id
    value="exmaple:indicator:654321"/>
  <category
    scheme="urn:ietf:params:rolie:category:information-type"
    term="indicator"/>
  <rolie:format
    ns="http://stix.mitre.org/XMLSchema/core/1.2/stix_core.xsd"/>
  <content type="application/xml"
    src="http://www.example.org/rolie/csirt/654321/data"/>
</entry>
```

Authors' Addresses

Stephen A. Banghart
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland
USA

Phone: (301) 975-4288
Email: sab3@nist.gov

John P. Field
Pivotal Software, Inc.
625 Avenue of the Americas
New York, New York
USA

Phone: (646) 792-5770
Email: jfield@pivotal.io

MILE Working Group
Internet-Draft
Intended status: Informational
Expires: September 29, 2019

S. Banghart
NIST
March 28, 2019

Definition of the ROLIE Vulnerability Extension
draft-ietf-mile-rolie-vuln-00

Abstract

This document extends the Resource-Oriented Lightweight Information Exchange (ROLIE) core to add the information type categories and related requirements needed to support Vulnerability use cases. Additional categories, properties, and requirements based on content type enables a higher level of interoperability between ROLIE implementations, and richer metadata for ROLIE consumers. In particular, usage of the Common Vulnerability Enumeration (CVE) [cve] format and the draft Vulnerability Description Ontology (VDO) [vdo] are discussed.

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 September 29, 2019.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

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	2
2. Terminology	2
3. The "vulnerability" information type	3
4. Data Format Requirements	3
4.1. CVE Format	4
4.1.1. Description	4
4.1.2. Requirements	4
4.2. VDO Format	5
4.2.1. Description	5
4.2.2. Usage	5
5. Use of the atom:link element	5
5.1. Link relations for the 'vulnerability' information-type	6
6. IANA Considerations	6
6.1. information-type registrations	6
6.1.1. vulnerability information-type	6
6.2. rolie:property name registrations	6
7. Security Considerations	6
8. Normative References	7
Author's Address	8

1. Introduction

Vulnerability data is used in a wide variety of security use cases. Researchers, CSIRTs, enterprises, software vendors, and consumers all have a need to communicate about computer vulnerabilities. Today, a number of formats are used to describe these vulnerabilities, some of them are standardized, some of them are proprietary, and some of them are as rudimentary as a vaguely descriptive email message.

This extension does not attempt to solve the vulnerability data format issue, this work is being done across standards groups and industry consortiums. Instead, this extension serves to address the problem of sharing these data formats to downstream consumers in a automated and efficient fashion.

2. Terminology

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 [RFC2119].

3. The "vulnerability" information type

When an "atom:category" element has a "scheme" attribute equal to "urn:ietf:params:rolie:category:information-type", the "term" attribute defines the information type of the associated resource. A new valid value for this attribute: "vulnerability", is described in this section, and registered in Section 6.1.1. When this value is used, the resource in question is considered to have an information-type of "vulnerability" as per [RFC8322] Section 7.1.2.

The "vulnerability" information-type represents any information describing or pertaining to a computer security vulnerability. This document uses the definition of vulnerability provided by [RFC4949]. Provided below is a non-exhaustive list of information that may be considered to be of a vulnerability information type.

- o Fundamental identifying information, such as a global ID or number, that identifies a given vulnerability.
- o Descriptive information, including but not limited to:
 - * Severity scoring - using some standardized scoring algorithm or otherwise,
 - * Execution details - how the vulnerability is exploited
 - * Impact - what the consequences are of this vulnerability
 - * History and provenance data - when was the vulnerability discovered, when was it reported and to whom,
 - * Plain text description of any of the above
- o Metadata attached to a vulnerability, such as information about the entity that discovered or described the vulnerability.

Note again that this list is not exhaustive, any information that in is the abstract realm of an vulnerability should be classified under this information-type.

4. Data Format Requirements

This section defines usage guidance and additional requirements related to data formats above and beyond those specified in [RFC8322]. The following formats are expected to be commonly used to express software descriptor information. For this reason, this document specifies additional requirements to ensure interoperability.

4.1. CVE Format

4.1.1. Description

The Common Vulnerability Enumeration (CVE) provides a globally unique identifier for vulnerabilities. Each CVE provides a CVE-ID, by which a vulnerability can be referred to in any context, as well as descriptive information about that vulnerability.

For more information and in-depth specifications, please see [cve].

CVE provides a valuable set of information fields, but itself does not provide a standardized data format. This extension is standardized around the NIST NVD CVE Entry format [nvdcvexml]. There is a second format using the CVE information fields, defined in JSON Schema 1.0 [nvdcvejson]. These two representations of a CVE are equivalent, so either are valid when used in a ROLIE CVE Entry.

4.1.2. Requirements

For an Entry to be considered as a "CVE Entry", it MUST fulfill the following conditions:

- o The information-type of the Entry is "vulnerability". For a typical Entry, this is derived from the information type of the Feed it is contained in. For a standalone Entry, this is provided by an "atom:category" element.
- o The document linked to by the "ref" attribute of the "atom:content" element is a CVE Entry as defined by either [nvdcvexml] or [nvdcvejson].

The XML and JSON formats follow different requirements. From here on out we will refer to "CVE Entry" which is defined above, and is in the XML or JSON formats, "XML CVE Entry", which is defined in the XML format, and "JSON CVE Entry", which is defined in the JSON format.

A "XML CVE Entry" MUST conform to the following requirements:

- o The value of the "type" attribute of the "atom:content" element MUST be "application/xml".
- o There MUST be one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "<name>" element in the attached CVE Entry. This allows for ROLIE consumers to more easily search for CVE Entries without needing to download the entry itself.

A "JSON CVE Entry" MUST conform to the following requirements:

- o The value of the "type" attribute of the "atom:content" element MUST be "application/json".
- o There MUST be one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "cve:{cve_data_meta}:{ID}" element in the attached CVE Entry. This allows for ROLIE consumers to more easily search for CVE Entries without needing to download the entry itself.

4.2. VDO Format

4.2.1. Description

The Vulnerability Description Ontology (VDO) provides a dictionary and ontology for standardizing human language descriptions of vulnerabilities. CVEs expose a decent amount of information, but one of those fields is a plain text description. The VDO provides a means of completing this description in a way that makes it machine parsable and universally understandable across organizations.

The VDO is currently defined in a draft National Institute of Standards and Technology (NIST) internal report. As this draft is not yet fully stable, this document will provide only guidance on using the VDO inside a ROLIE repository.

For more in depth information please find the draft at [vdo]

4.2.2. Usage

There is currently no standardized data format for the VDO, as such, there can be no ROLIE "VDO Entry". Instead, the VDO can be utilized in plain text fields in an Entry. ROLIE properties can contain long strings of text, exposing human language information. In the vulnerability context, these human language fields can be filled in using the VDO.

It is not recommended that the content element be populated with some plain text format using the VDO.

5. Use of the atom:link element

These sections define requirements for atom:link elements in Entries. Note that the requirements are determined by the information type that appears in either the Entry or in the parent Feed.

5.1. Link relations for the 'vulnerability' information-type

If the category of an Entry is the vulnerability information type, then the following requirements MUST be followed for support of atom:link elements.

Name	Description
severity	Links to a document describing or scoring the severity of this vulnerability.

Table 1: Link Relations for Resource-Oriented Lightweight Indicator Exchange

6. IANA Considerations

6.1. information-type registrations

IANA has added the following entries to the "ROLIE Security Resource Information Type Sub-Registry" registry located at <https://www.iana.org/assignments/rolie/category/information-type> .

6.1.1. vulnerability information-type

The entry is as follows:

name: vulnerability
index: TBD
reference: This document, Section 3

6.2. rolie:property name registrations

IANA has added the following entries to the "ROLIE URN Parameters" registry located in <https://www.iana.org/assignments/rolie/>.

7. Security Considerations

All security considerations of the core ROLIE document apply to use of this extension.

The use of this particular extension implies the use of ROLIE in sharing vulnerability information. In automated use cases, downstream consumers may be dynamically acquiring and acting on vulnerabilities posted to a ROLIE repository. In this case, a

compromised server could serve up false vulnerability information to trigger dangerous activity in automated consumers. Automatic remediation solutions that consume shared vulnerability information in high risk use cases should take care to verify data before taking action. If some global ID, such as a CVE-ID, is included, this verification should be trivial.

8. Normative References

- [cve] "Common Vulnerability Enumeration", <cve.mitre.org>.
- [nvdCVEjson] "NVD CVE Entry JSON Schema",
<https://csrc.nist.gov/schema/nvd/feed/1.0/nvd_cve_feed_json_1.0.schema>.
- [nvdCVEXml] "NVD CVE Entry XML Schema",
<<https://csrc.nist.gov/schema/nvd/nvdCVE.xsd>>.
- [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>>.
- [RFC4287] Nottingham, M., Ed. and R. Sayre, Ed., "The Atom Syndication Format", RFC 4287, DOI 10.17487/RFC4287, December 2005, <<https://www.rfc-editor.org/info/rfc4287>>.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/info/rfc4949>>.
- [RFC5023] Gregorio, J., Ed. and B. de hOra, Ed., "The Atom Publishing Protocol", RFC 5023, DOI 10.17487/RFC5023, October 2007, <<https://www.rfc-editor.org/info/rfc5023>>.
- [RFC8322] Field, J., Banghart, S., and D. Waltermire, "Resource-Oriented Lightweight Information Exchange (ROLIE)", RFC 8322, DOI 10.17487/RFC8322, February 2018, <<https://www.rfc-editor.org/info/rfc8322>>.
- [vdo] "Vulnerability Description Ontology", <https://csrc.nist.gov/CSRC/media/Publications/nistir/8138/draft/documents/nistir_8138_draft.pdf>.

Author's Address

Stephen A. Banghart
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland
USA

Phone: (301) 975-4288
Email: stephen.banghart@nist.gov

MILE Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 30, 2020

S. Banghart
NIST
October 28, 2019

Definition of the ROLIE Vulnerability Extension
draft-ietf-mile-rolie-vuln-03

Abstract

This document extends the Resource-Oriented Lightweight Information Exchange (ROLIE) core to add the information type categories and related requirements needed to support Vulnerability use cases. Additional categories, properties, and requirements based on content type enables a higher level of interoperability between ROLIE implementations, and richer metadata for ROLIE consumers. In particular, usage of the Common Vulnerability Enumeration (CVE) [cve] format is discussed.

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 April 30, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect 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	2
2. Terminology	3
3. The "vulnerability" information type	3
4. Common Vulnerability Enumeration (CVE) Format	4
4.1. Description	4
4.2. Requirements	5
5. Link relations for the 'vulnerability' information-type	5
6. IANA Considerations	6
6.1. information-type registrations	6
6.1.1. vulnerability information-type	6
7. Security Considerations	6
8. Normative References	7
Author's Address	8

1. Introduction

As our software becomes more complex and interconnected, the number of software vulnerabilities exploitable by actors with mal-intent has skyrocketed. Huge amounts of resources have been poured into the preemptive discovery, description, and remediation of these vulnerabilities, but it is often a challenge to share and communicate the results of these efforts. While bad-actors have vast collaboration networks that enable widespread knowledge of any vulnerability, the defensive community at large has no sharing consortium as prevalent. If we are to keep up with the rising difficulty of defending our systems, we must increase our ability to quickly, efficiently, and automatically share information about vulnerabilities.

The Resource-Oriented Lightweight Information Exchange (ROLIE) [RFC8322] provides a means to share computer security information with an eye towards automation and efficiency. By utilizing ROLIE to share vulnerability data, we get one step closer to establishing automated communication between each party involved in fighting vulnerabilities. A security researcher can send a newly discovered vulnerability to a vulnerability repository, where it is automatically retrieved and consumed by enterprise systems. At this final stage, the enterprise can cross-reference against their enterprise wide software load to begin mitigating the issue.

This extension to ROLIE introduces new requirements and IANA registrations to allow ROLIE repositories to share vulnerability data in a standardized and compatible way.

This extension does not attempt to solve the vulnerability data format issue, as this work is being done across standards groups and industry consortiums. Instead, this extension serves to address the problem of sharing these data formats to downstream consumers in a automated and efficient fashion.

2. Terminology

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 [RFC8174].

As an extension of [RFC8322], this document refers to many terms defined in that document. In particular, the use of "Entry" and "Feed" are aligned with the definitions presented there.

Several places in this document refer to the "information-type" of a Resource (Entry or Feed). This refers to the "term" attribute of an "atom:category" element whose scheme is "urn:ietf:params:rolie:category:information-type". For an Entry, this value can be inherited from it's containing Feed as per [RFC8322].

This document uses the definition of "vulnerability" given by [RFC4949].

3. The "vulnerability" information type

When an "atom:category" element has a "scheme" attribute equal to "urn:ietf:params:rolie:category:information-type", the "term" attribute defines the information type of the associated resource. A new valid value for this attribute: "vulnerability", is described in this section, and registered in Section 6.1.1. When this value is used, the resource in question is considered to have an information-type of "vulnerability" as per [RFC8322] Section 7.1.2.

The "vulnerability" information-type represents any information describing or pertaining to a computer security vulnerability. This document uses the definition of vulnerability provided by [RFC4949]. Provided below is a non-exhaustive list of information that may be considered to be of a vulnerability information type.

- o Fundamental identifying information, such as a global ID or number, that identifies a given vulnerability.

- o Descriptive information, including but not limited to:
 - * Severity scoring - using some standardized scoring algorithm or otherwise,
 - * Execution details - how the vulnerability is exploited
 - * Impact - what the consequences are of this vulnerability
 - * History and provenance data - when was the vulnerability discovered, when was it reported and to whom,
 - * Plain text description of any of the above
- o Metadata attached to a vulnerability, such as information about the entity that discovered or described the vulnerability.

Note again that this list is not exhaustive: any information that is in the abstract realm of a vulnerability should be classified under this information-type. The final decision as to the information type of an Entry is up to the provider and author of the Entry.

4. Common Vulnerability Enumeration (CVE) Format

4.1. Description

The Common Vulnerability Enumeration (CVE) provides a globally unique identifier for vulnerabilities. Each CVE provides a CVE-ID, by which a vulnerability can be referred to in any context, as well as descriptive information about that vulnerability.

For more information and in-depth specifications, please see [cve].

CVE provides a valuable set of information fields, but itself does not provide a standardized data format. This extension provides standardization around two common serializations of the CVE standard, both used by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). The NVD provides a repository of "CVE Entries" available in either serialization format. The first format is XML-based: the NIST NVD CVE Entry format [nvdcvexml], and the second is JSON-based: NIST NVD JSON CVE Entry Format [nvdcvejson]. These two representations of a CVE are equivalent, and can be losslessly converted.

This section defines usage guidance and additional requirements above and beyond those specified in [RFC8322] that apply when CVE data formats are in use.

4.2. Requirements

For an Entry to be considered a "CVE Entry", it MUST fulfill the following conditions:

- o The information-type of the Entry is "vulnerability". For a typical Entry, this is derived from the information type of the Feed it is contained in. For a standalone Entry, this is provided by an "atom:category" element.
- o The document linked to by the "ref" attribute of the "atom:content" element is a CVE Entry as defined by either [nvdcvexml] or [nvdcvejson]. Other well-defined CVE serializations would be valid but would not be subject to the following requirements, reducing their interoperability.

The XML and JSON NVD formats follow different requirements.

A "XML CVE Entry" MUST conform to the following requirements:

- o The value of the "type" attribute of the "atom:content" element MUST be "application/xml".
- o There MUST be one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "<name>" element in the attached CVE Entry. This allows for ROLIE consumers to more easily search for CVE Entries without needing to download the entry itself.

A "JSON CVE Entry" MUST conform to the following requirements:

- o The value of the "type" attribute of the "atom:content" element MUST be "application/json".
- o There MUST be one "rolie:property" with the "name" attribute equal to "urn:ietf:params:rolie:property:content-id" and the "value" attribute exactly equal to the "cve:{cve_data_meta}:{ID}" element in the attached CVE Entry. This allows for ROLIE consumers to more easily search for CVE Entries without needing to download the entry itself.

5. Link relations for the 'vulnerability' information-type

The atom:link element contains a "rel" attribute that describes the semantic meaning of the given link.

If the category of an Entry is the vulnerability information type, then the following link relations MUST be respected, that is, not

removed, by the server. Implementations can provide extra functionality by understanding the semantic meaning of these relations.

Name	Description
severity	Links to a document describing or scoring the severity of this vulnerability.

Table 1: Link Relations for Resource-Oriented Lightweight Indicator Exchange

6. IANA Considerations

6.1. information-type registrations

IANA has added the following entries to the "ROLIE Security Resource Information Type Sub-Registry" registry located at <https://www.iana.org/assignments/rolie/category/information-type> .

6.1.1. vulnerability information-type

The entry is as follows:

name: vulnerability

index: TBD

reference: This document, Section 3

7. Security Considerations

All security considerations of the core ROLIE document apply to use of this extension.

The use of this particular extension implies the use of ROLIE in sharing vulnerability information. In automated use cases, downstream consumers may be dynamically acquiring and acting on vulnerabilities posted to a ROLIE repository. In this case, a compromised server could serve up false vulnerability information to trigger dangerous activity in automated consumers. Automatic remediation solutions that consume shared vulnerability information in high risk use cases should take care to verify data before taking action. If some global ID, such as a CVE-ID, is included, this verification should be trivial.

8. Normative References

- [cve] "Common Vulnerability Enumeration",
<<https://cve.mitre.org/about/index.html>>.
- [cvexml] The MITRE Corporation, ,
<https://cve.mitre.org/schema/cve/cve_1.0.xsd>.
- [nvdCVEjson] National Institute of Standards and Technology, "NVD CVE Entry JSON Schema",
<https://csrc.nist.gov/schema/nvd/feed/1.0/nvd_cve_feed_json_1.0.schema>.
- [nvdCVExml] National Institute of Standards and Technology, "NVD CVE Entry XML Schema",
<<https://csrc.nist.gov/schema/nvd/nvdCVE.xsd>>.
- [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>>.
- [RFC4287] Nottingham, M., Ed. and R. Sayre, Ed., "The Atom Syndication Format", RFC 4287, DOI 10.17487/RFC4287, December 2005, <<https://www.rfc-editor.org/info/rfc4287>>.
- [RFC4949] Shirey, R., "Internet Security Glossary, Version 2", FYI 36, RFC 4949, DOI 10.17487/RFC4949, August 2007, <<https://www.rfc-editor.org/info/rfc4949>>.
- [RFC5023] Gregorio, J., Ed. and B. de hOra, Ed., "The Atom Publishing Protocol", RFC 5023, DOI 10.17487/RFC5023, October 2007, <<https://www.rfc-editor.org/info/rfc5023>>.
- [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>>.
- [RFC8322] Field, J., Banghart, S., and D. Waltermire, "Resource-Oriented Lightweight Information Exchange (ROLIE)", RFC 8322, DOI 10.17487/RFC8322, February 2018, <<https://www.rfc-editor.org/info/rfc8322>>.

Author's Address

Stephen A. Banghart
National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, Maryland
USA

Phone: (301) 975-4288
Email: stephen.banghart@nist.gov