MILE Working Group
Internet-Draft
Intended status: Informational
Expires: September 6, 2018

S. Banghart
NIST
J. Field
Pivotal

March 5, 2018

Definition of ROLIE CSIRT Extension
draft-banghart-mile-rolie-csirt-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 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

Copyright Notice

Table of Contents

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. Additional Requirements for the Atom Syndication Format

This document does not specify any additional requirements for the Atom Syndication Format. [RFC4287]

5. Information-type Extensions

5.1. The "incident" information type

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.

5.2. The "indicator" information type

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.

5.3. Use of the rolie:format element

This document does not contain any additional requirements for the rolie:format element; the formats that follow are provided as examples of formats that describe the incident and indicator information type. The formats are in no particular order, and are not requirements, nor suggestions by the authors.

5.3.1. IODEF Format

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 provides further high-level discussion and technical details.

5.3.2. STIX Format

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 use of STIX as the content of an Entry does not impose any additional requirements on ROLIE implementations.

6. rolie:property Extensions

This document provides new registrations for valid rolie:property names. These properties provide optional exposure point for valuable information in the linked content document. Exposing this information in a rolie:property element means that clients do not need to download the linked document to determine if it contains the information they are looking for.

6.1. urn:ietf:params:rolie:property:csirt:ID

Provides an XML element that can be populated with an identifier from the indicator or incident document linked to by an atom:content element. This value SHOULD be a uniquely identifying value for the document linked to in this entry’s atom:content element.

7. 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.

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

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

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.	SHOULD
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.	SHOULD
attacker	Provides a link to a collection of zero or more resources that provides a representation of the attacker.	SHOULD
vector	Provides a link to a collection of zero or more resources that provides a representation of the method used by the attacker.	SHOULD

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

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

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

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

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

7.3. Link relations for both information-types

If the category of an Entry is either information-type, the following requirements MUST be followed for inclusion of atom:link elements.

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

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

8. Other Extensions

This document defines additional extensions as follows:

8.1. Use of atom:category

8.1.1. 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.

8.1.2. 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.

9. IANA Considerations

9.1. 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> .

9.1.1. incident information-type

The entry is as follows:

name: incident

index: TBD

reference: This document, Section 5.1

9.1.2. indicator information-type

The entry is as follows:

name: indicator

index: TBD

reference: This document, Section 5.2

9.2. atom:category scheme registrations

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

9.2.1. 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 8.1.1

Subregistry: None

9.2.2. 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 8.1.1

Subregistry: None

9.3. rolie:property name registrations

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

9.3.1. 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

10. 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.

11. 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>.

[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>.

Appendix A. Non-Normative Examples

The following provide examples of some potential use cases of the CSIRT ROLIE extension, and provides a showcase for some of its benefits over traditional solutions.

The general non-normative examples provided in the core ROLIE document remain an excellent reference resource for typical ROLIE usage.

A.1. Use of Link Relations

A key benefit of using the RESTful architectural style is the ability to enable the client to navigate to related resources through the use of hypermedia links. In the Atom Syndication Format, the type of the related resource identified in a <link> element is indicated via the "rel" attribute, where the value of this attribute identifies the kind of related resource available at the corresponding "href" attribute. Thus, in lieu of a well-known URI template the URI itself is effectively opaque to the client, and therefore the client must understand the semantic meaning of the "rel" attribute in order to successfully navigate. Broad interoperability may be based upon a sharing consortium defining a well-known set of Atom Link Relation types. These Link Relation types may either be registered with IANA, or held in a private registry.

Individual CSIRTs may always define their own link relation types in order to support specific use cases, however support for a core set of well-known link relation types is encouraged as this will maximize interoperability.

In addition, it may be beneficial to define use case profiles that correspond to specific groupings of supported link relationship types. In this way, a CSIRT may unambiguously specify the classes of use cases for which a client can expect to find support.

The following sections provide non-normative examples of link relation usage. Three distinct cyber security information sharing use case scenarios are described. In each use case, the unique benefits of adopting a resource-oriented approach to information sharing are illustrated. It is important to note that these use cases are intended to be a small representative set and is by no means meant to be an exhaustive list. The intent is to illustrate how the use of link relationship types will enable this resource-oriented approach to cyber security information sharing to successfully support the complete range of existing use cases, and also to motivate an initial list of well-defined link relationship types.

A.1.1. Use Case: Incident Sharing

This section provides a non-normative example of an incident sharing use case.

In this use case, a member CSIRT shares incident information with another member CSIRT in the same consortium. The client CSIRT retrieves a feed of incidents, and is able to identify one particular entry of interest. The client then does an HTTP GET on that entry, and the representation of that resource contains link relationships for both the associated "indicators" and the incident "history", and so on. The client CSIRT recognizes that some of the indicator and history may be relevant within her local environment, and can respond proactively.

Example HTTP GET response for an incident entry:

```
<?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>http://www.example.org/csirt/private/incidents/123456</id>
  <title>Sample Incident</title>
  <link href="http://www.example.org/csirt/private/incidents/123456"
    rel="self"/>
  <link href="http://www.example.org/csirt/private/incidents/123456"
    rel="alternate"/>
  <published>2012-08-04T18:13:51.0Z</published>
  <updated>2012-08-05T18:13:51.0Z</updated>

  <link href="http://www.example.org/csirt/private/incidents/123456"
    rel="edit"/>

  <!-- The links to indicators related to this incident,
       and the history of this incident, and so on.... -->
  <link href="http://www.example.org/csirt/private/incidents/123456
    /relationships/indicators" rel="indicators"/>
  <link href="http://www.example.org/csirt/private/incidents/123456
    /relationships/history" rel="history"/>
  <link href="http://www.example.org/csirt/private/incidents/123456
    /relationships/campaign" rel="campaign"/>

  <!-- navigate up to the full collection.
       Might also be rel="collection" as per IANA registry -->
  <link href="http://www.example.org/csirt/private/incidents" rel="up"/>
  <rolie:format ns="urn:example:iodef"/>
  <content type="application/xml" src="example.org/123456/source">
  <!-- Content provided here as example, the content tag is only a
       link to this file. -->
    <iodef:IODEF-Document lang="en"
      xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
      <iodef:Incident purpose="traceback" restriction="need-to-know">
        <iodef:IncidentID name="http://www.example.org/csirt/private/
          incidents">123456</iodef:IncidentID>
        <!-- ...additional incident data.... -->
        </iodef:Incident>
    </iodef:IODEF-Document>

  </content>
</entry>
```


As can be seen in the example response, the Atom <link> elements enable the client to navigate to the related indicator resources, and/or the history entries associated with this incident.

A.1.2. Use Case: Collaborative Investigation

This section provides a non-normative example of a collaborative investigation use case.

In this use case, two member CSIRTs that belong to a closed sharing consortium are collaborating on an incident investigation. The initiating CSIRT performs an HTTP GET to retrieve the service document of the peer CSIRT, and determines the collection name to be used for creating a new investigation request. The initiating CSIRT then POSTs a new incident entry to the appropriate collection URL. The target CSIRT acknowledges the request by responding with an HTTP status code 201 Created.

Example HTTP GET response for the service document:


```
HTTP/1.1 200 OK
Date: Fri, 24 Aug 2012 17:09:11 GMT
Content-Length: 934
Content-Type: application/atomsvc+xml;charset="utf-8"

<?xml version="1.0" encoding="UTF-8"?>
<service xmlns="http://www.w3.org/2007/app"
         xmlns:atom="http://www.w3.org/2005/Atom">
    <workspace xml:lang="en-US"
      xmlns:xml="http://www.w3.org/XML/1998/namespace">
      <atom:title type="text">RID Use Case Requests</atom:title>
      <collection
        href="http://www.example.org/csirt/RID/InvestigationRequests">
         <atom:title type="text">Investigation Requests</atom:title>
         <accept>application/atom+xml; type=entry</accept>
      </collection>
      <collection href="http://www.example.org/csirt/RID/TraceRequests">
         <atom:title type="text">Trace Requests</atom:title>
         <accept>application/atom+xml; type=entry</accept>
      </collection>
      <!-- ...and so on.... -->
    </workspace>
</service>
```


As can be seen in the example response, the Atom <collection> elements enable the client to determine the appropriate collection URL to request an investigation or a trace.

The client CSIRT then POSTs a new entry to the appropriate feed collection. Note that the <content> element of the new entry may contain a RID message of type "InvestigationRequest" if desired, however this would NOT be required. The entry content itself need only be an IODEF document, with the choice of the target collection resource URL indicating the callers intent. A CSIRT would be free to use any URI template to accept investigationRequests.

```
POST /csirt/RID/InvestigationRequests HTTP/1.1
Host: www.example.org
Content-Type: application/atom+xml;type=entry
Content-Length: 852
```


```
<?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">
  <title>New Investigation Request</title>
  <id>http://www.example2.org/csirt/private/incidents/123456</id>
  <!-- id and updated not guranteed to be preserved -->
  <!-- may want to profile that behavior in this document -->
  <updated>2012-08-12T11:08:22Z</updated>
  <author><name>Name of peer CSIRT</name></author>
  <rolie:format ns="urn:example:iodef"/>
  <content type="application/xml">
    <iodef:IODEF-Document lang="en"
      xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
      <iodef:Incident purpose="traceback" restriction="need-to-know">
      <iodef:IncidentID name="http://www.example2.org/csirt/
        private/incidents">123</iodef:IncidentID>
        <!-- ...additional incident data.... -->
      </iodef:Incident>
    </iodef:IODEF-Document>
  </content>
</entry>
```


The receiving CSIRT acknowledges the request with HTTP return code 201 Created.

```
HTTP/1.1 201 Created
Date: Fri, 24 Aug 2012 19:17:11 GMT
Content-Length: 906
Content-Type: application/atom+xml;type=entry
Location: http://www.example.org/csirt/RID/InvestigationRequests/823
ETag: "8a9h9he4qphqh"
```


```
<?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">
  <title>New Investigation Request</title>
  <id>http://www.example.org/csirt/RID/InvestigationRequests/823</id>
  <!-- id and updated not guranteed to be preserved -->
  <!-- may want to profile that behavior in this document -->
  <updated>2012-08-12T11:08:30Z</updated>
  <published>2012-08-12T11:08:30Z</published>
  <author><name>Name of peer CSIRT</name></author>
  <rolie:format ns="urn:example:iodef"/>
  <content type="application/xml">
    <iodef:IODEF-Document lang="en"
      xmlns:iodef="urn:ietf:params:xml:ns:iodef-1.0">
      <iodef:Incident purpose="traceback" restriction="need-to-know">
      <iodef:IncidentID name="http://www.example.org/csirt/private
        /incidents">123</iodef:IncidentID>
        <!-- ...additional incident data.... -->
      </iodef:Incident>
    </iodef:IODEF-Document>
  </content>
</entry>
```


Consistent with HTTP/1.1 RFC, the location header indicates the URL of the newly created InvestigationRequest. If for some reason the request were not authorized, the client would receive an HTTP status code 403 Unauthorized. In this case the HTTP response body may contain additional details, if an as appropriate.

A.1.3. Use Case: Cyber Data Repository

This section provides a non-normative example of a cyber security data repository use case.

In this use case a client accesses a persistent repository of cyber security data via a RESTful usage model. Retrieving a feed collection is analogous to an SQL SELECT statement producing a result set. Retrieving an individual Atom Entry is analogous to a SQL SELECT statement based upon a primary key producing a unique record. The cyber security data contained in the repository may include different data types, including indicators, incidents, benchmarks, or any other related resources. In this use case, the repository is queried via HTTP GET, and the results that are returned to the client may optionally contain URL references to other cyber security resources that are known to be related. These related resources may also be persisted locally, or they may exist at another (remote) cyber data respository.

Example HTTP GET request to a persistent repository for any resources representing Distributed Denial of Service (DDOS) attacks:

```
GET /csirt/repository/ddos
Host: www.example.org
Accept: application/atom+xml
```

The corresponding HTTP response would be an XML document containing the DDOS feed.

Example HTTP GET response for a DDOS feed:


```
HTTP/1.1 200 OK
Date: Fri, 24 Aug 2012 17:20:11 GMT
Content-Length: nnnn
Content-Type: application/atom+xml;type=feed;charset="utf-8"

<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:rolie="urn:ietf:params:xml:ns:rolie-1.0"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.w3.org/2005/Atom
                        file:/C:/schemas/atom.xsd
                        urn:ietf:params:xml:ns:iodef-1.0
                        file:/C:/schemas/iodef-1.0.xsd"
    xml:lang="en-US">

    <generator version="1.0" xml:lang="en-US">
      emc-csirt-iodef-feed-service</generator>
    <id>http://www.example.org/csirt/repository/ddos</id>
    <title type="text" xml:lang="en-US">
      Atom formatted representation of a feed of known ddos resources.
      </title>
    <updated xml:lang="en-US">2012-05-04T18:13:51.0Z</updated>
    <author>
        <email>csirt@example.org</email>
        <name>EMC CSIRT</name>
    </author>

    <!-- By convention there is usually a self link for the feed -->
```

```
    <link href="http://www.example.org/csirt/repository/ddos"
      rel="self"/>

    &lt;entry&gt;
        &lt;id&gt;http://www.example.org/csirt/repository/ddos/123456&lt;/id&gt;
        &lt;title&gt;Sample DDOS Incident&lt;/title&gt;
        <link href="http://www.example.org/csirt/repository/ddos/123456"
          rel="self"/>          &lt;!-- by convention --&gt;
        <link href="http://www.example.org/csirt/repository/ddos/123456"
          rel="alternate"/>     &lt;!-- required by Atom spec --&gt;
        <link href="http://www.example.org/csirt/repository/ddos/987654"
          rel="related"/>       <!-- link to a related DDOS resource
          in this repository -->
        <link href="http://www.cyber-agency.gov/repository/
          indicators/1a2b3c" rel="related"/>
          &lt;!-- link to a related DDOS resource in another repository --&gt;
        &lt;published&gt;2012-08-04T18:13:51.0Z&lt;/published&gt;
        &lt;updated&gt;2012-08-05T18:13:51.0Z&lt;/updated&gt;
        <!-- The category is based upon IODEF
                    purpose and restriction attributes -->
        &lt;category term="traceback" scheme="purpose" label="trace back"/&gt;
        <category term="need-to-know" scheme="restriction"
          label="need to know" />
        <category term="ddos" scheme="ttp"
          label="tactics, techniques, and procedures"/>
        &lt;summary&gt;A short description of this DDOS attack, extracted
        from the IODEF Incident class, &lt;description&gt; element. &lt;/summary&gt;
        &lt;rolie:format ns="urn:example:iodef"/&gt;
        &lt;content href="http://www.example.org/ddos/123456/data"/&gt;
    &lt;/entry&gt;

    &lt;entry&gt;
        &lt;!-- ...another entry... --&gt;
    &lt;/entry&gt;

&lt;/feed&gt;
```

This feed document has two atom entries, one of which has been elided. The completed entry illustrates an Atom <entry> element that provides a summary of essential details about one particular DDOS incident. Based upon this summary information and the provided category information, a client may choose to do an HTTP GET operation to retrieve the full details of the DDOS incident. This example shows how a persistent repository may provide links to additional resources, both local and remote.

Note that the provider of a persistent repostory is not obligated to follow any particular URL template scheme. The repository available at the hypothetical provider "www.example.com" uses a different URL pattern than the hypothetical repository available at "www.cyber-agency.gov". When a client de-references a link to resource that is located in a remote repository the client may be challenged for authentication credentials acceptable to that provider. If the two repository providers choose to support a federated identity scheme or some other form of single-sign-on technology, then the user experience can be improved for interactive clients (e.g., a human user at a browser). However, this is not required and is an implementation choice that is out of scope for this specification.

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 T. Takahashi
Internet-Draft NICT
Intended status: Standards Track R. Danyliw
Expires: September 19, 2018 CERT
M. Suzuki
NICT
March 18, 2018

JSON binding of IODEF
draft-ietf-mile-jsoniodef-03

Abstract

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

Table of Contents

1. Introduction

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

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

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

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

1.1. Requirements Language

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

2. IODEF Data Types

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

2.1. Abstract Data Type to JSON Data Type Mapping

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

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

Figure 1

2.2. Complex JSON Types

2.2.1. Multilingual Strings

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

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

2.2.2. Software

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

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

2.2.3. StructuredInfo

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

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

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

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

3. IODEF JSON Data Model

3.1. Classes and Elements

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

```
+-----------------------------+--------------------+---------------+
| IODEF Class                 | Class              | Corresponding |
|                             | Elements and       | Section       |
```

	Attribute	in [RFC7970]
IODEF-Document	version 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? GenrationTime? Description* Description_ML* 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?      | 3.6           |
   |                              | ext-restriction?  |               |
   |                              | IncidentID*       |               |
   |                              | URL*              |               |
   |                              | ThreatActor*      |               |
   |                              | Campaign*         |               |
   |                              | IndicatorID*      |               |
   |                              | Confidence?       |               |
   |                              | Description*      |               |
   |                              | AdditionalData*   |               |
   +------------------------------+-------------------+---------------+
   | ThreatActor                  | restriction?      | 3.7           |
   |                              | ext-restriction?  |               |
   |                              | ThreatActorID*    |               |
   |                              | URL*              |               |
   |                              | Description*      |               |
   |                              | Description_ML*   |               |
   |                              | AdditionalData*   |               |
   +------------------------------+-------------------+---------------+
   | Campaign                     | restriction?      |               |
   |                              | ext-restriction?  |               |
   |                              | CampaignID*       |               |
   |                              | URL*              |               |
   |                              | Description*      |               |
   |                              | Description_ML*   |               |
   |                              | AdditionalData*   | 3.8           |
   +------------------------------+-------------------+---------------+
   | Contact                      | role              |               |
   |                              | ext-role?         |               |
   |                              | type              |               |
   |                              | ext-type?         |               |
   |                              | restriction?      |               |
   |                              | ext-restriction?  |               |
   |                              | ContactName*,ContactName_ML* |    |
   |                              | ContactTitle*     |               |
   |                              | ContactTitle_ML*  |               |
   |                              | Description*      |               |
   |                              | Description_ML*   |               |
   |                              | RegistryHandle*   |               |
   |                              | PostalAddress*    |               |
   |                              | Email*            |               |
   |                              | Telephone*        |               |
   |                              | Timezone?         |               |
   |                              | Contact*          |               |
   |                              | AdditionalData*   | 3.9           |
   +------------------------------+-------------------+---------------+
   | RegistryHandle               | handle|           |               |
   |                              | registry|         |               |
```

	ext-registry?	3.9.1
PostalAddress	type?| ext-type?| PAddress| Description*| Description_ML*	3.9.2
Email	type? ext-type? EmailTo Description* Description_ML*	3.9.3
Telephone	type? ext-type? TelephoneNumber Description* Description_ML*	3.9.4
Discovery	source? ext-source? restriction? ext-restriction? Description* Description_ML* Contact* DetectionPattern*	3.10
DetectionPattern	restriction? ext-restriction? observable-id? Application Description* Description_ML* DetectionConfiguration*	3.10.1
Method	restriction? ext-restriction? Reference* Description* Description_ML* AttackPattern* Vulnerability* Weakness*	3.11
Reference	observable-id? ReferenceName?	

	URL* Description* Description_ML*	3.11.1
Assessment	occurence? restriction? ext-restriction? observable-id? IncidentCategory* SystemImpact* BusinessImpact* TimeImpact* MonetaryImpact* IntendedImpact* Counter* MitigationFactor* MitigationFactor_ML* Cause* Cause_ML* Confidence? AdditionalData*	3.12
SystemImpact	severity? completion? type ext-type? Description* Description_ML*	3.12.1
BusinessImpact	severity? ext-severity? type ext-type? Description* Description_ML*	3.12.2
TimeImpact	value severity? metric ext-metric? duration? ext-duration?	3.12.3
MonetaryImpact	value severity? currency?	3.12.4
Confidence	value	

	rating	
	ext-rating?	3.12.5
History	restriction?	
	ext-restriction?	
	HistoryItem+	3.13
HistoryItem	action	
	ext-action?	
	restriction?	
	ext-restriction?	
	observable-id?	
	DateTime	
	IncidentID?	
	Contact?	
	Description*	
	Description_ML*	
	DefinedCOA*	
	AdditionalData*	3.13.1
EventData	restriction?	
	ext-restriction?	
	observable-id?	
	Description*	
	Description_ML*	
	DetectTime?	
	StartTime?	
	EndTime?	
	RecoveryTime?	
	ReportTime?	
	Contact*	
	Discovery*	
	Assessment?	
	Method*	
	Expectation*	
	RecordData*	
	EventData*	
	AdditionalData*	3.14
Expectation	action?	
	ext-action?	
	severity?	
	restriction?	
	ext-restriction?	
	Description*	
	Description_ML*	
	DefinedCOA*	
	StartTime?	

	EndTime? Contact?	3.15
System	category? ext-category? interface? spoofed? virtual? ownership? ext-ownership? restriction? ext-restriction? Node NodeRole* Service* OperatingSystem* Counter* AssetID* Description* Description_ML* AdditionalData*	3.16
Node	DomainData* Address* PostalAddress? Location* Location_ML* Counter*	3.17
Address	value category ext-category? vlan-name? vlan-num? observable-id?	3.17.1
NodeRole	category ext-category? Description* Description_ML*	3.17.2
Counter	value type ext-type? unit ext-unit? meaning? meaning_ML?	

	duration? ext-duration?	3.17.3
DomainData	system-status ext-system-status? domain-status ext-domain-status? observable-id? Name DateDomainWasChecked? RegistrationDate? ExpirationDate ? RelatedDNS* Nameservers* DomainContacts?	3.18
Nameserver	Server Address*	3.18.1
DomainContacts	SameDomainContact? Contact+	3.18.2
Service	ip-protocol? observable-id? ServiceName? Port? Portlist? ProtoCode? ProtoType? ProtoField? ApplicationHeaderField+ EmailData? Application?	3.19
ServiceName	IANAService? URL* Description* Description_ML*	3.19.1
EmailData	observable-id? EmailTo* EmailFrom? EmailSubject? EmailX-Mailer? EmailHeaderField* EmailHeaders? EmailBody? EmailMessage?	

```
   |                              | HashData*         |               |
   |                              | Signature*        | 3.19.2        |
   +------------------------------+-------------------+---------------+
   | RecordData                   | restriction?      |               |
   |                              | ext-restriction?  |               |
   |                              | observable-id?    |               |
   |                              | DateTime?         |               |
   |                              | Description*      |               |
   |                              | Description_ML*   |               |
   |                              | Application?      |               |
   |                              | RecordPattern*    |               |
   |                              | RecordItem*       |               |
   |                              | URL*              |               |
   |                              | FileData*         |               |
   |                              | WindowsRegistryKeysModified*|     |
   |                              | CertificateData*  |               |
   |                              | AdditionalData*   | 3.19.3        |
   +------------------------------+-------------------+---------------+
   | RecordPattern                | type              |               |
   |                              | ext-type?         |               |
   |                              | offset?           |               |
   |                              | offsetunit?       |               |
   |                              | ext-offsetunit?   |               |
   |                              | instance?         |               |
   |                              | value             | 3.19.4        |
   +------------------------------+-------------------+---------------+
   | WindowsRegistryKeysModified  | observable-id?    | 3.20          |
   |                              | Key+              |               |
   +------------------------------+-------------------+---------------+
   | Key                          | registryaction?   |               |
   |                              | ext-registryaction?|              |
   |                              | observable-id?    |               |
   |                              | KeyName           |               |
   |                              | KeyValue?         | 3.20.1        |
   +------------------------------+-------------------+---------------+
   | CertificateData              | restriction?      |               |
   |                              | ext-restriction?  |               |
   |                              | observable-id?    |               |
   |                              | Certificate+      | 3.21          |
   +------------------------------+-------------------+---------------+
   | Certificate                  | observable-id?    |               |
   |                              | X509Data          |               |
   |                              | Description*      |               |
   |                              | Description_ML*   | 3.21.1        |
   +------------------------------+-------------------+---------------+
   | FileData                     | restriction?      |               |
   |                              | ext-restriction?  |               |
   |                              | observable-id?    |               |
```

	File+	3.22
File	observable-id?	
	FileName?	
	FileSize?	
	FileType?	
	URL*	
	HashData?	
	Signature*	
	AssociatedSoftware?	
	FileProperties*	3.22.1
HashData	scope	
	HashTargetID?	
	Hash*	
	FuzzyHash*	3.23
Hash	DigestMethod	
	DigestValue	
	CanonicalizationMethod?	
	Application?	3.23.1
FuzzyHash	FuzzyHashValue+	
	Application?	
	AdditionalData?	3.23.2
Indicator	restriction?	
	ext-restriction?	
	IndicatorID	
	AlternativeIndicatorID*	
	Description*	
	Description_ML*	
	StartTime?	
	EndTime?	
	Confidence?	
	Contact*	
	Observable?	
	uid-ref?	
	IndicatorExpression?	
	IndicatorReference?	
	NodeRole*	
	AttackPhase*	
	Reference*	
	AdditionalData*	3.24
IndicatorID	id	
	name	
	version	3.24.1

AlternativeIndicatorID	restriction? ext-restriction? IndicatorReference+	3.24.2
Observable	restriction? ext-restriction? System? Address? DomainData? Service? EmailData? WindowsRegistryKeysModified? FileData? CertificateData? RegistryHandle? RecordData? EventData? Incident? Expectation? Reference? Assessment? DetectionPattern? HistoryItem? BulkObservable? AdditionalData*	3.24.3
BulkObservable	type? ext-type? BulkObservableFormat? BulkObservableList AdditionalData*	3.24.4
BulkObservableFormat	Hash? AdditionalData*	3.24.5
IndicatorExpression	operator? ext-operator? IndicatorExpression* Observable* uid-ref* IndicatorReference* Confidence? AdditionalData*	3.24.6
IndicatorReference	uid-ref? euid-ref? version?	3.24.7

AttackPhase	AttackPhaseID* URL* Description* Description_ML* AdditionalData*	 3.24.8

3.2. Mapping between JSON and XML IODEF

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

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

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

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

- 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.

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

- 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.

- The elements of ML_STRING type are prepared as two separate elements: one of STRING type and another of ML_STRING type, in order to maintain the simplicity of IODEF documents when writing with only STRING type characters.

4. Examples

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

4.1. Minimal Example

A document containing only the mandatory elements and attributes.


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


4.2. Indicators from a Campaign

An example of C2 domains from a given campaign.


```
{
  "version": "2.0",
  "lang": "en",
  "Incidents": [
    {
      "purpose": "watch",
      "restriction": "green",
      "IncidentID": {
        "id": "897923",
        "name": "csirt.example.com"
      },
      "RelatedActivity": [
        {
          "ThreatActor": [
            {
```

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

```
              "09ijk23jfj0k8.example.net",
              "klknjwfjiowjefr923.example.org",
              "oimireik79msd.example.org"
            ]
          }
        }
      ]
    }
  ]
}
```


5. The IODEF Data Model (JSON Schema)


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

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

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

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

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

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

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

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

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

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

```
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Node": {"$ref": "#/definitions/Node"},
        "NodeRole": {
          "type": "array","items": {"$ref": "#/definitions/NodeRole"}},
        "Service": {
          "type": "array","items": {"$ref": "#/definitions/Service"}},
        "OperatingSystem": {
          "type": "array","items": {"$ref": "#/definitions/SoftwareType"}},
        "Counter": {
          "type": "array","items": {"$ref": "#/definitions/Counter"}},
        "AssetID": {"type": "array","items": {"type": "string"}},
        "Description": {"type": "array","items": {"type": "string"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["Node"],
      "additionalProperties": false},
    "Node": {
      "type": "object",
      "properties": {
        "DomainData": {
          "type": "array","items": {"$ref": "#/definitions/DomainData"}},
        "Address": {
          "type": "array","items": {"$ref": "#/definitions/Address"}},
        "PostalAddress": {"type": "string"},
        "Location": {"type": "array","items": {"type": "string"}},
        "Counter": {"type": "array","items":{"$ref":"#/definitions/Counter"}}},
      "required": [],
      "additionalProperties": false},
    "Address": {
      "type": "object",
      "properties": {
        "value": {"type": "string"},
        "category": {
           "enum": ["asn","atm","e-mail","ipv4-addr","ipv4-net",
                    "ipv4-net-masked","ipv4-net-mask","ipv6-addr","ipv6-net",
                    "ipv6-net-masked","mac","site-url","ext-value"]},
        "ext-category": {"type": "string"},
        "vlan-name": {"type": "string"},
        "vlan-num": {"type": "integer"},
        "observable-id": {"$ref": "#/definitions/IDtype"}},
      "required": ["category"],
      "additionalProperties": false},
    "NodeRole": {
      "type": "object",
      "properties": {
        "category": {
          "enum":["client","client-enterprise","clent-partner","client-remote",
                  "client-kiosk","client-mobile","server-internal",
                  "server-public","www","mail","webmail","messaging",
```

```
                  "streaming","voice","file","ftp","p2p","name","directory",
                  "credential","print","application","database","backup",
                  "dhcp","assessment","source-control","config-management",
                  "monitoring","infra","infra-firewall","infra-router",
                  "infra-switch","camera","proxy","remote-access","log",
                  "virtualization","pos", "scada", "scada-supervisory",
                  "sinkhole","honeypot","anomyzation","c2-server",
                  "malware-distribution","drop-server","hot-point","reflector",
                  "phishing-site","spear-phishing-site","recruiting-site",
                  "fraudulent-site","ext-value"]},
        "ext-category": {"type": "string"},
        "Description": {"type": "array","items": {"type": "string"}}},
      "required": ["category"],
      "additionalProperties": false},
    "Counter": {
      "type": "object",
      "properties": {
        "value": {"type": "string"},
        "type": {"enum": ["count","peak","average","ext-value"]},
        "ext-type": {"type": "string"},
        "unit": {"enum": ["byte","mbit","packet","flow","session","alert",
                 "message","event","host","site","organization","ext-value"]},
        "ext-unit": {"type": "string"},
        "meaning": {"type": "string"},
        "duration": {"$ref":"#/definitions/duration"},
        "ext-duration": {"type": "string"}},
      "required": ["type","unit"],
      "additionalProperties": false},
    "DomainData": {
      "type": "object",
      "properties": {
        "system-status": {
          "enum": ["spoofed","fraudulent","innocent-hacked",
                   "innocent-hijacked","unknown","ext-value"]},
        "ext-system-status": {"type": "string"},
        "domain-status": {
          "enum": [
            "reservedDelegation","assignedAndActive","assignedAndInactive",
            "assignedAndOnHold","revoked","transferPending","registryLock",
            "registrarLock","other","unknown","ext-value"]},
        "ext-domain-status": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Name": {"type": "string"},
        "DateDomainWasChecked": {"$ref": "#/definitions/DATETIME"},
        "RegistrationDate": {"$ref": "#/definitions/DATETIME"},
        "ExpirationDate": {"$ref": "#/definitions/DATETIME"},
        "RelatedDNS": {
          "type": "array","items": {"$ref": "#/definitions/ExtensionType"}},
```

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

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

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

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

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

```
        "ext-restriction": {"type": "string"},
        "System": {"$ref": "#/definitions/System"},
        "Address": {"$ref": "#/definitions/Address"},
        "DomainData": {"$ref": "#/definitions/DomainData"},
        "EmailData": {"$ref": "#/definitions/EmailData"},
        "Service": {"$ref": "#/definitions/Service"},
        "WindowsRegistryKeysModified": {
          "$ref": "#/definitions/WindowsRegistryKeysModified"},
        "FileData": {"$ref": "#/definitions/FileData"},
        "CertificateData": {"$ref": "#/definitions/CertificateData"},
        "RegistryHandle": {"$ref": "#/definitions/RegistryHandle"},
        "RecordData": {"type": "array", "item": {"$ref": "#/definitions/Record"}
},
        "EventData": {"$ref": "#/definitions/EventData"},
        "Incident": {"$ref": "#/definitions/Incident"},
        "Expectation": {"$ref": "#/definitions/Expectation"},
        "Reference": {"$ref": "#/definitions/Reference"},
        "Assessment": {"$ref": "#/definitions/Assessment"},
        "DetectionPattern": {"$ref": "#/definitions/DetectionPattern"},
        "HistoryItem": {"$ref": "#/definitions/HistoryItem"},
        "BulkObservable": {"$ref": "#/definitions/BulkObservable"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "BulkObservable": {
      "type": "object",
      "properties": {
        "type": {"enum": ["asn","atm","e-mail","ipv4-addr","ipv4-net",
                 "ipv4-net-mask","ipv6-addr","ipv6-net","ipv6-net-mask","mac",
                 "site-url","domain-name","domain-to-ipv4","domain-to-ipv6",
                 "domain-to-ipv4-timestamp","domain-to-ipv6-timestamp",
                 "ipv4-port","ipv6-port","windows-reg-key","file-hash",
                 "email-x-mailer","email-subject","http-user-agent",
                 "http-request-url","mutex","file-path","user-name",
                 "ext-value"]},
        "ext-type": {"type": "string"},
        "BulkObservableFormant":{"$ref": "#/definitions/BulkObservableFormat"},
        "BulkObservableList": {"type": "array", "item":{"type": "string"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "BulkObservableFormat": {
      "type": "object",
      "properties": {
        "Hash": {"$ref": "#/definitions/Hash"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "IndicatorExpression": {
```

```
      "type": "object",
      "properties": {
        "operator": {"enum": ["not","and","or","xor"]},
        "ext-operator": {"type": "string"},
        "IndicatorExpression": {
          "type": "array",
          "items": {"$ref": "#/definitions/IndicatorExpression"}},
        "Observable": {
          "type": "array","items": {"$ref": "#/definitions/Observable"}},
        "uid-ref": {"type": "string"},
        "IndicatorReference": {
          "type": "array",
         "items": {"$ref": "#/definitions/IndicatorReference"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "IndicatorReference": {
      "type": "object",
      "properties": {
        "uid-ref": {"type": "string"},
        "euid-ref": {"type": "string"},
        "version": {"type": "string"}},
      "required": [],
      "additionalProperties": false},
    "AttackPhase": {
      "type": "object",
      "properties": {
        "AttackPhaseID": {"type": "array","items": {"type": "string"}},
        "URL": {"type": "array","items": {"$ref": "#/definitions/URLtype"}},
        "Description": {"type": "array","items": {"type": "string"}},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false}},
  "title": "IODEF-Document",
  "description": "JSON schema for IODEF-Document class",
  "type": "object",
  "properties": {
    "version": {"type": "string"},
    "lang": {"$ref": "#/definitions/lang"},
    "format-id": {"type": "string"},
    "private-enum-name": {"type": "string"},
    "private-enum-id": {"type": "string"},
    "Incident": {
      "type": "array","items": {"$ref": "#/definitions/Incident"}},
      "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
  "required": ["version","Incident"],
  "additionalProperties": false}
```

Figure 2: JSON schema

6. Acknowledgements

TBD.

7. IANA Considerations

This memo includes no request to IANA.

8. Security Considerations

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

9. Normative References

[jsonschema]
"JSON Schema", 2006.

http://json-schema.org/

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

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

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 T. Takahashi
Internet-Draft NICT
Intended status: Standards Track R. Danyliw
Expires: September 2, 2020 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

Copyright Notice

Table of Contents

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 it 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	occurence? restriction? ext-restriction? observable-id? IncidentCategory* SystemImpact* BusinessImpact* TimeImpact* MonetaryImpact* IntendedImpact* Counter* MitigatingFactor* Cause* Confidence? AdditionalData*	3.12
SystemImpact	severity? completion? type ext-type? Description*	3.12.1
BusinessImpact	severity? ext-severity? type ext-type? Description*	3.12.2
TimeImpact	value severity? metric ext-metric? duration? ext-duration?	3.12.3
MonetaryImpact	value severity? currency?	3.12.4
Confidence	value rating ext-rating?	3.12.5

History	restriction? ext-restriction? HistoryItem+	3.13
HistoryItem	action ext-action? restriction? ext-restriction? observable-id? DateTime IncidentID? Contact? Description* DefinedCOA* AdditionalData*	3.13.1
EventData	restriction? ext-restriction? observable-id? Description* DetectTime? StartTime? EndTime? RecoveryTime? ReportTime? Contact* Discovery* Assessment? Method* System* Expectation* RecordData* EventData* AdditionalData*	3.14
Expectation	action? ext-action? severity? restriction? ext-restriction? observable-id? Description* DefinedCOA* StartTime? EndTime? Contact?	3.15
System	category?	

	ext-category? interface? spoofed? virtual? ownership? ext-ownership? restriction? ext-restriction? Node NodeRole* Service* OperatingSystem* Counter* AssetID* Description* AdditionalData*	3.17
Node	DomainData* Address* PostalAddress? Location* Counter*	3.18
Address	value category ext-category? vlan-name? vlan-num? observable-id?	3.18.1
NodeRole	category ext-category? Description*	3.18.2
Counter	value type ext-type? unit ext-unit? meaning? duration? ext-duration?	3.18.3
DomainData	system-status ext-system-status? domain-status ext-domain-status? observable-id?	

	Name DateDomainWasChecked? RegistrationDate? ExpirationDate? RelatedDNS* Nameservers* DomainContacts?	3.19
Nameserver	Server Address*	3.19.1
DomainContacts	SameDomainContact? Contact+	3.19.2
Service	ip-protocol? observable-id? ServiceName? Port? Portlist? ProtoCode? ProtoType? ProtoField? ApplicationHeaderField* EmailData? Application?	3.20
ServiceName	IANAService? URL* Description*	3.20.1
EmailData	observable-id? EmailTo* EmailFrom? EmailSubject? EmailX-Mailer? EmailHeaderField* EmailHeaders? EmailBody? EmailMessage? HashData* Signature*	3.21
RecordData	restriction? ext-restriction? observable-id? DateTime? Description* Application?	

	RecordPattern* RecordItem* URL* FileData* WindowsRegistryKeysModified* CertificateData* AdditionalData*	3.22.1
RecordPattern	type ext-type? offset? offsetunit? ext-offsetunit? instance? value	3.22.2
WindowsRegistryKeysModified	observable-id? 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.

- Signature, X509Data, and RawData are encoded using base64 encoding for JSON IODEF and binary representation for CBOR IODEF to represent them as BYTE object.

- 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.

- 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.

- 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.

- 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.

- 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)
                        4F72616E676520476972616666665
                                          # "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)
            53756D6D6172697A6573207468652049 6E64696361746F7273206F6620436F6D70
726F6D69736520666F7220746865204F72616E6765204769726166666520636 16D706169676E206F6
6207468652041676772657373697665204275747465726666C79206372696D652067616E672E
                                          # "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)
               43534952542066F72206578616D706C652E636F6D
                                  # "CSIRT for example.com"
         18 22                    # unsigned(34)
         81                       # array(1)
            A1                    # map(1)
               18 29              # unsigned(41)
               78 19              # text(25)
                  636F6E74616374406373697274 2E6578616D706C652E636F6D
                                  # "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 .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 "[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" /
"anomyzation" / "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], impelementers 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":["nidps","hips","siem","av","third-party-monitoring",
                  "incident","os-log","application-log","device-log",
                  "network-flow","passive-dns","investigation","audit",
                  "internal-notification","external-notification","leo",
                  "partner","actor","unknown","ext-value"]},
        "ext-source": {"type": "string"},
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "Contact": {
          "type": "array",
          "items": {"$ref": "#/definitions/Contact"},
          "minItems": 1},
        "DetectionPattern": {
          "type":"array",
          "items":{"$ref":"#/definitions/DetectionPattern"},
          "minItems": 1}},
      "required": [],
      "additionalProperties": false},
    "DetectionPattern": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Application": {"$ref": "#/definitions/SoftwareType"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "DetectionConfiguration": {
          "type": "array",
          "items": {"type": "string"},
          "minItems": 1}},
      "allOf": [
        {"required": ["Application"]},
        {"oneOf": [
          {"required":["Description"]},
          {"required":["DetectionConfiguration"]}]}]},
```

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

```
        "specIndex": {"type": "number"},
        "ID": {"$ref":"#/definitions/IDtype"}},
      "required": ["specIndex","ID"],
      "additionalProperties": false},
    "Assessment": {
      "type": "object",
      "properties": {
        "occurrence": {"enum":["actual","potential"]},
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "IncidentCategory": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "Impact": {
         "type": "array",
         "items": {
           "properties": {
             "SystemImpact":{"$ref":"#/definitions/SystemImpact"},
             "BusinessImpact":{"$ref":"#/definitions/BusinessImpact"},
             "TimeImpact":{"$ref":"#/definitions/TimeImpact"},
             "MonetaryImpact":{"$ref":"#/definitions/MonetaryImpact"},
             "IntendedImpact":{"$ref":"#/definitions/BusinessImpact"}},
           "additionalProperties":false},
         "minItems" : 1
        },
        "Counter": {
          "type": "array",
          "items": {"$ref": "#/definitions/Counter"},
          "minItems": 1},
        "MitigatingFactor": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "Cause": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "Confidence": {"$ref": "#/definitions/Confidence"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["Impact"],
      "additionalProperties": false},
    "SystemImpact": {
      "type": "object",
      "properties": {
        "severity": {"enum":["low","medium","high"]},
```

```
        "completion": {"enum":["failed","succeeded"]},
        "type": {
          "enum":["takeover-account","takeover-service",
            "takeover-system","cps-manipulation","cps-damage",
            "availability-data","availability-account",
            "availability-service","availability-system",
            "damaged-system","damaged-data","breach-proprietary",
            "breach-privacy","breach-credential",
            "breach-configuration","integrity-data",
            "integrity-configuration","integrity-hardware",
            "traffic-redirection","monitoring-traffic",
            "monitoring-host","policy","unknown","ext-value"]},
        "ext-type": {"type": "string"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1}},
      "required": ["type"],
      "additionalProperties": false},
    "BusinessImpact": {
      "type": "object",
      "properties": {
        "severity": {"enum":["none","low","medium","high","unknown",
                     "ext-value"],"default": "unknown"},
        "ext-severity": {"type":"string"},
        "type": {"enum":["breach-proprietary","breach-privacy",
          "breach-credential","loss-of-integrity","loss-of-service",
          "theft-financial","theft-service","degraded-reputation",
          "asset-damage","asset-manipulation","legal","extortion",
          "unknown","ext-value"]},
        "ext-type": {"type": "string"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1}},
      "required": ["type"],
      "additionalProperties": false},
    "TimeImpact": {
      "type": "object",
      "properties": {
        "value": {"$ref": "#/definitions/PositiveFloatType"},
        "severity": {"enum": ["low","medium","high"]},
        "metric": {"enum": ["labor","elapsed","downtime","ext-value"]},
        "ext-metric": {"type": "string"},
        "duration": {"$ref":"#/definitions/duration","default": "hour"},
        "ext-duration": {"type": "string"}},
      "required": ["value","metric"],
      "additionalProperties": false},
```

```
    "MonetaryImpact": {
      "type": "object",
      "properties": {
        "value": {"$ref": "#/definitions/PositiveFloatType"},
        "severity": {"enum":["low","medium","high"]},
        "currency": {"type": "string"}},
      "required": ["value"],
      "additionalProperties": false},
    "Confidence": {
      "type": "object",
      "properties": {
        "value": {"type": "number"},
        "rating": {"enum": ["low","medium","high","numeric","unknown",
                   "ext-value"]},
        "ext-rating": {"type":"string"}},
      "required": ["value","rating"],
      "additionalProperties": false},
    "History": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "HistoryItem": {
          "type": "array",
          "items": {"$ref": "#/definitions/HistoryItem"},
          "minItems": 1}},
      "required": ["HistoryItem"],
      "additionalProperties": false},
    "HistoryItem": {
      "type": "object",
      "properties": {
        "action": {"$ref": "#/definitions/action","default": "other"},
        "ext-action": {"type": "string"},
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "DateTime": {"$ref": "#/definitions/DATETIME"},
        "IncidentID": {"$ref": "#/definitions/IncidentID"},
        "Contact": {"$ref": "#/definitions/Contact"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "DefinedCOA": {
          "type": "array",
          "items": {"type": "string"},
```

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

```
      "required": [],
      "additionalProperties": false},
    "Expectation": {
      "type": "object",
      "properties": {
        "action": {"$ref":"#/definitions/action","default": "other"},
        "ext-action": {"type": "string"},
        "severity": {"enum": ["low","medium","high"]},
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "default"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "DefinedCOA": {
          "type": "array",
          "items": {"type": "string"},
          "minItems": 1},
        "StartTime": {"$ref": "#/definitions/DATETIME"},
        "EndTime": {"$ref": "#/definitions/DATETIME"},
        "Contact": {"$ref": "#/definitions/Contact"}},
      "required": [],
      "additionalProperties": false},
    "System": {
      "type": "object",
      "properties": {
        "category": {
          "enum": ["source","target","intermediate","sensor",
                   "infrastructure","ext-value"]},
        "ext-category": {"type": "string"},
        "interface": {"type": "string"},
        "spoofed": {"enum": ["unknown","yes","no"],"default":"unknown"},
        "virtual": {"enum": ["yes","no","unknown"],"default":"unknown"},
        "ownership": {
          "enum":["organization","personal","partner","customer",
                  "no-relationship","unknown","ext-value"]},
        "ext-ownership": {"type": "string"},
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Node": {"$ref": "#/definitions/Node"},
        "NodeRole": {
          "type": "array",
          "items": {"$ref": "#/definitions/NodeRole"},
          "minItems": 1},
```

```
        "Service": {
          "type": "array",
          "items": {"$ref": "#/definitions/Service"},
          "minItems": 1},
        "OperatingSystem": {
          "type": "array",
          "items": {"$ref": "#/definitions/SoftwareType"},
          "minItems": 1},
        "Counter": {
          "type": "array",
          "items": {"$ref": "#/definitions/Counter"},
          "minItems": 1},
        "AssetID": {
          "type": "array",
          "items": {"type": "string"},
          "minItems": 1},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["Node"],
      "additionalProperties": false},
    "Node": {
      "type": "object",
      "properties": {
        "DomainData": {
          "type": "array",
          "items": {"$ref": "#/definitions/DomainData"},
          "minItems": 1},
        "Address": {
          "type": "array",
          "items": {"$ref": "#/definitions/Address"},
          "minItems": 1},
        "PostalAddress": {"$ref": "#/definitions/PostalAddress"},
        "Location": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "Counter": {
          "type":"array",
          "items":{"$ref":"#/definitions/Counter"},
          "minItems": 1}},
      "anyOf": [
         {"required": ["DomainData"]},
         {"required": ["Address"]}
      ],
      "additionalProperties": false},
```

```
    "Address": {
      "type": "object",
      "properties": {
        "value": {"type": "string"},
        "category": {
          "enum":["asn","atm","e-mail","ipv4-addr","ipv4-net",
            "ipv4-net-masked","ipv4-net-mask","ipv6-addr","ipv6-net",
            "ipv6-net-masked","mac","site-uri","ext-value"],
            "default": "ipv6-addr"},
        "ext-category": {"type": "string"},
        "vlan-name": {"type": "string"},
        "vlan-num": {"type": "number"},
        "observable-id": {"$ref": "#/definitions/IDtype"}},
      "required": ["value","category"],
      "additionalProperties": false},
    "NodeRole": {
      "type": "object",
      "properties": {
        "category": {
          "enum":["client","client-enterprise","client-partner",
            "client-remote","client-kiosk","client-mobile",
            "server-internal","server-public","www","mail","webmail",
            "messaging","streaming","voice","file","ftp","p2p","name",
            "directory","credential","print","application","database",
            "backup","dhcp","assessment","source-control",
            "config-management","monitoring","infra","infra-firewall",
            "infra-router","infra-switch","camera","proxy",
            "remote-access","log","virtualization","pos", "scada",
            "scada-supervisory","sinkhole","honeypot","anomyzation",
            "c2-server","malware-distribution","drop-server",
            "hop-point","reflector","phishing-site",
            "spear-phishing-site","recruiting-site","fraudulent-site",
            "ext-value"]},
        "ext-category": {"type": "string"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1}},
      "required": ["category"],
      "additionalProperties": false},
    "Counter": {
      "type": "object",
      "properties": {
        "value": {"type": "number"},
        "type": {"enum": ["count","peak","average","ext-value"]},
        "ext-type": {"type": "string"},
        "unit":{"enum":["byte","mbit","packet","flow","session","alert",
          "message","event","host","site","organization","ext-value"]},
```

```
        "ext-unit": {"type": "string"},
        "meaning": {"type": "string"},
        "duration": {"$ref":"#/definitions/duration","default": "hour"},
        "ext-duration": {"type": "string"}},
      "required": ["value","type","unit"],
      "additionalProperties": false},
    "DomainData": {
      "type": "object",
      "properties": {
        "system-status": {
          "enum": ["spoofed","fraudulent","innocent-hacked",
                   "innocent-hijacked","unknown","ext-value"]},
        "ext-system-status": {"type": "string"},
        "domain-status": {
          "enum": [ "reservedDelegation","assignedAndActive",
                    "assignedAndInactive","assignedAndOnHold","revoked",
                    "transferPending","registryLock","registrarLock",
                    "other","unknown","ext-value"]},
        "ext-domain-status": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Name": {"type": "string"},
        "DateDomainWasChecked": {"$ref": "#/definitions/DATETIME"},
        "RegistrationDate": {"$ref": "#/definitions/DATETIME"},
        "ExpirationDate": {"$ref": "#/definitions/DATETIME"},
        "RelatedDNS": {
          "type": "array",
          "items": {"$ref": "#/definitions/ExtensionType"},
          "minItems": 1},
        "NameServers": {
          "type": "array",
          "items": {"$ref": "#/definitions/NameServers"},
          "minItems": 1},
        "DomainContacts": {"$ref": "#/definitions/DomainContacts"}},
      "required": ["Name","system-status","domain-status"],
      "additionalProperties": false},
    "NameServers": {
      "type": "object",
      "properties": {
        "Server": {"type": "string"},
        "Address": {
          "type":"array",
          "items":{"$ref":"#/definitions/Address"},
          "minItems": 1}},
      "required": ["Server","Address"],
      "additionalProperties": false},
    "DomainContacts": {
      "type": "object",
      "properties": {
```

```
        "SameDomainContact": {"type": "string"},
        "Contact": {
          "type":"array",
          "items":{"$ref":"#/definitions/Contact"},
          "minItems": 1}},
      "oneOf": [
         {"required": ["SameDomainContact"]},
         {"required": ["Contact"]}],
      "additionalProperties": false},
    "Service": {
      "type": "object",
      "properties": {
        "ip-protocol": {"type": "number"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "ServiceName": {"$ref": "#/definitions/ServiceName"},
        "Port": {"type": "number"},
        "Portlist": {"$ref": "#/definitions/PortlistType"},
        "ProtoCode": {"type": "number"},
        "ProtoType": {"type": "number"},
        "ProtoField": {"type": "number"},
        "ApplicationHeaderField":{
          "$ref":"#/definitions/ExtensionTypeList"},
        "EmailData": {"$ref": "#/definitions/EmailData"},
        "Application": {"$ref": "#/definitions/SoftwareType"}},
      "required": [],
      "additionalProperties": false},
    "ServiceName": {
      "type": "object",
      "properties": {
        "IANAService": {"type": "string"},
        "URL": {
          "type": "array","items": {"$ref": "#/definitions/URLtype"}},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1}},
      "required": [],
      "additionalProperties": false},
    "EmailData": {
      "type": "object",
      "properties": {
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "EmailTo": {
          "type": "array",
          "items": {"type": "string"},
          "minItems": 1},
        "EmailFrom": {"type": "string"},
        "EmailSubject": {"type": "string"},
```

```
        "EmailX-Mailer": {"type": "string"},
        "EmailHeaderField": {
          "type": "array",
          "items": {"$ref": "#/definitions/ExtensionType"},
          "minItems": 1},
        "EmailHeaders": {"type": "string"},
        "EmailBody": {"type": "string"},
        "EmailMessage": {"type": "string"},
        "HashData": {
          "type": "array",
          "items": {"$ref": "#/definitions/HashData"},
          "minItems": 1},
        "Signature": {
          "type": "array",
          "items": {"$ref": "#/definitions/BYTE"},
          "minItems": 1}},
      "required": [],
      "additionalProperties": false},
    "RecordData": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "DateTime": {"$ref": "#/definitions/DATETIME"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "Application": {"$ref": "#/definitions/SoftwareType"},
        "RecordPattern": {
          "type": "array",
          "items": {"$ref": "#/definitions/RecordPattern"},
          "minItems": 1},
        "RecordItem": {
          "type": "array",
          "items": {"$ref": "#/definitions/ExtensionType"},
          "minItems": 1},
        "URL": {
          "type": "array",
          "items": {"$ref": "#/definitions/URLtype"},
          "minItems": 1},
        "FileData": {
          "type": "array",
          "items": {"$ref": "#/definitions/FileData"},
          "minItems": 1},
        "WindowsRegistryKeysModified": {
```

```
          "type": "array",
          "items": {"$ref":"#/definitions/WindowsRegistryKeysModified"},
          "minItems": 1},
        "CertificateData": {
          "type":"array",
          "items":{"$ref":"#/definitions/CertificateData"},
          "minItems": 1},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "RecordPattern": {
      "type": "object",
      "properties": {
        "value": {"type": "string"},
        "type": {"enum": ["regex","binary","xpath","ext-value"],
                 "default": "regex"},
        "ext-type": {"type": "string"},
        "offset": {"type": "number"},
        "offsetunit": {"enum":["line","byte","ext-value"] ,
                       "default": "line"},
        "ext-offsetunit": {"type": "string"},
        "instance": {"type": "number"}},
      "required": ["value","type"],
      "additionalProperties": false},
    "WindowsRegistryKeysModified": {
      "type": "object",
      "properties": {
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Key": {
          "type": "array",
          "items": {"$ref": "#/definitions/Key"},
          "minItems": 1}},
      "required": ["Key"],
      "additionalProperties": false},
    "Key": {
      "type": "object",
      "properties": {
        "registryaction": {"enum": ["add-key","add-value","delete-key",
                           "delete-value","modify-key","modify-value",
                           "ext-value"]},
        "ext-registryaction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "KeyName": {"type":"string"},
        "KeyValue": {"type": "string"}},
      "required": ["KeyName"],
      "additionalProperties": false},
    "CertificateData": {
      "type": "object",
```

```
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "Certificate": {
          "type": "array",
          "items": {"$ref": "#/definitions/Certificate"},
          "minItems": 1}},
      "required": ["Certificate"],
      "additionalProperties": false},
    "Certificate": {
      "type": "object",
      "properties": {
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "X509Data": {"$ref": "#/definitions/BYTE"},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1}},
      "required": ["X509Data"],
      "additionalProperties": false},
    "FileData": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction"},
        "ext-restriction": {"type": "string"},
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "File": {
          "type": "array",
          "items": {"$ref": "#/definitions/File"},
          "minItems": 1}},
      "required": ["File"],
      "additionalProperties": false},
    "File": {
      "type": "object",
      "properties": {
        "observable-id": {"$ref": "#/definitions/IDtype"},
        "FileName": {"type": "string"},
        "FileSize": {"type": "number"},
        "FileType": {"type": "string"},
        "URL": {
          "type": "array",
          "items": {"$ref": "#/definitions/URLtype"},
          "minItems": 1},
        "HashData": {"$ref": "#/definitions/HashData"},
        "Signature": {
          "type": "array",
```

```
          "items": {"$ref": "#/definitions/BYTE"},
          "minItems": 1},
        "AssociatedSoftware": {"$ref": "#/definitions/SoftwareType"},
        "FileProperties": {
          "type":"array",
          "items":{"$ref":"#/definitions/ExtensionType"},
          "minItems": 1}},
      "required": [],
      "additionalProperties": false},
    "HashData": {
      "type": "object",
      "properties": {
        "scope": {"enum": ["file-contents","file-pe-section",
          "file-pe-iat","file-pe-resource","file-pdf-object",
          "email-hash","email-headers-hash","email-body-hash",
          "ext-value"]},
        "HashTargetID": {"type": "string"},
        "Hash": {
          "type": "array",
          "items": {"$ref": "#/definitions/Hash"},
          "minItems": 1},
        "FuzzyHash": {
          "type": "array",
          "items": {"$ref": "#/definitions/FuzzyHash"},
          "minItems": 1}},
      "required": ["scope"],
      "additionalProperties": false},
    "Hash": {
      "type": "object",
      "properties": {
        "DigestMethod": {"$ref": "#/definitions/BYTE"},
        "DigestValue": {"$ref": "#/definitions/BYTE"},
        "CanonicalizationMethod": {"$ref": "#/definitions/BYTE"},
        "Application": {"$ref": "#/definitions/SoftwareType"}},
      "required": ["DigestMethod","DigestValue"],
      "additionalProperties": false},
    "FuzzyHash": {
      "type": "object",
      "properties": {
        "FuzzyHashValue": {
          "type": "array",
          "items": {"$ref": "#/definitions/ExtensionType"},
          "minItems": 1},
        "Application": {"$ref": "#/definitions/SoftwareType"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["FuzzyHashValue"],
      "additionalProperties": false},
    "Indicator": {
```

```
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "IndicatorID": {"$ref": "#/definitions/IndicatorID"},
        "AlternativeIndicatorID": {
          "type": "array",
          "items": {"$ref": "#/definitions/AlternativeIndicatorID"},
          "minItems": 1},
        "Description": {
          "type": "array",
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "StartTime": {"$ref": "#/definitions/DATETIME"},
        "EndTime": {"$ref": "#/definitions/DATETIME"},
        "Confidence": {"$ref": "#/definitions/Confidence"},
        "Contact": {
          "type": "array",
          "items": {"$ref": "#/definitions/Contact"},
          "minItems": 1},
        "Observable": {"$ref": "#/definitions/Observable"},
        "uid-ref": {"$ref": "#/definitions/IDREFType"},
        "IndicatorExpression":{
         "$ref":"#/definitions/IndicatorExpression"},
        "IndicatorReference":{
         "$ref": "#/definitions/IndicatorReference"},
        "NodeRole": {
          "type": "array",
          "items": {"$ref": "#/definitions/NodeRole"},
          "minItems": 1},
        "AttackPhase": {
          "type": "array",
          "items": {"$ref": "#/definitions/AttackPhase"},
          "minItems": 1},
        "Reference": {
          "type": "array",
          "items": {"$ref": "#/definitions/Reference"},
          "minItems": 1},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "allOf": [
        {"required": ["IndicatorID"]},
        {"oneOf": [
          {"required":["Observable"]},
          {"required":["uid-ref"]},
          {"required":["IndicatorExpression"]},
          {"required":["IndicatorReference"]}]}],
      "additionalProperties": false},
```

```
    "IndicatorID": {
      "type": "object",
      "properties": {
        "id": {"type": "string"},
        "name": {"type": "string"},
        "version": {"type": "string"}},
      "required": ["id","name","version"],
      "additionalProperties": false},
    "AlternativeIndicatorID": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
          "default": "private"},
        "ext-restriction": {"type": "string"},
        "IndicatorID": {
          "type": "array",
          "items": {"$ref": "#/definitions/IndicatorID"},
          "minItems": 1}},
      "required": ["IndicatorID"],
      "additionalProperties": false},
    "Observable": {
      "type": "object",
      "properties": {
        "restriction": {"$ref": "#/definitions/restriction",
                        "default": "private"},
        "ext-restriction": {"type": "string"},
        "System": {"$ref": "#/definitions/System"},
        "Address": {"$ref": "#/definitions/Address"},
        "DomainData": {"$ref": "#/definitions/DomainData"},
        "EmailData": {"$ref": "#/definitions/EmailData"},
        "Service": {"$ref": "#/definitions/Service"},
        "WindowsRegistryKeysModified": {
          "$ref": "#/definitions/WindowsRegistryKeysModified"},
        "FileData": {"$ref": "#/definitions/FileData"},
        "CertificateData": {"$ref": "#/definitions/CertificateData"},
        "RegistryHandle": {"$ref": "#/definitions/RegistryHandle"},
        "RecordData":  {"$ref": "#/definitions/RecordData"},
        "EventData": {"$ref": "#/definitions/EventData"},
        "Incident": {"$ref": "#/definitions/Incident"},
        "Expectation": {"$ref": "#/definitions/Expectation"},
        "Reference": {"$ref": "#/definitions/Reference"},
        "Assessment": {"$ref": "#/definitions/Assessment"},
        "DetectionPattern": {"$ref": "#/definitions/DetectionPattern"},
        "HistoryItem": {"$ref": "#/definitions/HistoryItem"},
        "BulkObservable": {"$ref": "#/definitions/BulkObservable"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
        "oneOf": [
          {"required":["System"]},
```

```
          {"required":["Address"]},
          {"required":["DomainData"]},
          {"required":["EmailData"]},
          {"required":["Service"]},
          {"required":["WindowsRegistryKeysModified"]},
          {"required":["FileData"]},
          {"required":["CertificateData"]},
          {"required":["RegistryHandle"]},
          {"required":["RecordData"]},
          {"required":["EventData"]},
          {"required":["Incident"]},
          {"required":["Expectation"]},
          {"required":["Reference"]},
          {"required":["Assessment"]},
          {"required":["DetectionPattern"]},
          {"required":["HistoryItem"]},
          {"required":["BulkObservable"]},
          {"required":["AdditionalData"]}],
      "additionalProperties": false},
    "BulkObservable": {
      "type": "object",
      "properties": {
        "type": {"enum": ["asn","atm","e-mail","ipv4-addr","ipv4-net",
          "ipv4-net-mask","ipv6-addr","ipv6-net","ipv6-net-mask",
          "mac","site-uri","domain-name","domain-to-ipv4",
          "domain-to-ipv6","domain-to-ipv4-timestamp",
          "domain-to-ipv6-timestamp","ipv4-port","ipv6-port",
          "windows-reg-key","file-hash","email-x-mailer",
          "email-subject","http-user-agent","http-request-url",
          "mutex","file-path","user-name","ext-value"]},
        "ext-type": {"type": "string"},
        "BulkObservableFormat":{
          "$ref": "#/definitions/BulkObservableFormat"},
        "BulkObservableList": {"type": "string"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": ["BulkObservableList"],
      "additionalProperties": false},
    "BulkObservableFormat": {
      "type": "object",
      "properties": {
        "Hash": {"$ref": "#/definitions/Hash"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "oneOf": [
         {"required": ["Hash"]},
         {"required": ["AdditionalData"]}
      ],
      "additionalProperties": false},
    "IndicatorExpression": {
```

```
      "type": "object",
      "properties": {
        "operator": {"enum": ["not","and","or","xor"],"default": "and"},
        "ext-operator": {"type": "string"},
        "IndicatorExpression": {
          "type": "array",
          "items": {"$ref": "#/definitions/IndicatorExpression"},
          "minItems": 1},
        "Observable": {
          "type": "array",
          "items": {"$ref": "#/definitions/Observable"},
          "minItems": 1},
        "uid-ref": {
          "type": "array",
          "items": {"$ref": "#/definitions/IDREFType"},
          "minItems": 1},
        "IndicatorReference": {
          "type": "array",
          "items": {"$ref": "#/definitions/IndicatorReference"},
          "minItems": 1},
        "Confidence": {"$ref":"#/definitions/Confidence"},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false},
    "IndicatorReference": {
      "type": "object",
      "properties": {
        "uid-ref": {"$ref":"#/definitions/IDREFType"},
        "euid-ref": {"type": "string"},
        "version": {"type": "string"}},
      "oneOf": [
         {"required": ["uid-ref"]},
         {"required": ["euid-ref"]}
      ],
      "additionalProperties": false},
    "AttackPhase": {
      "type": "object",
      "properties": {
        "AttackPhaseID": {
          "type": "array",
          "items": {"type": "string"},
          "minItems": 1},
        "URL": {
          "type": "array",
          "items": {"$ref": "#/definitions/URLtype"},
          "minItems": 1},
        "Description": {
          "type": "array",
```

```
          "items": {"$ref": "#/definitions/MLStringType"},
          "minItems": 1},
        "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
      "required": [],
      "additionalProperties": false}},
  "title": "IODEF-Document",
  "description": "JSON schema for IODEF-Document class",
  "type": "object",
  "properties": {
    "version": {"type": "string"},
    "lang": {"$ref": "#/definitions/lang"},
    "format-id": {"type": "string"},
    "private-enum-name": {"type": "string"},
    "private-enum-id": {"type": "string"},
    "Incident": {
      "type": "array",
      "items": {"$ref": "#/definitions/Incident"},
      "minItems": 1},
    "AdditionalData": {"$ref":"#/definitions/ExtensionTypeList"}},
  "required": ["version","Incident"],
  "additionalProperties": false}
```

Figure 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 N. Cam-Winget, Ed.
Internet-Draft S. Appala
Intended status: Standards Track S. Pope
Expires: August 12, 2018 Cisco Systems
P. Saint-Andre
Mozilla
February 8, 2018

Using XMPP for Security Information Exchange
draft-ietf-mile-xmpp-grid-05

Abstract

This document describes how to use the Extensible Messaging and Presence Protocol (XMPP) to collect and distribute security-relevant information between network-connected devices. To illustrate the principles involved, this document describes such a usage for the Incident Object Description Exchange Format (IODEF).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document describes "XMPP-Grid": a method for using the Extensible Messaging and Presence Protocol (XMPP) [RFC6120] to collect and distribute security-relevant information among network platforms, endpoints, and any other network-connected device. Among other things, XMPP provides a publish-subscribe service [XEP-0060] that acts as a broker, enabling control-plane functions by which entities can discover available information to be published or consumed. Although such information can take the form of any structured data (XML, JSON, etc.), this document illustrates the principles of XMPP-Grid with examples that use the Incident Object Description Exchange Format (IODEF) [RFC7970].

2. Terminology

This document uses XMPP terminology defined in [RFC6120] and [XEP-0060] as well as Security Automation and Continuous Monitoring (SACM) terminology defined in [I-D.ietf-sacm-terminology]. Because the intended audience for this document is those who implement and deploy security reporting systems, in general the SACM terms are used (however, mappings are provided for the benefit of XMPP developers and operators).

Broker: In SACM, a specific type of controller containing control plane functions; as used here, the term refers to an XMPP publish-subscribe service.

Broker Flow: In SACM, a method by which security-related information is published and consumed in a mediated fashion through a Broker. In this flow, the Broker handles authorization of Consumers and Providers to Topics, receives messages from Providers, and delivers published messages to Consumers.

Consumer: In SACM, an entity that contains functions to receive information from other components; as used here, the term refers to an XMPP publish-subscribe Subscriber.

Controller: In SACM, a "component containing control plane functions that manage and facilitate information sharing or execute on security functions"; as used here, the term refers to an XMPP server, which provides core message delivery [RFC6120] used by publish-subscribe entities.

Node: The XMPP term for a Topic.

Platform: Any entity that connects to the XMPP-Grid in order to publish or consume security-related data.

Provider: In SACM, an entity that contains functions to provide information to other components; as used here, the term refers to an XMPP publish-subscribe Publisher.

Publisher: The XMPP term for a Provider.

Publish-Subscribe Service: The XMPP term for the kind Broker discussed here.

Subscriber: The XMPP term for a Consumer.

Topic: A contextual information channel created on a Broker at which messages generated by a Provider are propagated in real time to one or more Consumers. Each Topic is limited to a specific type and format of security data (e.g., IODEF) and provides an XMPP interface by which the data can be obtained.

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. Architecture

The following figure illustrates the architecture of XMPP-Grid.

```
             +--------------------------------------+
             | +--------------------------------------+
             | | +--------------------------------------+
             | | |                                      |
             +-| |             Platforms                |
               +-|                                      |
                 +--------------------------------------+
                   /   \         /   \            /   \
                  /  C  \       /     \          /     \
                  -  o  -       -  d  -          -     -
                   ||n||A        | a  |B          |   |C
                   ||t||         | t  |           |   |
                  -  r  -       -  a  -           |   |
                  \  o  /       \     /           |   |
                   \ l /         \   /            |   |
                /|---------------------|\         |   |
         /|----/                         \--------| d |--|\
        /     /        Controller         \ ctrl  | a |    \
        \     \        & Broker           / plane | t |    /
         \|----\                         /--------| a |--|/
                \|---------------------|/         |   |
                   /   \         /   \            |   |
                  /  C  \       /     \           |   |
                  -  o  -       -  d  -           |   |
                   ||n||A        | a |B           |   |C
                   ||t||         | t |            |   |
                  -  r  -       -  a  -          -     -
                  \  o  /       \     /          \     /
                   \ l /         \   /            \   /
                 +------------------------------------+
                 |                                    |-+
                 |            Platforms               | |
                 |                                    | |-+
                 +------------------------------------+ | |
                   +------------------------------------+ |
                     +------------------------------------+
```

Figure 1: XMPP-Grid Architecture

Platforms connect to the Controller (XMPP server) to authenticate and then establish appropriate authorizations and relationships (e.g., Provider or Consumer) at the Broker. The control plane messaging is established through XMPP and shown as "A" (control plane interface) in Figure 1. Authorized nodes can then share data either thru the

Broker (shown as "B" in Figure 1) or in some cases directly (shown as "C" in Figure 1). This document focuses primarily on the Broker Flow for information sharing ("direct flow" interactions can be used for specialized purposes such as bulk data transfer, but methods for doing so are outside the scope of this document).

4. Workflow

A typical XMPP-Grid workflow is as follows:

a. A Platform with a source of security data requests connection to the XMPP-Grid via a Controller (XMPP server).

b. The Controller authenticates the Platform.

c. The Platform establishes authorized privileges (e.g. privilege to publish and/or subscribe to security data Topics) with a Broker.

d. The Platform can publish security-related data to a Topic, subscribe to a Topic, query a Topic, or any combination of these operations.

e. A Provider unicasts its Topic updates to the Grid in real time through a Broker. The Broker handles replication and distribution of the Topic to Consumers. A Provider can publish the same or different data to multiple Topics.

f. Any Platform on the Grid can subscribe to any Topics published to the Grid (as permitted by authorization policy), and as Consumers will then receive a continual, real-time stream of updates from the Topics to which it is subscribed.

The general workflow is summarized in the figure below:

```
   +--------------+         +------------+          +---------------+
   | IODEF Client |         | Controller |          | IODEF Service |
   |  (Consumer)  |         |  & Broker  |          |  (Provider)   |
   +--------------+         +------------+          +---------------+
           |                      |                         |
           |  Establish XMPP      |                         |
           |  Client Session      |                         |
           |  (RFC 6120)          |                         |
           |--------------------->|                         |
           |                      | Establish XMPP          |
           |                      | Client Session          |
           |                      | (RFC 6120)              |
           |                      |<------------------------|
           |                      | Request Topic Creation  |
           |                      | (XEP-0060)              |
           |                      |<------------------------|
           |                      | Topic Creation Success  |
           |                      | (XEP-0060)              |
           |                      |------------------------>|
           | Request Topic List   |                         |
           | (XEP-0030)           |                         |
           |--------------------->|                         |
           | Return Topic List    |                         |
           | (XEP-0030)           |                         |
           |<---------------------|                         |
           |                      |                         |
           | Query Each Topic     |                         |
           | (XEP-0030)           |                         |
           |--------------------->|                         |
           | Return Topic Data    |                         |
           | Including Topic Type |                         |
           | (XEP-0030)           |                         |
           |<---------------------|                         |
           |                      |                         |
           | Subscribe to IODEF   |                         |
           | Topic (XEP-0060)     |                         |
           |--------------------->|                         |
           | Subscription Success |                         |
           | (XEP-0060)           |                         |
           |<---------------------|                         |
           |                      | Publish IODEF Incident  |
           |                      | (XEP-0060)              |
           | Receive IODEF        |<------------------------|
           | Incident (XEP-0060)  |                         |
           |<---------------------|                         |
           |                      |                         |
```

Figure 2: IODEF Example Workflow

The following sections provide protocol examples for the service discovery and publish-subscribe parts of the workflow.

5. Service Discovery

Using the XMPP service discovery extension [XEP-0030], a Controller enables Platforms to discover what information can be consumed through the Broker, and at which Topics. As an example, the Controller at 'security-grid.example' might provide a Broker at 'broker.security-grid.example' hosting a number of Topics. A Platform at 'xmpp-grid-client@mile-host.example' would query the Broker about its available Topics by sending an XMPP "disco#items" request to the Broker:

```
<iq type='get'
    from='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    to='broker.security-grid.example'
    id='B3C17F7B-B9EF-4ABA-B08D-805DA9F34626'>
  <query xmlns='http://jabber.org/protocol/disco#items'/>
</iq>
```

The Broker responds with the Topics it hosts:

```
<iq type='result'
    from='broker.security-grid.example'
    to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    id='B3C17F7B-B9EF-4ABA-B08D-805DA9F34626'>
  <query xmlns='http://jabber.org/protocol/disco#items'>
    <item node='NEA1'
          name='Endpoint Posture Information'
          jid='broker.security-grid.example'/>
    <item node='MILEHost'
          name='MILE Host Data'
          jid='broker.security-grid.example'/>
  </query>
</iq>
```

In order to determine the exact nature of each Topic (i.e., in order to find topics that publish incidents in the IODEF format), a Platform would send an XMPP "disco#info" request to each Topic:

```
<iq type='get'
    from='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    to='broker.security-grid.example'
    id='D367D4ED-2795-489C-A83E-EAAFA07A0356'
  <query xmlns='http://jabber.org/protocol/disco#info'
         node='MILEHost'/>
</iq>
```

The Broker responds with the "disco#info" description, which SHOULD include an XMPP Data Form [XEP-0004] including a 'pubsub#type' field that specifies the supported namespace (in this example, the IODEF namespace defined in [RFC7970]):

```
<iq type='result'
    from='broker.security-grid.example'
    to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    id='D367D4ED-2795-489C-A83E-EAAFA07A0356'/>
  <query xmlns='http://jabber.org/protocol/disco#info'
         node='MILEHost'>
    <identity category='pubsub' type='leaf'/>
    <feature var='http://jabber.org/protocol/pubsub'/>
    <x xmlns='jabber:x:data' type='result'>
      <field var='FORM_TYPE' type='hidden'>
        <value>http://jabber.org/protocol/pubsub#meta-data</value>
      </field>
      <field var='pubsub#type' label='Payload type' type='text-single'>
        <value>urn:ietf:params:xml:ns:iodef-2.0</value>
      </field>
    </x>
  </query>
</iq>
```

6. Publish-Subscribe

Using the XMPP publish-subscribe extension [XEP-0030], a Consumer subscribes to a Topic and a Provider publishes information to that Topic, which the Broker then distributes to all subscribed Consumers.

First, a Provider would create a Topic as follows:

```
<iq type='set'
    from='datasource@provider.example/F12C2EFC9BB0'
    to='broker.security-grid.example'
    id='A67507DF-2F22-4937-8D30-88D2F7DBA279'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <create node='MILEHost'/>
  </pubsub>
</iq>
```

Note: The foregoing example is the minimal protocol needed to create a Topic with the default node configuration on the XMPP publish-subscribe service specified in the 'to' address of the creation request stanza. Depending on security requirements, the Provider might need to request a non-default configuration for the node; see [XEP-0060] for detailed examples.

Unless an error occurs (see [XEP-0060] for various error flows), the Broker responds with success:

```
<iq type='result'
    from='broker.security-grid.example'
    to='datasource@provider.example/F12C2EFC9BB0'
    id='A67507DF-2F22-4937-8D30-88D2F7DBA279'/>
```

Second, a Consumer would subscribe as follows:

```
<iq type='set'
    from='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    to='broker.security-grid.example'
    id='9C6EEE9E-F09A-4418-8D68-3BA6AF852522'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <subscribe node='MILEHost'
               jid='xmpp-grid-client@mile-host.example'/>
  </pubsub>
</iq>
```

Unless an error occurs (see [XEP-0060] for various error flows), the Broker responds with success:

```
<iq type='result'
    from='broker.security-grid.example'
    to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    id='9C6EEE9E-F09A-4418-8D68-3BA6AF852522'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <subscription
        node='MILEHost'
        jid='xmpp-grid-client@mile-host.example'
        subscription='subscribed'/>
  </pubsub>
</iq>
```

Third, a Provider would publish an incident as follows:

```
<iq type='set'
    from='datasource@provider.example/F12C2EFC9BB0'
    to='broker.security-grid.example'
    id='2A17D283-0DAE-4A6C-85A9-C10B1B40928C'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <publish node='MILEHost'>
      <item id='8bh1g27skbga47fh9wk7'>
        <IODEF-Document version="2.00" xml:lang="en"
          xmlns="urn:ietf:params:xml:ns:iodef-2.0"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation=
            "http://www.iana.org/assignments/xml-registry/
             schema/iodef-2.0.xsd">
          <Incident purpose="reporting" restriction="private">
            <IncidentID name="csirt.example.com">492382</IncidentID>
            <GenerationTime>2015-07-18T09:00:00-05:00</GenerationTime>
            <Contact type="organization" role="creator">
              <Email>
                <EmailTo>contact@csirt.example.com</EmailTo>
              </Email>
            </Contact>
          </Incident>
        </IODEF-Document>
      </item>
    </publish>
  </pubsub>
</iq>
```

(The payload in the foregoing example is from [RFC7970]; payloads for additional use cases can be found in [RFC8274].)

The Broker would then deliver that incident report to all Consumers who are subscribe to the Topic:

```
<message
    from='broker.security-grid.example'
    to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    id='37B3921D-4F7F-450F-A589-56119A88BC2E'>
  <event xmlns='http://jabber.org/protocol/pubsub#event'>
    <items node='MILEHost'>
      <item id='iah37s61s964gquqy47aksbx9453ks77'>
        <IODEF-Document version="2.00" xml:lang="en"
          xmlns="urn:ietf:params:xml:ns:iodef-2.0"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation=
            "http://www.iana.org/assignments/xml-registry/
             schema/iodef-2.0.xsd">
          <Incident purpose="reporting" restriction="private">
            <IncidentID name="csirt.example.com">492382</IncidentID>
            <GenerationTime>2015-07-18T09:00:00-05:00</GenerationTime>
            <Contact type="organization" role="creator">
              <Email>
                <EmailTo>contact@csirt.example.com</EmailTo>
              </Email>
            </Contact>
          </Incident>
        </IODEF-Document>
      </item>
    </items>
  </event>
</message>
```


7. IANA Considerations

This document has no actions for IANA.

8. Security Considerations

An XMPP-Grid Controller serves as an controlling broker for XMPP-Grid Platforms such as Enforcement Points, Policy Servers, CMDBs, and Sensors, using a publish-subscribe-search model of information exchange and lookup. By increasing the ability of XMPP-Grid Platforms to learn about and respond to security-relevant events and data, XMPP-Grid can improve the timeliness and utility of the security system. However, this integrated security system can also be exploited by attackers if they can compromise it. Therefore, strong security protections for XMPP-Grid are essential.

This section provides a security analysis of the XMPP-Grid data transfer protocol and the architectural elements that employ it, specifically with respect to their use of this protocol. Three subsections define the trust model (which elements are trusted to do what), the threat model (attacks that can be mounted on the system), and the countermeasures (ways to address or mitigate the threats previously identified).

8.1. Trust Model

The first step in analyzing the security of the XMPP-Grid transport protocol is to describe the trust model, listing what each architectural element is trusted to do. The items listed here are assumptions, but provisions are made in the Threat Model and Countermeasures sections for elements that fail to perform as they were trusted to do.

8.1.1. Network

The network used to carry XMPP-Grid messages (i.e., the underlying network transport layer over which XMPP runs) is trusted to:

- o Perform best effort delivery of network traffic

The network used to carry XMPP-Grid messages is not expected (trusted) to:

- o Provide confidentiality or integrity protection for messages sent over it

- o Provide timely or reliable service

8.1.2. XMPP-Grid Platforms

Authorized XMPP-Grid Platforms are trusted to:

- o Preserve the confidentiality of sensitive data retrieved via the XMPP-Grid Controller

8.1.3. XMPP-Grid Controller

The XMPP-Grid Controller (including its associated Broker) is trusted to:

- o Broker requests for data and enforce authorization of access to this data throughout its lifecycle

- o Perform service requests in a timely and accurate manner

- o Create and maintain accurate operational attributes

- o Only reveal data to and accept service requests from authorized parties

The XMPP-Grid Controller is not expected (trusted) to:

- o Verify the truth (correctness) of data

8.1.4. Certification Authority

The Certification Authority (CA) that issues certificates for the XMPP-Grid Controller and/or XMPP-Grid Platforms (or each CA, if there are several) is trusted to:

- o Ensure that only proper certificates are issued and that all certificates are issued in accordance with the CA's policies

- o Revoke certificates previously issued when necessary

- o Regularly and securely distribute certificate revocation information

- o Promptly detect and report any violations of this trust so that they can be handled

The CA is not expected (trusted) to:

- o Issue certificates that go beyond the XMPP-Grid needs or other constraints imposed by a relying party.

8.2. Threat Model

To secure the XMPP-Grid data transfer protocol and the architectural elements that implement it, this section identifies the attacks that can be mounted against the protocol and elements.

8.2.1. Network Attacks

A variety of attacks can be mounted using the network. For the purposes of this subsection the phrase "network traffic" can be taken to mean messages and/or parts of messages. Any of these attacks can be mounted by network elements, by parties who control network elements, and (in many cases) by parties who control network-attached devices.

- o Network traffic can be passively monitored to glean information from any unencrypted traffic

- Even if all traffic is encrypted, valuable information can be gained by traffic analysis (volume, timing, source and destination addresses, etc.)

- Network traffic can be modified in transit

- Previously transmitted network traffic can be replayed

- New network traffic can be added

- Network traffic can be blocked, perhaps selectively

- A "Man In The Middle" (MITM) attack can be mounted where an attacker interposes itself between two communicating parties and poses as the other end to either party or impersonates the other end to either or both parties

- Resist attacks (including denial of service and other attacks from XMPP-Grid Platforms)

- Undesired network traffic can be sent in an effort to overload an architectural component, thus mounting a denial of service attack

8.2.2. XMPP-Grid Platforms

An unauthorized XMPP-Grid Platform (one which is not recognized by the XMPP-Grid Controller or is recognized but not authorized to perform any actions) cannot mount any attacks other than those listed in the Network Attacks section above.

An authorized XMPP-Grid Platform, on the other hand, can mount many attacks. These attacks might occur because the XMPP-Grid Platform is controlled by a malicious, careless, or incompetent party (whether because its owner is malicious, careless, or incompetent or because the XMPP-Grid Platform has been compromised and is now controlled by a party other than its owner). They might also occur because the XMPP-Grid Platform is running malicious software; because the XMPP-Grid Platform is running buggy software (which can fail in a state that floods the network with traffic); or because the XMPP-Grid Platform has been configured improperly. From a security standpoint, it generally makes no difference why an attack is initiated. The same countermeasures can be employed in any case.

Here is a list of attacks that can be mounted by an authorized XMPP-Grid Platform:

- Cause many false alarms or otherwise overload the XMPP-Grid Controller or other elements in the network security system (including human administrators) leading to a denial of service or disabling parts of the network security system

- Omit important actions (such as posting incriminating data), resulting in incorrect access

- Use confidential information obtained from the XMPP-Grid Controller to enable further attacks (such as using endpoint health check results to exploit vulnerable endpoints)

- Advertise data crafted to exploit vulnerabilities in the XMPP-Grid Controller or in other XMPP-Grid Platforms, with a goal of compromising those systems

- Issue a search request or set up a subscription that matches an enormous result, leading to resource exhaustion on the XMPP-Grid Controller, the publishing XMPP-Grid Platform, and/or the network

- Establish a communication channel using another XMPP-Grid Platform’s session-id

Dependencies of or vulnerabilities of authorized XMPP-Grid Platforms can be exploited to effect these attacks. Another way to effect these attacks is to gain the ability to impersonate an XMPP-Grid Platform (through theft of the XMPP-Grid Platform’s identity credentials or through other means). Even a clock skew between the XMPP-Grid Platform and XMPP-Grid Controller can cause problems if the XMPP-Grid Platform assumes that old XMPP-Grid Platform data deserves to be ignored.

8.2.3. XMPP-Grid Controllers

An unauthorized XMPP-Grid Controller (one which is not trusted by XMPP-Grid Platforms) cannot mount any attacks other than those listed in the Network Attacks section above.

An authorized XMPP-Grid Controller can mount many attacks. Similar to the XMPP-Grid Platform case described above, these attacks might occur because the XMPP-Grid Controller is controlled by a malicious, careless, or incompetent party (either an XMPP-Grid Controller administrator or an attacker who has seized control of the XMPP-Grid Controller). They might also occur because the XMPP-Grid Controller is running malicious software, because the XMPP-Grid Controller is running buggy software (which can fail in a state that corrupts data or floods the network with traffic), or because the XMPP-Grid Controller has been configured improperly.

All of the attacks listed for XMPP-Grid Platform above can be mounted by the XMPP-Grid Controller. Detection of these attacks will be more difficult since the XMPP-Grid Controller can create false operational attributes and/or logs that imply some other party created any bad data.

Additional XMPP-Grid Controller attacks can include:

- Expose different data to different XMPP-Grid Platforms to mislead investigators or cause inconsistent behavior

- Mount an even more effective denial of service attack than a single XMPP-Grid Platform could

- Obtain and cache XMPP-Grid Platform credentials so they can be used to impersonate XMPP-Grid Platforms even after a breach of the XMPP-Grid Controller is repaired

- Obtain and cache XMPP-Grid Controller administrator credentials so they can be used to regain control of the XMPP-Grid Controller after the breach of the XMPP-Grid Controller is repaired

Dependencies of or vulnerabilities of the XMPP-Grid Controller can be exploited to obtain control of the XMPP-Grid Controller and effect these attacks.

8.2.4. Certification Authority

A Certification Authority trusted to issue certificates for the XMPP-Grid Controller and/or XMPP-Grid Platforms can mount several attacks:

- Issue certificates for unauthorized parties, enabling them to impersonate authorized parties such as the XMPP-Grid Controller or an XMPP-Grid Platform. This can lead to all the threats that can be mounted by the certificate’s subject.

- Issue certificates without following all of the CA’s policies. Because this can result in issuing certificates that can be used to impersonate authorized parties, this can lead to all the threats that can be mounted by the certificate’s subject.

- Fail to revoke previously issued certificates that need to be revoked. This can lead to undetected impersonation of the certificate’s subject or failure to revoke authorization of the subject, and therefore can lead to all of the threats that can be mounted by that subject.

- Fail to regularly and securely distribute certificate revocation information. This can cause a relying party to accept a revoked certificate, leading to undetected impersonation of the certificate's subject or failure to revoke authorization of the subject, and therefore can lead to all of the threats that can be mounted by that subject. It can also cause a relying party to refuse to proceed with a transaction because timely revocation information is not available, even though the transaction should be permitted to proceed.

- Allow the CA's private key to be revealed to an unauthorized party. This can lead to all the threats above. Even worse, the actions taken with the private key will not be known to the CA.

- Fail to promptly detect and report errors and violations of trust so that relying parties can be promptly notified. This can cause the threats listed earlier in this section to persist longer than necessary, leading to many knock-on effects.

8.3. Countermeasures

Below are countermeasures for specific attack scenarios to the XMPP-Grid infrastructure.

8.3.1. Securing the XMPP-Grid Data Transfer Protocol

To address network attacks, the XMPP-Grid data transfer protocol described in this document requires that the XMPP-Grid messages MUST be carried over TLS (minimally TLS 1.2 [RFC5246]) as described in [RFC6120] and updated by [RFC7590]. The XMPP-Grid Platform MUST verify the XMPP-Grid Controller's certificate and determine whether the XMPP-Grid Controller is trusted by this XMPP-Grid Platform before completing the TLS handshake. The XMPP-Grid Controller MUST authenticate the XMPP-Grid Platform either using the SASL EXTERNAL mechanism or using the SASL SCRAM mechanism (with the SCRAM-SHA-256-PLUS variant being preferred over the SCRAM-SHA-256 variant and SHA-256 variants [RFC7677] being preferred over SHA-1 varients [RFC5802]). XMPP-Grid Platforms and XMPP-Grid Controllers using mutual certificate-based authentication SHOULD each verify the revocation status of the other party's certificate. All XMPP-Grid Controllers and XMPP-Grid Platforms MUST implement both SASL EXTERNAL and SASL SCRAM. The selection of which XMPP-Grid Platform authentication technique to use in any particular deployment is left to the administrator.

These protocol security measures provide protection against all the network attacks listed in the above document section except denial of service attacks. If protection against these denial of service attacks is desired, ingress filtering, rate limiting per source IP address, and other denial of service mitigation measures can be employed. In addition, an XMPP-Grid Controller MAY automatically disable a misbehaving XMPP-Grid Platform.

8.3.2. Securing XMPP-Grid Platforms

XMPP-Grid Platforms can be deployed in locations that are susceptible to physical attacks. Physical security measures can be taken to avoid compromise of XMPP-Grid Platforms, but these are not always practical or completely effective. An alternative measure is to configure the XMPP-Grid Controller to provide read-only access for such systems. The XMPP-Grid Controller SHOULD also include a full authorization model so that individual XMPP-Grid Platforms can be configured to have only the privileges that they need. The XMPP-Grid Controller MAY provide functional templates so that the administrator can configure a specific XMPP-Grid Platform as a DHCP server and authorize only the operations and metadata types needed by a DHCP server to be permitted for that XMPP-Grid Platform. These techniques can reduce the negative impacts of a compromised XMPP-Grid Platform without diminishing the utility of the overall system.

To handle attacks within the bounds of this authorization model, the XMPP-Grid Controller MAY also include rate limits and alerts for unusual XMPP-Grid Platform behavior. XMPP-Grid Controllers SHOULD make it easy to revoke an XMPP-Grid Platform’s authorization when necessary. Another way to detect attacks from XMPP-Grid Platforms is to create fake entries in the available data (honeytokens) which normal XMPP-Grid Platforms will not attempt to access. The XMPP-Grid Controller SHOULD include auditable logs of XMPP-Grid Platform activities.

To avoid compromise of XMPP-Grid Platform, XMPP-Grid Platform SHOULD be hardened against attack and minimized to reduce their attack surface. They should be well managed to minimize vulnerabilities in the underlying platform and in systems upon which the XMPP-Grid Platform depends. Personnel with administrative access should be carefully screened and monitored to detect problems as soon as possible.

8.3.3. Securing XMPP-Grid Controllers

Because of the serious consequences of XMPP-Grid Controller compromise, XMPP-Grid Controllers need to be especially well hardened against attack and minimized to reduce their attack surface. They need to be well managed to minimize vulnerabilities in the underlying platform and in systems upon which the XMPP-Grid Controller depends. Network security measures such as firewalls or intrusion detection systems can be used to monitor and limit traffic to and from the XMPP-Grid Controller. Personnel with administrative access ought to be carefully screened and monitored to detect problems as soon as possible. Administrators SHOULD NOT use password-based authentication but should instead use non-reusable credentials and multi-factor authentication (where available). Physical security measures ought to be employed to prevent physical attacks on XMPP-Grid Controllers.

To ease detection of XMPP-Grid Controller compromise should it occur, XMPP-Grid Controller behavior should be monitored to detect unusual behavior (such as a reboot, a large increase in traffic, or different views of an information repository for similar XMPP-Grid Platforms). XMPP-Grid Platforms should log and/or notify administrators when peculiar XMPP-Grid Controller behavior is detected. To aid forensic investigation, permanent read-only audit logs of security-relevant information (especially administrative actions) should be maintained. If XMPP-Grid Controller compromise is detected, a careful analysis should be performed of the impact of this compromise. Any reusable credentials that can have been compromised should be reissued.

8.3.4. Broker Access Models for Topics

The XMPP publish-subscribe specification [XEP-0060] defines five access models for subscribing to Topics at a Broker: open, presence, roster, authorize, and whitelist. The first model allows uncontrolled access and the next two models are appropriate only in instant-messaging applications. Therefore, a Broker SHOULD support only the authorize model (under which the Topic owner needs to approve all subscription requests and only subscribers can retrieve data items) and the whitelist model (under which only preconfigured Platforms can subscribe or retrieve data items). In order to ease the deployment burden, subscription approvals and whitelist management can be automated (e.g, the Topic "owner" can be a policy server). The choice between "authorize" and "whitelist" as the default access model is a matter for local service policy.

8.3.5. Limit on Search Result Size

While XMPP-Grid is designed for high scalability to 100,000s of Platforms, an XMPP-Grid Controller MAY establish a limit to the amount of data it is willing to return in search or subscription results. This mitigates the threat of an XMPP-Grid Platform causing resource exhaustion by issuing a search or subscription that leads to an enormous result.

8.3.6. Securing the Certification Authority

As noted above, compromise of a Certification Authority (CA) trusted to issue certificates for the XMPP-Grid Controller and/or XMPP-Grid Platforms is a major security breach. Many guidelines for proper CA security have been developed: the CA/Browser Forum's Baseline Requirements, the AICPA/CICA Trust Service Principles, etc. The CA operator and relying parties should agree on an appropriately rigorous security practices to be used.

Even with the most rigorous security practices, a CA can be compromised. If this compromise is detected quickly, relying parties can remove the CA from their list of trusted CAs, and other CAs can revoke any certificates issued to the CA. However, CA compromise may go undetected for some time, and there's always the possibility that a CA is being operated improperly or in a manner that is not in the interests of the relying parties. For this reason, relying parties may wish to "pin" a small number of particularly critical certificates (such as the certificate for the XMPP-Grid Controller). Once a certificate has been pinned, the relying party will not accept another certificate in its place unless the Administrator explicitly commands it to do so. This does not mean that the relying party will not check the revocation status of pinned certificates. However, the Administrator can still be consulted if a pinned certificate is revoked, since the CA and revocation process are not completely trusted.

8.4. Summary

XMPP-Grid's considerable value as a broker for security-sensitive data exchange distribution also makes the protocol and the network security elements that implement it a target for attack. Therefore, strong security has been included as a basic design principle within the XMPP-Grid design process.

The XMPP-Grid data transfer protocol provides strong protection against a variety of different attacks. In the event that an XMPP-Grid Platform or XMPP-Grid Controller is compromised, the effects of this compromise have been reduced and limited with the recommended role-based authorization model and other provisions, and best practices for managing and protecting XMPP-Grid systems have been described. Taken together, these measures should provide protection commensurate with the threat to XMPP-Grid systems, thus ensuring that they fulfill their promise as a network security clearing-house.

9. Privacy Considerations

XMPP-Grid Platforms can publish information about endpoint health, network access, events (which can include information about what services an endpoint is accessing), roles and capabilities, and the identity of the end user operating the endpoint. Any of this published information can be queried by other XMPP-Grid Platforms and could potentially be used to correlate network activity to a particular end user.

Dynamic and static information brokered by an XMPP-Grid Controller, ostensibly for purposes of correlation by XMPP-Grid Platforms for intrusion detection, could be misused by a broader set of XMPP-Grid Platforms which hitherto have been performing specific roles with strict well-defined separation of duties.

Care needs to be taken by deployers of XMPP-Grid to ensure that the information published by XMPP-Grid Platforms does not violate agreements with end users or local and regional laws and regulations. This can be accomplished either by configuring XMPP-Grid Platforms to not publish certain information or by restricting access to sensitive data to trusted XMPP-Grid Platforms. That is, the easiest means to ensure privacy or protect sensitive data, is to omit or not share it at all.

Another consideration for deployers is to enable end-to-end encryption to ensure the data is protected from the data layer to data layer and thus protect it from the transport layer.

10. Acknowledgements

The authors would like to acknowledge the contributions, authoring and/or editing of the following people: Joseph Salowey, Lisa Lorenzin, Clifford Kahn, Henk Birkholz, Jessica Fitzgerald-McKay, Steve Hanna, and Steve Venema. In addition, we want to thank Takeshi Takahashi, Panos Kampanakis, Adam Montville, Chris Inacio, and Dave Cridland for reviewing and providing valuable comments.

11. References

11.1. Normative References

[I-D.ietf-sacm-terminology]
Birkholz, H., Lu, J., Strassner, J., and N. Cam-Winget, "Secure Automation and Continuous Monitoring (SACM) Terminology", draft-ietf-sacm-terminology-14 (work in progress), December 2017.

[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>.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <https://www.rfc-editor.org/info/rfc6120>.

[RFC7590] Saint-Andre, P. and T. Alkemade, "Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP)", RFC 7590, DOI 10.17487/RFC7590, June 2015, <https://www.rfc-editor.org/info/rfc7590>.

[RFC7677] Hansen, T., "SCRAM-SHA-256 and SCRAM-SHA-256-PLUS Simple Authentication and Security Layer (SASL) Mechanisms", RFC 7677, DOI 10.17487/RFC7677, November 2015, <https://www.rfc-editor.org/info/rfc7677>.

[XEP-0004] Eatmon, R., Hildebrand, J., Miller, J., Muldowney, T., and P. Saint-Andre, "Data Forms", XSF XEP 0004, August 2007.

[XEP-0030] Hildebrand, J., Millard, P., Eatmon, R., and P. Saint-Andre, "Service Discovery", XSF XEP 0030, July 2010.

[XEP-0060] Millard, P., Saint-Andre, P., and R. Meijer, "Publish-Subscribe", XSF XEP 0060, December 2017.

11.2. Informative References

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, DOI 10.17487/RFC5246, August 2008, <https://www.rfc-editor.org/info/rfc5246>.

[RFC5802] Newman, C., Menon-Sen, A., Melnikov, A., and N. Williams, "Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms", RFC 5802, DOI 10.17487/RFC5802, July 2010, <https://www.rfc-editor.org/info/rfc5802>.

[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>.

[RFC8274] Kampanakis, P. and M. Suzuki, "Incident Object Description Exchange Format Usage Guidance", RFC 8274, DOI 10.17487/RFC8274, November 2017, <https://www.rfc-editor.org/info/rfc8274>.

Authors' Addresses

Nancy Cam-Winget (editor)
Cisco Systems
3550 Cisco Way
San Jose, CA 95134
USA

Email: ncamwing@cisco.com

Syam Appala
Cisco Systems
3550 Cisco Way
San Jose, CA 95134
USA

Email: syam1@cisco.com

Scott Pope
Cisco Systems
5400 Meadows Road
Suite 300
Lake Oswego, OR 97035
USA

Email: scottp@cisco.com

Peter Saint-Andre
Mozilla

Email: stpeter@mozilla.com

MILE N. Cam-Winget, Ed.
Internet-Draft S. Appala
Intended status: Standards Track S. Pope
Expires: September 28, 2019 Cisco Systems
P. Saint-Andre
Mozilla
March 27, 2019

Using XMPP for Security Information Exchange
draft-ietf-mile-xmpp-grid-11

Abstract

This document describes how to use the Extensible Messaging and Presence Protocol (XMPP) to collect and distribute security incident reports and other security-relevant information between network-connected devices, primarily for the purpose of communication among Computer Security Incident Response Teams and associated entities. To illustrate the principles involved, this document describes such a usage for the Incident Object Description Exchange Format (IODEF).

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

This document defines an architecture, i.e., "XMPP-Grid", as a method for using the Extensible Messaging and Presence Protocol (XMPP) [RFC6120] to collect and distribute security incident reports and other security-relevant information among network platforms, endpoints, and any other network-connected device, primarily for the purpose of communication among Computer Security Incident Response Teams and associated entities. In effect, this document specifies an Applicability Statement ([RFC2026], Section 3.2) that defines how to use XMPP for the exchange of security notifications on a controlled-access network among authorized entities.

Among other things, XMPP provides a publish-subscribe service [XEP-0060] that acts as a broker, enabling control-plane functions by which entities can discover available information to be published or consumed. Although such information can take the form of any structured data (XML, JSON, etc.), this document illustrates the principles of XMPP-Grid with examples that use the Incident Object Description Exchange Format (IODEF) [RFC7970]. That is, while other security information formats can be shared using XMPP, this document uses IODEF as one such example format that can be published and consumed using XMPP.

2. Terminology

This document uses XMPP terminology defined in [RFC6120] and [XEP-0060]. Because the intended audience for this document is those who implement and deploy security reporting systems, mappings are provided for the benefit of XMPP developers and operators.

Broker: A specific type of controller containing control plane functions; as used here, the term refers to an XMPP publish-subscribe service.

Broker Flow: A method by which security incident reports and other security-relevant information is published and consumed in a mediated fashion through a Broker. In this flow, the Broker handles authorization of Consumers and Providers to Topics, receives messages from Providers, and delivers published messages to Consumers.

Consumer: An entity that contains functions to receive information from other components; as used here, the term refers to an XMPP publish-subscribe Subscriber.

Controller: A "component containing control plane functions that manage and facilitate information sharing or execute on security functions"; as used here, the term refers to an XMPP server, which provides core message delivery [RFC6120] used by publish-subscribe entities.

Node: The XMPP term for a Topic.

Platform: Any entity that connects to the XMPP-Grid in order to publish or consume security-relevant information.

Provider: An entity that contains functions to provide information to other components; as used here, the term refers to an XMPP publish-subscribe Publisher.

Topic: A contextual information channel created on a Broker at which messages generated by a Provider are propagated in real time to one or more Consumers. Each Topic is limited to a specific type and format of security data (e.g. IODEF namespace) and provides an XMPP interface by which the data can be obtained.

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.

3. Architecture

The following figure illustrates the architecture of XMPP-Grid.

```
             +--------------------------------------+
             | +--------------------------------------+
             | | +--------------------------------------+
             | | |                                      |
             +-| |             Platforms                |
               +-|                                      |
                 +--------------------------------------+
                   /   \         /   \            /   \
                  /  C  \       /     \          /     \
                  -  o  -       -  d  -          -     -
                   ||n||A        | a  |B          |   |C
                   ||t||         | t  |           |   |
                  -  r  -       -  a  -           |   |
                  \  o  /       \     /           |   |
                   \ l /         \   /            |   |
                /|---------------------|\         |   |
         /|----/                         \--------| d |--|\
        /     /        Controller         \ ctrl  | a |    \
        \     \        & Broker           / plane | t |    /
         \|----\                         /--------| a |--|/
                \|---------------------|/         |   |
                   /   \         /   \            |   |
                  /  C  \       /     \           |   |
                  -  o  -       -  d  -           |   |
                   ||n||A        | a |B           |   |C
                   ||t||         | t |            |   |
                  -  r  -       -  a  -          -     -
                  \  o  /       \     /          \     /
                   \ l /         \   /            \   /
                 +------------------------------------+
                 |                                    |-+
                 |            Platforms               | |
                 |                                    | |-+
                 +------------------------------------+ | |
                   +------------------------------------+ |
                     +------------------------------------+
```

Figure 1: XMPP-Grid Architecture

Platforms connect to the Controller (XMPP server) to authenticate and then establish appropriate authorizations to be a Provider or Consumer of topics of interest at the Broker. The control plane messaging is established through XMPP and shown as "A" (control plane interface) in Figure 1. Authorized Platforms can then share data either through the Broker (shown as "B" in Figure 1) or in some cases directly (shown as "C" in Figure 1). This document focuses primarily on the Broker Flow for information sharing ("direct flow" interactions can be used for specialized purposes such as bulk data transfer, but methods for doing so are outside the scope of this document).

4. Workflow

Implementations of XMPP-Grid workflow adhere to the following workflow:

a. A Platform with a source of security data requests connection to the XMPP-Grid via a Controller.

b. The Controller authenticates the Platform.

c. The Platform establishes authorized privileges (e.g. privilege to publish and/or subscribe to one or more Topics) with a Broker.

d. The Platform can publish security incident reports and other security-relevant information to a Topic, subscribe to a Topic, query a Topic, or any combination of these operations.

e. A Provider unicasts its Topic updates to the Grid in real time through a Broker. The Broker handles replication and distribution of the Topic to Consumers. A Provider can publish the same or different data to multiple Topics.

f. Any Platform on the Grid can subscribe to any Topics published to the Grid (as permitted by authorization policy), and (as Consumers) will then receive a continual, real-time stream of updates from the Topics to which it is subscribed.

The general workflow is summarized in the figure below:

```
   +--------------+        +------------+           +---------------+
   | IODEF Client |        | Controller |           | IODEF Service |
   |  (Consumer)  |        |  & Broker  |           |  (Provider)   |
   +--------------+        +------------+           +---------------+
           |                      |                         |
           |  Establish XMPP      |                         |
           |  Client Session      |                         |
           |  (RFC 6120)          |                         |
           |--------------------->|                         |
           |                      | Establish XMPP          |
           |                      | Client Session          |
           |                      | (RFC 6120)              |
           |                      |<------------------------|
           |                      | Request Topic Creation  |
           |                      | (XEP-0060)              |
           |                      |<------------------------|
           |                      | Topic Creation Success  |
           |                      | (XEP-0060)              |
           |                      |------------------------>|
           | Request Topic List   |                         |
           | (XEP-0030)           |                         |
           |--------------------->|                         |
           | Return Topic List    |                         |
           | (XEP-0030)           |                         |
           |<---------------------|                         |
           |                      |                         |
           | Query Each Topic     |                         |
           | (XEP-0030)           |                         |
           |--------------------->|                         |
           | Return Topic Data    |                         |
           | Including Topic Type |                         |
           | (XEP-0030)           |                         |
           |<---------------------|                         |
           |                      |                         |
           | Subscribe to IODEF   |                         |
           | Topic (XEP-0060)     |                         |
           |--------------------->|                         |
           | Subscription Success |                         |
           | (XEP-0060)           |                         |
           |<---------------------|                         |
           |                      | Publish IODEF Incident  |
           |                      | (XEP-0060)              |
           | Receive IODEF        |<------------------------|
           | Incident (XEP-0060)  |                         |
           |<---------------------|                         |
           |                      |                         |
```

Figure 2: IODEF Example Workflow

XMPP-Grid implementations MUST adhere to the mandatory-to-implement and mandatory-to-negotiate features as defined in [RFC6120]. Similarly, implementations MUST implement [XEP-0060] to facilitate the asynchronous sharing for information. Implementations SHOULD implement Service Discovery as defined in [XEP-0030] to facilitate the means to dynamically discover the available information and namespaces (Topics) to be published or consumed. Implementations should take caution if their deployments allow for a large number of topics. The Result Set Management as defined in [XEP-0059], SHOULD be used to allow the requesting entity to explicitly request Service Discovery result sets to be returned in pages or limited size, if the discovery results are larger in size. Note that the control plane may optionally also implement [XEP-0203] to facilitate delayed delivery of messages to the connected consumer as described in [XEP-0060]. Since information may be timely and sensitive, capability providers should communicate to the controller whether its messages can be cached for delayed delivery during configuration; such function is out of scope for this document.

The following sections provide protocol examples for the service discovery and publish-subscribe parts of the workflow.

5. Service Discovery

Using the XMPP service discovery extension [XEP-0030], a Controller enables Platforms to discover what information can be consumed through the Broker, and at which Topics. Platforms could use [XEP-0059] to restrict the size of the result sets the Controller returns in Service Discovery response. As an example, the Controller at 'security-grid.example' might provide a Broker at 'broker.security-grid.example' hosting a number of Topics. A Platform at 'xmpp-grid-client@mile-host.example' would query the Broker about its available Topics by sending an XMPP "disco#items" request to the Broker:

```
<iq type='get'
    from='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    to='broker.security-grid.example'
    id='B3C17F7B-B9EF-4ABA-B08D-805DA9F34626'>
  <query xmlns='http://jabber.org/protocol/disco#items'/>
</iq>
```

The Broker responds with the Topics it hosts:

```
<iq type='result'
    from='broker.security-grid.example'
    to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    id='B3C17F7B-B9EF-4ABA-B08D-805DA9F34626'>
  <query xmlns='http://jabber.org/protocol/disco#items'>
    <item node='NEA1'
          name='Endpoint Posture Information'
          jid='broker.security-grid.example'/>
    <item node='MILEHost'
          name='MILE Host Data'
          jid='broker.security-grid.example'/>
  </query>
</iq>
```

In order to determine the exact nature of each Topic (i.e., in order to find topics that publish incidents in the IODEF format), a Platform would send an XMPP "disco#info" request to each Topic:

```
<iq type='get'
    from='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    to='broker.security-grid.example'
    id='D367D4ED-2795-489C-A83E-EAAFA07A0356'
  <query xmlns='http://jabber.org/protocol/disco#info'
         node='MILEHost'/>
</iq>
```

The Broker responds with the "disco#info" description, which MUST include an XMPP Data Form [XEP-0004] including a 'pubsub#type' field that specifies the supported namespace (in this example, the IODEF namespace defined in [RFC7970]):

```
<iq type='result'
    from='broker.security-grid.example'
    to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    id='D367D4ED-2795-489C-A83E-EAAFA07A0356'/>
  <query xmlns='http://jabber.org/protocol/disco#info'
       node='MILEHost'>
    <identity category='pubsub' type='leaf'/>
    <feature var='http://jabber.org/protocol/pubsub'/>
    <x xmlns='jabber:x:data' type='result'>
     <field var='FORM_TYPE' type='hidden'>
      <value>http://jabber.org/protocol/pubsub#meta-data</value>
     </field>
     <field var='pubsub#type' label='Payload type' type='text-single'>
      <value>urn:ietf:params:xml:ns:iodef-2.0</value>
     </field>
    </x>
  </query>
</iq>
```

The Platform discovers the topics by obtaining the Broker's response and obtaining the namespaces returned in the "pubsub#type" field (in the foregoing example, IODEF 2.0).

6. Publish-Subscribe

Using the XMPP publish-subscribe extension [XEP-0060], a Consumer subscribes to a Topic and a Provider publishes information to that Topic, which the Broker then distributes to all subscribed Consumers.

First, a Provider would create a Topic as follows:

```
<iq type='set'
    from='datasource@provider.example/F12C2EFC9BB0'
    to='broker.security-grid.example'
    id='A67507DF-2F22-4937-8D30-88D2F7DBA279'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <create node='MILEHost'/>
  </pubsub>
</iq>
```

Note: The foregoing example is the minimal protocol needed to create a Topic with the default node configuration on the XMPP publish-subscribe service specified in the 'to' address of the creation request stanza. Depending on security requirements, the Provider might need to request a non-default configuration for the node; see [XEP-0060] for detailed examples. To also help with the Topic configuration, the Provider may also optionally include configurations parameters such as:

```
<configure>
  <x xmlns='jabber:x:data' type='submit'>
    <field var='FORM_TYPE' type='hidden'>
      <value>http://jabber.org/protocol/pubsub#node_config</value>
    </field>
    <field var='pubsub#access_model'><value>authorize</value></field>
    <field var='pubsub#persist_items'><value>1</value></field>
    <field var='pubsub#send_last_published_item'><value>never</value></field>
  </x>
</configure>
```

The above configuration indicates the Topic is configured to enable the XMPP-Controller to manage the subscriptions, be in persistent mode and disables the Broker from cacheing the last item published. Please refer to [XEP-0060] a more detailed description of these configuration and other available configuration options.

Unless an error occurs (see [XEP-0060] for various error flows), the Broker responds with success:

```
<iq type='result'
    from='broker.security-grid.example'
    to='datasource@provider.example/F12C2EFC9BB0'
    id='A67507DF-2F22-4937-8D30-88D2F7DBA279'/>
```

Second, a Consumer would subscribe as follows:

```
<iq type='set'
    from='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    to='broker.security-grid.example'
    id='9C6EEE9E-F09A-4418-8D68-3BA6AF852522'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <subscribe node='MILEHost'
               jid='xmpp-grid-client@mile-host.example'/>
  </pubsub>
</iq>
```

Unless an error occurs (see [XEP-0060] for various error flows), the Broker responds with success:

```
<iq type='result'
    from='broker.security-grid.example'
    to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    id='9C6EEE9E-F09A-4418-8D68-3BA6AF852522'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <subscription
        node='MILEHost'
        jid='xmpp-grid-client@mile-host.example'
        subscription='subscribed'/>
  </pubsub>
</iq>
```


Third, a Provider would publish an incident to the broker using the MILEHost topic as follows:


```
<iq type='set'
    from='datasource@provider.example/F12C2EFC9BB0'
    to='broker.security-grid.example'
    id='2A17D283-0DAE-4A6C-85A9-C10B1B40928C'>
  <pubsub xmlns='http://jabber.org/protocol/pubsub'>
    <publish node='MILEHost'>
      <item id='8bh1g27skbga47fh9wk7'>
        <IODEF-Document version="2.00" xml:lang="en"
          xmlns="urn:ietf:params:xml:ns:iodef-2.0"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation=
            "http://www.iana.org/assignments/xml-registry/
             schema/iodef-2.0.xsd">
          <Incident purpose="reporting" restriction="private">
            <IncidentID name="csirt.example.com">492382</IncidentID>
            <GenerationTime>2015-07-18T09:00:00-05:00</GenerationTime>
            <Contact type="organization" role="creator">
              <Email>
                <EmailTo>contact@csirt.example.com</EmailTo>
              </Email>
            </Contact>
          </Incident>
        </IODEF-Document>
      </item>
    </publish>
  </pubsub>
</iq>
```


(The payload in the foregoing example is from [RFC7970]; payloads for additional use cases can be found in [RFC8274].)

The Broker would then deliver that incident report to all Consumers who are subscribed to the Topic:

```
<message
    from='broker.security-grid.example'
    to='xmpp-grid-client@mile-host.example/2EBE702A97D6'
    id='37B3921D-4F7F-450F-A589-56119A88BC2E'>
  <event xmlns='http://jabber.org/protocol/pubsub#event'>
    <items node='MILEHost'>
      <item id='iah37s61s964gquqy47aksbx9453ks77'>
        <IODEF-Document version="2.00" xml:lang="en"
          xmlns="urn:ietf:params:xml:ns:iodef-2.0"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
          xsi:schemaLocation=
            "http://www.iana.org/assignments/xml-registry/
             schema/iodef-2.0.xsd">
          <Incident purpose="reporting" restriction="private">
            <IncidentID name="csirt.example.com">492382</IncidentID>
            <GenerationTime>2015-07-18T09:00:00-05:00</GenerationTime>
            <Contact type="organization" role="creator">
              <Email>
                <EmailTo>contact@csirt.example.com</EmailTo>
              </Email>
            </Contact>
          </Incident>
        </IODEF-Document>
      </item>
    </items>
  </event>
</message>
```

Note that [XEP-0060] uses the XMPP "<message />" stanza for delivery of content. To ensure that messages are delivered to the Consumer even if the Consumer is not online at the same time that the Publisher generates the message, an XMPP-Grid Controller MUST support "offline messaging" delivery semantics as specified in [RFC6121], best practices for which are further explained in [XEP-0160].

7. IANA Considerations

This document has no actions for IANA.

8. Security Considerations

An XMPP-Grid Controller serves as an controlling broker for XMPP-Grid Platforms such as Enforcement Points, Policy Servers, CMDBs, and Sensors, using a publish-subscribe-search model of information exchange and lookup. By increasing the ability of XMPP-Grid Platforms to learn about and respond to security incident reports and other security-relevant information, XMPP-Grid can improve the timeliness and utility of the security system. However, this integrated security system can also be exploited by attackers if they can compromise it. Therefore, strong security protections for XMPP-Grid are essential.

As XMPP is the core of this document, the security considerations of [RFC6120] applies. In addition, as XMPP-Grid defines a specific instance, this section provides a security analysis of the XMPP-Grid data transfer protocol and the architectural elements that employ it, specifically with respect to their use of this protocol. Three subsections define the trust model (which elements are trusted to do what), the threat model (attacks that can be mounted on the system), and the countermeasures (ways to address or mitigate the threats previously identified).

8.1. Trust Model

The first step in analyzing the security of the XMPP-Grid transport protocol is to describe the trust model, listing what each architectural element is trusted to do. The items listed here are assumptions, but provisions are made in the Threat Model and Countermeasures sections for elements that fail to perform as they were trusted to do.

8.1.1. Network

The network used to carry XMPP-Grid messages (i.e., the underlying network transport layer over which XMPP runs) is trusted to:

- o Perform best effort delivery of network traffic

The network used to carry XMPP-Grid messages is not expected (trusted) to:

- o Provide confidentiality or integrity protection for messages sent over it
- o Provide timely or reliable service

8.1.2. XMPP-Grid Platforms

Authorized XMPP-Grid Platforms are trusted to:

- o Preserve the confidentiality of sensitive data retrieved via the XMPP-Grid Controller

8.1.3. XMPP-Grid Controller

The XMPP-Grid Controller (including its associated Broker) is trusted to:

- o Broker requests for data and enforce authorization of access to this data throughout its lifecycle
- o Perform service requests in a timely and accurate manner
- o Create and maintain accurate operational attributes
- o Only reveal data to and accept service requests from authorized parties
- o Preserve the integrity (and confidentiality against unauthorized parties) of the data flowing through it.

The XMPP-Grid Controller is not expected (trusted) to:

- o Verify the truth (correctness) of data

8.1.4. Certification Authority

To allow XMPP-Grid Platforms to mutually authenticate with XMPP-Grid Controllers, it is expected that a Certification Authority (CA) is employed to issue certificates. Such a CA (or each CA, if there are several) is trusted to:

- o Ensure that only proper certificates are issued and that all certificates are issued in accordance with the CA's policies
- o Revoke certificates previously issued when necessary
- o Regularly and securely distribute certificate revocation information
- o Promptly detect and report any violations of this trust so that they can be handled

The CA is not expected (trusted) to:

- o Issue certificates that go beyond the XMPP-Grid needs or other constraints imposed by a relying party.

8.2. Threat Model

To secure the XMPP-Grid data transfer protocol and the architectural elements that implement it, this section identifies the attacks that can be mounted against the protocol and elements.

8.2.1. Network Attacks

A variety of attacks can be mounted using the network. For the purposes of this subsection the phrase "network traffic" can be taken to mean messages and/or parts of messages. Any of these attacks can be mounted by network elements, by parties who control network elements, and (in many cases) by parties who control network-attached devices.

- Network traffic can be passively monitored to glean information from any unencrypted traffic

- Even if all traffic is encrypted, valuable information can be gained by traffic analysis (volume, timing, source and destination addresses, etc.)

- Network traffic can be modified in transit

- Previously transmitted network traffic can be replayed

- New network traffic can be added

- Network traffic can be blocked, perhaps selectively

- A "Man In The Middle" (MITM) attack can be mounted where an attacker interposes itself between two communicating parties and poses as the other end to either party or impersonates the other end to either or both parties

- Undesired network traffic can be sent in an effort to overload an architectural component, thus mounting a denial of service attack

8.2.2. XMPP-Grid Platforms

An unauthorized XMPP-Grid Platform (one which is not recognized by the XMPP-Grid Controller or is recognized but not authorized to perform any actions) cannot mount any attacks other than those listed in the Network Attacks section above.

An authorized XMPP-Grid Platform, on the other hand, can mount many attacks. These attacks might occur because the XMPP-Grid Platform is controlled by a malicious, careless, or incompetent party (whether because its owner is malicious, careless, or incompetent or because the XMPP-Grid Platform has been compromised and is now controlled by a party other than its owner). They might also occur because the XMPP-Grid Platform is running malicious software; because the XMPP-Grid Platform is running buggy software (which can fail in a state that floods the network with traffic); or because the XMPP-Grid Platform has been configured improperly. From a security standpoint, it generally makes no difference why an attack is initiated. The same countermeasures can be employed in any case.

Here is a list of attacks that can be mounted by an authorized XMPP-Grid Platform:

- Cause many false alarms or otherwise overload the XMPP-Grid Controller or other elements in the network security system (including human administrators) leading to a denial of service or disabling parts of the network security system

- Omit important actions (such as posting incriminating data), resulting in incorrect access

- Use confidential information obtained from the XMPP-Grid Controller to enable further attacks (such as using endpoint health check results to exploit vulnerable endpoints)

- Advertise data crafted to exploit vulnerabilities in the XMPP-Grid Controller or in other XMPP-Grid Platforms, with a goal of compromising those systems

- Issue a search request or set up a subscription that matches an enormous result, leading to resource exhaustion on the XMPP-Grid Controller, the publishing XMPP-Grid Platform, and/or the network

- Establish a communication channel using another XMPP-Grid Platform’s session-id

- Advertise false data that leads to incorrect (e.g., potentially attacker-controlled or -induced) behavior of XMPP-Grid Platforms, by virtue of applying correct procdeures to the falsified input.

Dependencies of or vulnerabilities of authorized XMPP-Grid Platforms can be exploited to effect these attacks. Another way to effect these attacks is to gain the ability to impersonate an XMPP-Grid Platform (through theft of the XMPP-Grid Platform’s identity credentials or through other means). Even a clock skew between the XMPP-Grid Platform and XMPP-Grid Controller can cause problems if the XMPP-Grid Platform assumes that old XMPP-Grid Platform data should be ignored.

8.2.3. XMPP-Grid Controllers

An unauthorized XMPP-Grid Controller (one which is not trusted by XMPP-Grid Platforms) cannot mount any attacks other than those listed in the Network Attacks section above.

An authorized XMPP-Grid Controller can mount many attacks. Similar to the XMPP-Grid Platform case described above, these attacks might occur because the XMPP-Grid Controller is controlled by a malicious, careless, or incompetent party (either an XMPP-Grid Controller administrator or an attacker who has seized control of the XMPP-Grid Controller). They might also occur because the XMPP-Grid Controller is running malicious software, because the XMPP-Grid Controller is running buggy software (which can fail in a state that corrupts data or floods the network with traffic), or because the XMPP-Grid Controller has been configured improperly.

All of the attacks listed for XMPP-Grid Platform above can be mounted by the XMPP-Grid Controller. Detection of these attacks will be more difficult since the XMPP-Grid Controller can create false operational attributes and/or logs that imply some other party created any bad data.

Additional XMPP-Grid Controller attacks can include:

- Expose different data to different XMPP-Grid Platforms to mislead investigators or cause inconsistent behavior

- Mount an even more effective denial of service attack than a single XMPP-Grid Platform could; some mechanisms include inducing the many platforms to perform the same operation in an amplification-style attack, completely refusing to pass any traffic at all, or sending floods of traffic to (certain) platforms or other targets.

- Obtain and cache XMPP-Grid Platform credentials so they can be used to impersonate XMPP-Grid Platforms even after a breach of the XMPP-Grid Controller is repaired. Some SASL mechanisms (including the mandatory-to-implement SCRAM and EXTERNAL with TLS mutual certificate-based authentication) do not admit this class of attack, but others (such as PLAIN) are susceptible.

- Obtain and cache XMPP-Grid Controller administrator credentials so they can be used to regain control of the XMPP-Grid Controller after the breach of the XMPP-Grid Controller is repaired.

- Eavesdrop, inject or modify the data being transferred between provider and consumer

Dependencies of or vulnerabilities of the XMPP-Grid Controller can be exploited to obtain control of the XMPP-Grid Controller and effect these attacks.

8.2.4. Certification Authority

A Certification Authority trusted to issue certificates for the XMPP-Grid Controller and/or XMPP-Grid Platforms can mount several attacks:

- o Issue certificates for unauthorized parties, enabling them to impersonate authorized parties such as the XMPP-Grid Controller or an XMPP-Grid Platform. This can lead to all the threats that can be mounted by the certificate's subject.

- o Issue certificates without following all of the CA's policies. Because this can result in issuing certificates that can be used to impersonate authorized parties, this can lead to all the threats that can be mounted by the certificate's subject.

- o Fail to revoke previously issued certificates that need to be revoked. This can lead to undetected impersonation of the certificate's subject or failure to revoke authorization of the subject, and therefore can lead to all of the threats that can be mounted by that subject.

- o Fail to regularly and securely distribute certificate revocation information. This can cause a relying party to accept a revoked certificate, leading to undetected impersonation of the certificate's subject or failure to revoke authorization of the subject, and therefore can lead to all of the threats that can be mounted by that subject. It can also cause a relying party to refuse to proceed with a transaction because timely revocation information is not available, even though the transaction should be permitted to proceed.

- o Allow the CA's private key to be revealed to an unauthorized party. This can lead to all the threats above. Even worse, the actions taken with the private key will not be known to the CA.

- o Fail to promptly detect and report errors and violations of trust so that relying parties can be promptly notified. This can cause the threats listed earlier in this section to persist longer than necessary, leading to many knock-on effects.

8.3. Countermeasures

Below are countermeasures for specific attack scenarios to the XMPP-Grid infrastructure.

8.3.1. Securing the XMPP-Grid Data Transfer Protocol

To address network attacks, the XMPP-Grid data transfer protocol described in this document requires that the XMPP-Grid messages MUST be carried over TLS (minimally TLS 1.2 and preferrably TLS 1.3 [RFC8446]) as described in [RFC6120] and updated by [RFC7590]. The XMPP-Grid Controller and XMPP-Grid Platforms SHOULD mutually authenticate. The XMPP-Grid Platform MUST verify the XMPP-Grid Controller's certificate and determine whether the XMPP-Grid Controller is trusted by this XMPP-Grid Platform before completing the TLS handshake. To ensure interoperability, implementations MUST implement at least one of either the SASL EXTERNAL mechanism [RFC4422] or the SASL SCRAM mechanism. When using the SASL SCRAM mechanism, the SCRAM-SHA-256-PLUS variant SHOULD be preferred over the SCRAM-SHA-256 variant; and SHA-256 variants [RFC7677] SHOULD be preferred over SHA-1 variants [RFC5802]). XMPP-Grid Platforms and XMPP-Grid Controllers using certificate-based authentication SHOULD each verify the revocation status of the other party's certificate. The selection of which XMPP-Grid Platform authentication technique to use in any particular deployment is left to the administrator.

These protocol security measures provide protection against all the network attacks listed in the above document section except denial of service attacks. If protection against these denial of service attacks is desired, ingress filtering, rate limiting per source IP address, and other denial of service mitigation measures can be employed. In addition, an XMPP-Grid Controller MAY automatically disable a misbehaving XMPP-Grid Platform.

8.3.2. Securing XMPP-Grid Platforms

XMPP-Grid Platforms can be deployed in locations that are susceptible to physical attacks. Physical security measures can be taken to avoid compromise of XMPP-Grid Platforms, but these are not always practical or completely effective. An alternative measure is to configure the XMPP-Grid Controller to provide read-only access for such systems. The XMPP-Grid Controller SHOULD also include a full authorization model so that individual XMPP-Grid Platforms can be configured to have only the privileges that they need. The XMPP-Grid Controller MAY provide functional templates so that the administrator can configure a specific XMPP-Grid Platform as a DHCP [RFC2131] server and authorize only the operations and metadata types needed by a DHCP server to be permitted for that XMPP-Grid Platform. These techniques can reduce the negative impacts of a compromised XMPP-Grid Platform without diminishing the utility of the overall system.

To handle attacks within the bounds of this authorization model, the XMPP-Grid Controller MAY also include rate limits and alerts for unusual XMPP-Grid Platform behavior. XMPP-Grid Controllers SHOULD make it easy to revoke an XMPP-Grid Platform's authorization when necessary. The XMPP-Grid Controller SHOULD include auditable logs of XMPP-Grid Platform activities.

To avoid compromise of XMPP-Grid Platform, XMPP-Grid Platform SHOULD be hardened against attack and minimized to reduce their attack surface. They should be well managed to minimize vulnerabilities in the underlying platform and in systems upon which the XMPP-Grid Platform depends. Personnel with administrative access should be carefully screened and monitored to detect problems as soon as possible.

8.3.3. Securing XMPP-Grid Controllers

Because of the serious consequences of XMPP-Grid Controller compromise, XMPP-Grid Controllers need to be especially well hardened against attack and minimized to reduce their attack surface. They need to be well managed to minimize vulnerabilities in the underlying platform and in systems upon which the XMPP-Grid Controller depends. Network security measures such as firewalls or intrusion detection systems can be used to monitor and limit traffic to and from the XMPP-Grid Controller. Personnel with administrative access ought to be carefully screened and monitored to detect problems as soon as possible. Administrators SHOULD NOT use password-based authentication but SHOULD instead use non-reusable credentials and multi-factor authentication (where available). Physical security measures ought to be employed to prevent physical attacks on XMPP-Grid Controllers.

To ease detection of XMPP-Grid Controller compromise should it occur, XMPP-Grid Controller behavior should be monitored to detect unusual behavior (such as a reboot, a large increase in traffic, or different views of an information repository for similar XMPP-Grid Platforms). It is a matter of local policy whether XMPP-Grid Platforms log and/or notify administrators when peculiar XMPP-Grid Controller behavior is detected, and whether read-only audit logs of security-relevant information (especially administrative actions) are maintained; however, such behavior is encouraged to aid in forensic analysis. Furthermore, if compromise of an XMPP-Grid Controller is detected, a careful analysis should be performed and any reusable credentials that can have been compromised should be reissued.

To address the potential for the XMPP-Grid controller to eavesdrop, modify or inject data, it would be desirable to deploy end-to-end encryption between the provider and the consumer(s). Unfortunately, because there is no standardized method for encryption of one-to-many messages within XMPP, techniques for enforcing end-to-end encryption are out of scope for this specification.

8.3.4. Broker Access Models for Topics

The XMPP publish-subscribe specification [XEP-0060] defines five access models for subscribing to Topics at a Broker: open, presence, roster, authorize, and whitelist. The first model allows uncontrolled access and the next two models are appropriate only in instant-messaging applications. Therefore, a Broker SHOULD support only the authorize model (under which the Topic owner needs to approve all subscription requests and only subscribers can retrieve data items) and the whitelist model (under which only preconfigured Platforms can subscribe or retrieve data items). In order to ease the deployment burden, subscription approvals and whitelist management can be automated (e.g, the Topic "owner" can be a policy server). The choice between "authorize" and "whitelist" as the default access model is a matter for local service policy.

8.3.5. Limit on Search Result Size

While XMPP-Grid is designed for high scalability to 100,000s of Platforms, an XMPP-Grid Controller MAY establish a limit to the amount of data it is willing to return in search or subscription results. Platforms could use [XEP-0059] to restrict the size of the result sets the Controller returns in search or subscription results or topics' service discovery. This mitigates the threat of an XMPP-Grid Platform causing resource exhaustion by issuing a search or subscription that leads to an enormous result.

8.3.6. Securing the Certification Authority

As noted above, compromise of a Certification Authority (CA) trusted to issue certificates for the XMPP-Grid Controller and/or XMPP-Grid Platforms is a major security breach. Many guidelines for proper CA security have been developed: the CA/Browser Forum's Baseline Requirements, the AICPA/CICA Trust Service Principles, the IETF's Certificate Transparency [RFC6962] etc. The CA operator and relying parties should agree on an appropriately rigorous security practices to be used.

Even with the most rigorous security practices, a CA can be compromised. If this compromise is detected quickly, relying parties can remove the CA from their list of trusted CAs, and other CAs can revoke any certificates issued to the CA. However, CA compromise may go undetected for some time, and there’s always the possibility that a CA is being operated improperly or in a manner that is not in the interests of the relying parties. For this reason, relying parties may wish to "pin" a small number of particularly critical certificates (such as the certificate for the XMPP-Grid Controller). Once a certificate has been pinned, the relying party will not accept another certificate in its place unless the Administrator explicitly commands it to do so. This does not mean that the relying party will not check the revocation status of pinned certificates. However, the Administrator can still be consulted if a pinned certificate is revoked, since the CA and revocation process are not completely trusted. By "pinning" one or a small set of certificates, the relying party has the effective XMPP-Grid Controller(s) authorized to connect to.

8.3.7. End-to-End Encryption of Messages

Because it is expected that there will be a relatively large number of Consumers for every Topic, for purposes of content discovery and scaling this document specifies a "one-to-many" communications pattern using the XMPP Publish-Subscribe extension. Unfortunately, there is no standardized technology for end-to-end encryption of one-to-many messages in XMPP. This implies that messages can be subject to eavesdropping, data injection, and data modification attacks within a Broker or Controller. If it is necessary to mitigate against such attacks, implementers would need to select a messaging pattern other than [XEP-0060], most likely the basic "instant messaging" pattern specified in [RFC6121] with a suitable XMPP extension for end-to-end encryption (such as [RFC3923] or a more modern method such as [XEP-0384]). The description of such an approach is out of scope for this document.

8.4. Summary

XMPP-Grid’s considerable value as a broker for security-sensitive data exchange distribution also makes the protocol and the network security elements that implement it a target for attack. Therefore, strong security has been included as a basic design principle within the XMPP-Grid design process.

The XMPP-Grid data transfer protocol provides strong protection against a variety of different attacks. In the event that an XMPP-Grid Platform or XMPP-Grid Controller is compromised, the effects of this compromise have been reduced and limited with the recommended role-based authorization model and other provisions, and best practices for managing and protecting XMPP-Grid systems have been described. Taken together, these measures should provide protection commensurate with the threat to XMPP-Grid systems, thus ensuring that they fulfill their promise as a network security clearing-house.

9. Privacy Considerations

XMPP-Grid Platforms can publish information about endpoint health, network access, events (which can include information about what services an endpoint is accessing), roles and capabilities, and the identity of the end user operating the endpoint. Any of this published information can be queried by other XMPP-Grid Platforms and could potentially be used to correlate network activity to a particular end user.

Dynamic and static information brokered by an XMPP-Grid Controller, ostensibly for purposes of correlation by XMPP-Grid Platforms for intrusion detection, could be misused by a broader set of XMPP-Grid Platforms which hitherto have been performing specific roles with strict well-defined separation of duties.

Care needs to be taken by deployers of XMPP-Grid to ensure that the information published by XMPP-Grid Platforms does not violate agreements with end users or local and regional laws and regulations. This can be accomplished either by configuring XMPP-Grid Platforms to not publish certain information or by restricting access to sensitive data to trusted XMPP-Grid Platforms. That is, the easiest means to ensure privacy or protect sensitive data, is to omit or not share it at all.

Similarly, care must be taken by deployers and XMPP-Grid Controller implementations as they implement the appropriate auditing tools. In particular, any information, such as logs must be sensitive to the type of information stored to ensure that the information does not violate privacy and agreements with end users or local and regional laws and regulations.

Another consideration for deployers is to enable end-to-end encryption to ensure the data is protected from the data layer to data layer and thus protect it from the transport layer. The means to achieve end-to-end encrpytion is beyond the scope of this document.

10. Operations and Management Considerations

In order to facilitate the management of Providers and the onboarding of Consumers, it is helpful to generate the following ahead of time:

- o Agreement between the operators of Provider services and the implementers of Consumer software regarding identifiers for common

Topics (e.g., these could be registered with the XMPP Software Foundation's registry of well-known nodes for service discovery and publish-subscribe located at <https://xmpp.org/registrar/nodes.html>).

- Security certificates (including appropriate certificate chains) for Controllers, including identification of any Providers associated with the Controllers (which might be located at subdomains).

- Consistent and secure access control policies for publishing and subscribing to Topics.

These matters are out of scope for this document but ought to be addressed by the XMPP-Grid community.

11. Acknowledgements

The authors would like to acknowledge the contributions, authoring and/or editing of the following people: Joseph Salowey, Lisa Lorenzin, Clifford Kahn, Henk Birkholz, Jessica Fitzgerald-McKay, Steve Hanna, and Steve Venema. In addition, we want to thank Takeshi Takahashi, Panos Kampanakis, Adam Montville, Chris Inacio, and Dave Cridland for reviewing and providing valuable comments.

12. References

12.1. Normative References

[RFC2026] Bradner, S., "The Internet Standards Process -- Revision 3", BCP 9, RFC 2026, DOI 10.17487/RFC2026, October 1996, <https://www.rfc-editor.org/info/rfc2026>.

[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>.

[RFC3923] Saint-Andre, P., "End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP)", RFC 3923, DOI 10.17487/RFC3923, October 2004, <https://www.rfc-editor.org/info/rfc3923>.

[RFC4422] Melnikov, A., Ed. and K. Zeilenga, Ed., "Simple Authentication and Security Layer (SASL)", RFC 4422, DOI 10.17487/RFC4422, June 2006, <https://www.rfc-editor.org/info/rfc4422>.

[RFC5802] Newman, C., Menon-Sen, A., Melnikov, A., and N. Williams, "Salted Challenge Response Authentication Mechanism (SCRAM) SASL and GSS-API Mechanisms", RFC 5802, DOI 10.17487/RFC5802, July 2010, <https://www.rfc-editor.org/info/rfc5802>.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, DOI 10.17487/RFC6120, March 2011, <https://www.rfc-editor.org/info/rfc6120>.

[RFC6121] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence", RFC 6121, DOI 10.17487/RFC6121, March 2011, <https://www.rfc-editor.org/info/rfc6121>.

[RFC7590] Saint-Andre, P. and T. Alkemade, "Use of Transport Layer Security (TLS) in the Extensible Messaging and Presence Protocol (XMPP)", RFC 7590, DOI 10.17487/RFC7590, June 2015, <https://www.rfc-editor.org/info/rfc7590>.

[RFC7677] Hansen, T., "SCRAM-SHA-256 and SCRAM-SHA-256-PLUS Simple Authentication and Security Layer (SASL) Mechanisms", RFC 7677, DOI 10.17487/RFC7677, November 2015, <https://www.rfc-editor.org/info/rfc7677>.

[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>.

[XEP-0004] Eatmon, R., Hildebrand, J., Miller, J., Muldowney, T., and P. Saint-Andre, "Data Forms", XSF XEP 0004, August 2007.

[XEP-0030] Hildebrand, J., Millard, P., Eatmon, R., and P. Saint-Andre, "Service Discovery", XSF XEP 0030, July 2010.

[XEP-0059] Paterson, I., Saint-Andre, P., Mercier, V., and J. Seguineau, "Result Set Management", XSF XEP 0059, September 2006.

[XEP-0060] Millard, P., Saint-Andre, P., and R. Meijer, "Publish-Subscribe", XSF XEP 0060, December 2017.

[XEP-0203]
Saint-Andre, P., "Delayed Delivery", XSF XEP 0203, December 2009.

[XEP-0384]
Straub, A., "Publish-Subscribe", XSF XEP 0384, July 2018.

12.2. Informative References

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, DOI 10.17487/RFC2131, March 1997, <https://www.rfc-editor.org/info/rfc2131>.

[RFC6962] Laurie, B., Langley, A., and E. Kasper, "Certificate Transparency", RFC 6962, DOI 10.17487/RFC6962, June 2013, <https://www.rfc-editor.org/info/rfc6962>.

[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>.

[RFC8274] Kampanakis, P. and M. Suzuki, "Incident Object Description Exchange Format Usage Guidance", RFC 8274, DOI 10.17487/RFC8274, November 2017, <https://www.rfc-editor.org/info/rfc8274>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[XEP-0160]
Saint-Andre, P., "Publish-Subscribe", XSF XEP 0160, October 2016.

Authors' Addresses

Nancy Cam-Winget (editor)
Cisco Systems
3550 Cisco Way
San Jose, CA 95134
USA

Email: ncamwing@cisco.com

Syam Appala
Cisco Systems
3550 Cisco Way
San Jose, CA 95134
USA

Email: syam1@cisco.com

Scott Pope
Cisco Systems
5400 Meadows Road
Suite 300
Lake Oswego, OR 97035
USA

Email: scottp@cisco.com

Peter Saint-Andre
Mozilla

Email: stpeter@mozilla.com