draft-ietf-mile-rfc5070-bis-13

Roman Danyliw <rdd@cert.org>

MILE Interim Meeting

June 23, 2015

What is IODEFv2?

- An XML format to represent data elements commonly exchanged by CSIRTs:
  - Computer security incident reports
  - Cyber security indicators
- IODEFv2 is an update to the Incident Object Description Exchange Format (IODEF)/RFC5070
- IODEF is extended by various extensions
  - RFC 5901 (Phishing)
  - RFC 7203 (Structured Cybersecurity Information)
  - draft-murillo-mile-cps-00 (Cyber Physical Incidents)
  - draft-schaad-mile-iodef-plasma-00 (Policy Framework)
  - draft-suzuki-mile-darknet-00 (Darknet Monitoring)
- IODEFv2 is exchanged with RID (RFC 6545) and ROILE (draft-field-mile-rolie)

Drafts Since IETF 92 (Dallas)

- -12 (06-18-2015)
- -13 (06-20-2015)

Issues Closed in -12 and -13

ID	Issue Summary	Status
#47	Clarify definition of iodef:SoftwareType	-13
#48	Disambiguating private enumerated attribute extensions	-12
#49	Clarify the uniqueness of the @translation-id scope	-12
#50	Provide support for "bulk observables"	-12
#51	Distinguish between protocol and port number	-12
#52	Flexibility in the rates expressed in Counter	-12
#53	Add and instance of iodef:SoftwareType to File	-12
#1	Fix internationalization	Revisited in -12

http://trac.tools.ietf.org/wg/mile/trac/report/1?asc=1&sort=ticket

Incompatibilities with v1

- IODEF-Document@version="1.00" → "2.00"
- Service@ip_protocol → @ip-protocol
- Node/Name → Node/DomainData/Name
- Node/DataTime → Node/DomainData/DateTime
- NodeRole moved to System (from Node)
- Reference class is now defined by draft-ietf-mile-enum-reference-format-11
- Impact v1 class is now SystemImpact and IncidentCategory classes
- Extending ENUM attribute with IANA registries too
- All iodef:MLStringType classes use xml:lang; all @lang attributes now xml:lang
- Counter@type → Counter@unit (there is still a @type)
- IODEF-Document@formatid → @format-id

Issue #47: Clarify `iodef:SoftwareType`

- Redefined `iodef:SoftwareType`
- Support external structured (e.g., SWID, CPE) and free-form approaches (e.g., text, URL) to reference software

```
<Application>
  <SoftwareReference spec-name="swid">
      [insert SWID XML here]
  </SoftwareReference>
</Application>
```

```
<Application>
  <SoftwareReference spec-name="cpe">
      [insert CPE XML here]
  </SoftwareReference>
</Application>
```

```
<Application>
  <SoftwareReference spec-name="custom"
                     dtype="string">
      [some text blog]
  </SoftwareReference>
</Application>
```

Issue #48: Identifying Private Extensions

- Added `IODEF-Document@private-enum-name` and `@private-enum-id`
- Uniquely identify source of private extensions

```
<IODEF-Document
      version="2.00"
      private-enum-name="cert.org"
...>
...
  <NodeRole category="ext-value"
            ext-category="my-value1"
...
```

```
<IODEF-Document
      version="2.00"
      private-enum-name="cert.org"
      private-enum-id="3932"
...>
...
  <NodeRole category="ext-value"
            ext-category="my-value1"
...
```

Issue #50: List of Indicators

- Added `Observable/BulkObservable`
- Enumerate a list of commonly shared indicators

```
<BulkObservable type="fqdn">
  <BulkObservableList>
Foo.example.com
Bar.example.com
Moon.example.com
...
</BulkObservableList>
</BulkObservable>
```

Issue #51: Identifying the Service

- Added `Service/ServiceName`
- Distinguish between observed port and the service running on that port

```
<Service ip-protocol="6">
  <ServiceName>http</ServiceName>
  <Port>39182</Port>
   ...
</Service>
```

Issue #52: Expressing a Rate in `Counter`

- Updated `Counter@{type, unit}`
- Express peak and average rates (i.e., rates that are not simple counts)

Count of 384923 packets

```
<Counter type="count"
         unit="packet">
384923
</Counter>
```

Peak rate of 293 Mbps

```
<Counter type="peak"
         unit="mbit"
         duration="second">
293
</Counter>
```

Other Changes

- Corrected schema to add `xml:lang` into IODEF-Document and MLStringType (per ML, http://mailarchive.ietf.org/arch/msg/mile/KyBng_nav6xMvXtLEBwjt8HP-sE)

Outstanding Issues

ID	Issue Summary	Status
#39	RelatedDNS documentation	
#46	Missing data elements from NIST SP800-61 and CERT's Handbook for CSIRTs	6 of 7
#54	Reorganize IODEF schema	
#38	Improve example in Section 7	

+ Various editorial changes to clean up the text and schema

http://trac.tools.ietf.org/wg/mile/trac/report/1?asc=1&sort=ticket

Issue #39: RelatedDNS

- Problem: RelatedDNS is underspecified
  - http://trac.tools.ietf.org/wg/mile/trac/ticket/39
- Previously Discussed Options:
  1. Use draft-hoffman-dns-in-json-02, a JSON representation
  2. A comma separated value list of DNS fields
  3. Defining RelatedDNS as iodef:AdditionalData and requiring an extension
  4. Define an alternative representation for RelatedDNS

Prior Discussion: http://www.ietf.org/mail-archive/web/mile/current/msg01637.html

Issue #46: Cause of the incident?

- Problem: 5070bis doesn't specify the cause of the incident
  - http://trac.tools.ietf.org/wg/mile/trac/ticket/46

- Question
  - Is `iodef-sci:Weakness` sufficient?

Discussion