

draft-ietf-mile-rfc5070-bis-18

Roman Danyliw <rdd@cert.org>

IETF 95

April 5, 2016

What is IODEFv2?

- An XML format to represent data elements commonly exchanged by CSIRTs:
 - Computer security incident reports
 - Cyber security indicators
- Update to the Incident Object Description Exchange Format (IODEF) (RFC5070)
- IODEF is extended by various extensions
 - RFC 5901 (Phishing)
 - RFC 7203 (Structured Cybersecurity Information)
 - RFC 7495 (Reference format)
- IODEFv2 is exchanged with:
 - RID (RFC 6545 and RFC 6546)
 - XMPP (draft-appala-mile-grid-00)

Drafts Since IETF 94 (Yokohama)

- **-16 (02-01-2016)**
 - <https://www.ietf.org/mail-archive/web/mile/current/msg01800.html>
- **-17 (03-20-2016)**
 - <https://www.ietf.org/mail-archive/web/mile/current/msg01811.html>
- **-18 (03-21-2016)**
 - <https://www.ietf.org/mail-archive/web/mile/current/msg01813.html>
- **WGLC started on October 2015**

Issues Closed in -16, -17 and -18

ID	Issue Summary	Status
#38	Improve example in Section 7	-16
#39	RelatedDNS documentation	-16
#54	Reorganize IODEF schema	-16
WGLC Feedback 1	David Waltermire https://www.ietf.org/mail-archive/web/mile/current/msg01775.html	-16, -17
WGLC Feedback 2	Alexey Melnikov https://www.ietf.org/mail-archive/web/mile/current/msg01802.html	-17
WGLC Feedback 3	Takeshi Takahashi https://www.ietf.org/mail-archive/web/mile/current/msg01804.html	-18

- Substantial editorial changes

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

Incompatibilities with v1

- The IODEF-Document@version attribute is set to "2.0".
- Attributes with enumerated values can now also be extended with IANA registries.
- All iodef:MLStringType classes use xml:lang. IODEF-Document also uses xml:lang.
- The Service@ip_protocol attribute was renamed to @ip-protocol.
- The Node/NodeName class was removed in favor of representing domain names with Node/DomainData/Name class. The Node/DataTime class was also removed so that the Node/DomainData/ DateDomainWasChecked class can represent the time at which the name to address resolution occurred.
- The Node/NodeRole class was moved to System/NodeRole.
- The Reference class is now defined by [RFC-ENUM].
- The data previously represented in the Impact class is now in the SystemImpact and IncidentCategory classes. The Impact class has been removed.
- The semantics of Counter@type are now represented in Counter@unit.
- The IODEF-Document@formatid attribute has been renamed to @format-id.
- Incident/ReportTime is no longer mandatory. However, GenerationTime is.
- **The Fax class was removed and is now represented by a generic Telephone class.**
- **The Telephone, Email and PostalAddress classes were redefined from improved internationalization.**

Reorganized UML Datatypes

- Introduced SOFTWARE and EXTENSION data types

```
+-----+
| iodef:SoftwareType |
+-----+
|                               |<--{0..1}--[ SoftwareReference ]
|                               |<--{0..*}--[ URL ]
|                               |<--{0..*}--[ Description ]
+-----+
```

```
+-----+
| iodef:ExtensionType |
+-----+
| xs:any |
|       |
| STRING name |
| ENUM dtype |
| STRING ext-dtype |
| STRING meaning |
| STRING formatid |
| ENUM restriction |
| STRING ext-restriction |
| ID observable-id |
+-----+
```

EXTENSION type now used by AdditionalData, RecordItem, FileProperties, RelatedDNS, ApplicationHeaderField and EmailHeaderField

SOFTWARE type now used by Application, OperatingSystem and AssociatedSoftware

Outstanding Issues



[IETF Home](#)
[About Tools](#)
Tools:
[diffs](#) [spell](#)
[xml2rfc](#) [idnits](#)
[tracker_src](#)
[News](#)
[Get Passwd](#)
IETF-95:
[Rooms](#)
[Agenda](#)
[Calendar](#)
[Documents](#)
[RFCs](#)
Doc fetch:

Wikis:
[IESG](#) [IRTF](#)

mile

logged in as rdd@cert.org | [Logout](#) | [About Trac](#) | [Preferences](#) | [Help/Guide](#)

[Wiki](#) | [Timeline](#) | [Roadmap](#) | [Browse Source](#) | **View Tickets** | [New Ticket](#) | [Search](#)

[Available Reports](#) | [Custom Query](#)

{1} Active Tickets

- List all active tickets by priority.
- Color each row based on priority.

No matches found.

Note: See [TracReports](#) for help on using and creating reports.

Download in other formats:
[RSS Feed](#) | [Comma-delimited Text](#) | [Tab-delimited Text](#) | [SQL Query](#)

 Powered by [Trac 0.12.5](#)
By Edgewall Software

Administered by webmaster@tools.ietf.org

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

Discussion