draft-ietf-mile-rfc5070-bis-25

Roman Danyliw <rdd@cert.org>

IETF 96

July 21, 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)

- Currently in “AD Followup” state; 1 uncleared Discuss

Drafts Since IETF 95 (Buenos Aires)

- Nits from WGLC
  -19 (04-21-2016)
- AD Review
  -20 (05-09-2016)
    - https://www.ietf.org/mail-archive/web/mile/current/msg01847.html
- Shepherd Write-up and draft-ietf-mile-iodef-guidance-05 feedback
  -21 (05-10-2016)
    - https://www.ietf.org/mail-archive/web/mile/current/msg01851.html
  -22 (05-27-2016)
    - https://www.ietf.org/mail-archive/web/mile/current/msg01867.html
- IETF LC, Security Review and IESG Review
  -23 (06-20-2016)
    - https://www.ietf.org/mail-archive/web/mile/current/msg01932.html
  -24 (06-20-2016)
    - https://www.ietf.org/mail-archive/web/mile/current/msg01944.html
  -25 (06-24-2016)
    - https://www.ietf.org/mail-archive/web/mile/current/msg01961.html

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.

Obsoleting and Expert Review

- Explicitly deprecate RFC5070 and RFC6685
- Require expert review on IANA registered namespaces containing the string “iodef” per RFC6685

Processing IODEF Documents

- Parsers s/MUST/SHOULD/ reject syntax errors
- Parsers s/SHOULD NOT/MUST NOT/ download schemas at runtime
- IODEF implementations MUST periodically update their schema and MAY need to update their parsing algorithms to incorporate newly registered values

Security Considerations

- Discuss privacy implications of IODEF
- Clarify where executable content exists in the data model
- Clarify out-of-band negotiation of field semantics
- Clarify the interpretation of confidence values

Added new attribute/classes

- System@observable-id and Observable/System per use cases in Section 4 of draft-ietf-mile-iodef-guidance-05
- Address@type={ipv4-net-masked, ipv6-net-masked}
- IndicatorExpression/Confidence

Discussion