draft-ietf-mile-rfc5070-bis-07

Roman Danyliw <rdd@cert.org>

IETF 90

July 23, 2014

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 89 (London)

- -07 (2014-04-21)
  - *Temporary location:*

    https://github.com/rdanyliw/iodef-spec/blob/draft-ietf-mile-rfc5070-bis-07/draft-ietf-mile-rfc5070-bis.txt
  - *CHANGELOG*:

    http://www.ietf.org/mail-archive/web/mile/current/msg01487.html

Issues closed in -07

#2	Add better reference (citation) to RecordPattern@type=regex	-07	2013-06-14
#14	Add predicate logic for indicators	-07	2013-07-27
#17	Review completeness of Incident@purpose	No Action	2013-07-28
#28	Describe the time window during which an indicator should be used	-07	2013-08-29
#41	@indicator-* attribute documentation	-07	2014-02-26
#42	Attributes with "-watchlist" values documentation	-07	2014-02-26

Incident Report

```
<IODEF-Document>
  <Incident>
     <EventData>
      {incident report}
     </EventData>
</Incident>
</IODEF-Document>
```

Incident Report + Indicators

```
<IODEF-Document>
  <Incident>
     <EventData>
      {incident report}
      +/- {observables}
     </EventData>
     <IndicatorData>
      {indicators}
     </IndicatorData>
  </Incident>
</IODEF-Document>
```

Indicator List

```
<IODEF-Document>
  <Incident>
     <IndicatorData>
      {indicators}
     </IndicatorData>
  </Incident>
</IODEF-Document>
```

Outstanding Issues

#1	Fix internationalization	VOLUNTEER	2013-06-14
#3	Review implementation of extending enumerated values	VOLUNTEER	2013-06-14
#6	Harmonize the specification for Reference with other WG activity	WG ACTION	2013-06-14
#10	Review completeness of Impact@type	ON LIST	2013-06-14
#12	Define clear scope for the core data model relative to other WG documents	WG ACTION	2013-06-14
#20	Review how to provide a list of file and email indicators	TODO	2013-08-21
#25	Clarify what type attribute of HashInformation should be used to represent a TLS certificate	ON LIST	2013-08-29
#29	Clarifying the scope of HashInformation@valid	ON LIST	2013-08-29
#37	Add intended purpose of attack to Assessment	TODO	2013-10-16
#38	Improve example in Section 7	TODO	2014-01-08
#39	RelatedDNS documentation	PROPOSAL	2014-02-26
#40	Reference@attacktype documentation	TODO	2014-02-26
#43	{Application,OperatingSystem}@user-agent documentation	ON LIST	2014-02-26
#44	HashData/{ds:Signature,ds:KeyInfo,ds:KeyReference} documentation	ON LIST	2014-02-26
#45	Clarifying the computation of a file and email hash	-08	2014-02-27
#46	Missing data elements from NIST SP800-61 and CERT's Handbook for CSIRTs	TODO	2014-02-27

All post-IETF-87 survey items but Issue 37 are complete

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

Discussion