draft-ietf-mile-rfc5070-bis-06

Roman Danyliw <rdd@cert.org>

IETF 89

March 7, 2014

Drafts Since IETF 87 (Berlin)

- -01 -- 2013-08-29
  - http://www.ietf.org/mail-archive/web/mile/current/msg01185.html
- -02 -- 2013-10-20
  - http://www.ietf.org/mail-archive/web/mile/current/msg01223.html
- -03 -- 2014-01-08
  - http://www.ietf.org/mail-archive/web/mile/current/msg01267.html
- -04 -- 2014-01-18
  - http://www.ietf.org/mail-archive/web/mile/current/msg01296.html
- -05 -- 2014-01-31
  - http://www.ietf.org/mail-archive/web/mile/current/msg01345.html
- -06 -- 2014-02-14
  - http://www.ietf.org/mail-archive/web/mile/current/msg01369.html

ULRs reference the relevant Changelog

Results of post-IETF-87 Survey

- Discussion #1: Cyber Intelligence
  - ~~Issue #22: Describing actors and tactics~~ (-02,-05)
  - ~~Issue #23: Extension point for file info~~ (-05)
  - ~~Issue #24: Arbitrary email headers~~ (-05)
  - Issue #25: Representing a TLS certificate
  - ~~Issue #26: Arbitrary layer-7 headers~~ (-05)
  - ~~Issue #27: Describing a IDS/HIDS signature~~ (-06)
- Discussion #2: Indicator IDs and RelatedActivity
  - ~~Issue #30: Add @indicator-uid to DomainData~~ (-03)
  - ~~Issue #31: Expand RelatedData~~ (-02)
  - Issue #28: Define a time window for an indicator
  - Issue #41: @indicator-* documentation

Results of post-IETF-87 Survey (2)

- Discussion #3: Cyber Incident Reporting
  - ~~Issue #11: Geolocation of a Node~~ (-04)
  - ~~Issue #32: Courses of Action~~ (-04)
  - ~~Issue #32: Ownership information in System~~ (-02)
  - ~~Issue #33: Asset identifier to System~~ (-02)
  - ~~Issue #34: Title added to Contact~~ (-02)
  - ~~Issue #36: Business impact~~ (-05)
  - Issue #37: Intended purpose of the attack
- Discussion #4: Workflow
  - No action

Other Changes

- Issue #7: Updated NodeRole@category
- Issue #8: Updated HistoryItem@action
- Issue #9: Updated @restriction
- Issue #10: Corrected RFC2119 language
- Issue #15: Removed ReportID
- Issue #16 Add support for describing if a device is physical or virtual
- Issue #19 Scope statement in Section 1.0
- Ensure all element and attribute names follow convention; are consistency defined between text and schema; all attributes are extensible; and all text has a data type
- Consistent application of @indicator-*
- Added IODEF-Document/AdditionalData
- Removed Service/{Email,EmailSubject, X-Mailer}
- Renamed Service@ip_protocol to @ip-protocol
- Added System@virtual
- Added values to Expectation@action, Contact@role, AdditionalData@dtype

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

- Future Work
  - Reference class to be defined as draft-ietf-mile-enum-reference-format-03

Issue Status

#1	Fix internationaliztion	VOLUNTEER	2013-06-14
#2	Add better reference (citation) to RecordPattern@type=regex	ON LIST	2013-06-14
#3	Review implementation of extending enumerated values	TODO	2013-06-14
#6	Harmonize the specification for Reference with other WG activity	WG ACTION	2013-06-14
#10	Review completeness of Impact@type	TODO	2013-06-14
#12	Define clear scope for the core data model relative to other WG documents	WG ACTION	2013-06-14
#14	Add predicate logic for indicators	PROPOSAL	2013-07-27
#17	Review completeness of Incident@purpose	ON LIST	2013-07-28
#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
#28	Describe the time window during which an indicator should be used	2 PROPOSALS	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
#41	@indicator-* attribute documentation	PROPOSAL	2014-02-26
#42	Attributes with "-watchlist" values documentation	PROPOSAL	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	ON LIST	2014-02-27

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

Untracked Discussions

- Computer email and file hashes
  - http://www.ietf.org/mail-archive/web/mile/current/msg01374.html
- Missing data for incident reporting
  - http://www.ietf.org/mail-archive/web/mile/current/msg01377.html
- Others?

Discussion