IODEF-extension to support structured cybersecurity information

draft-ietf-mile-sci-02.txt

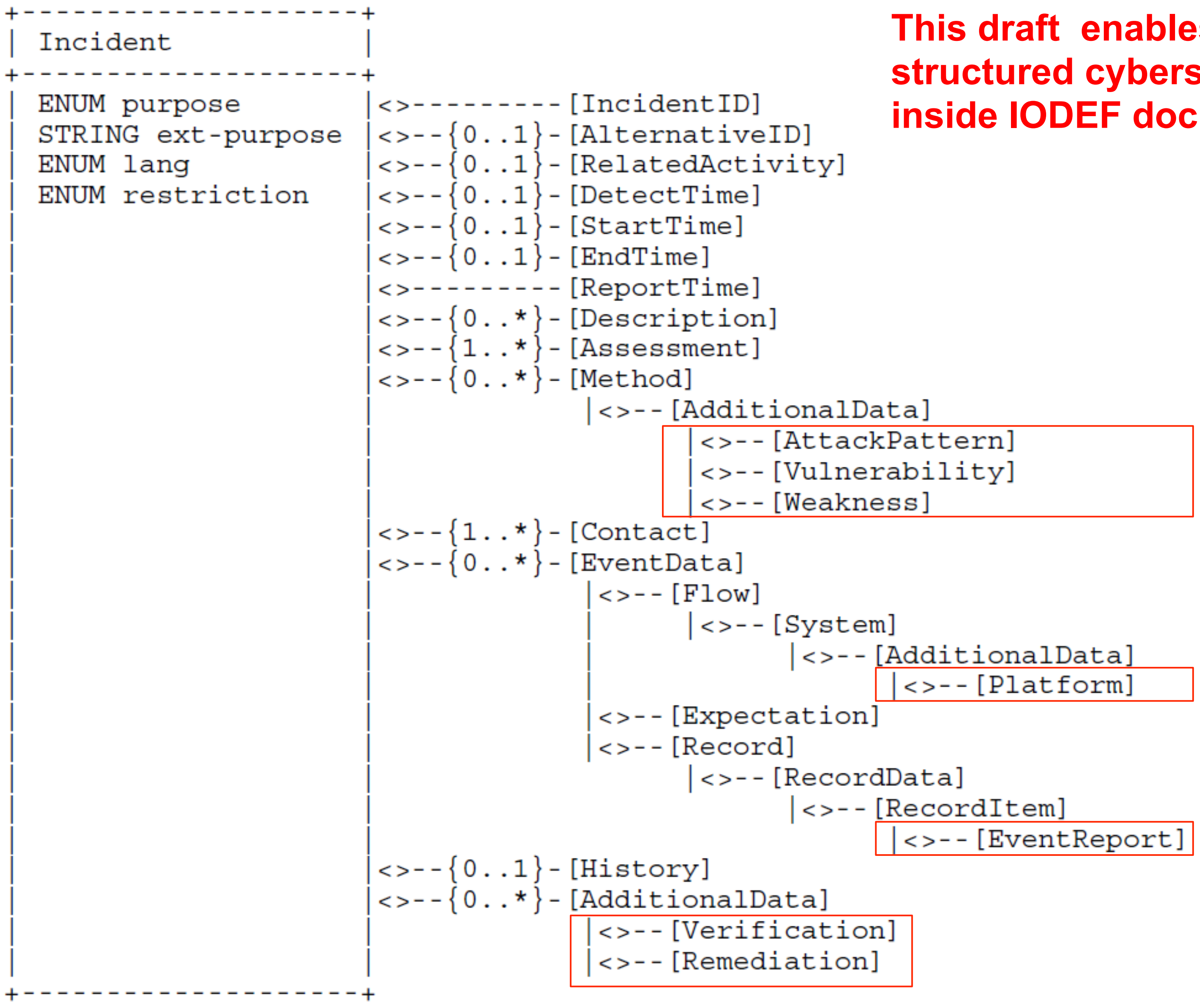
Takeshi Takahashi (NICT), Kent Landfield (McAfee),
Thomas Millar (US-CERT), Youki Kadobayashi (WIDE/NAIST)

Agenda

- Brief Overview of the extension

- Discussion issues

Brief overview of the draft



```
+--------------------+
| Incident           |
+--------------------+
| ENUM purpose       |<>---------[IncidentID]
| STRING ext-purpose |<>--{0..1}-[AlternativeID]
| ENUM lang          |<>--{0..1}-[RelatedActivity]
| ENUM restriction   |<>--{0..1}-[DetectTime]
|                    |<>--{0..1}-[StartTime]
|                    |<>--{0..1}-[EndTime]
|                    |<>---------[ReportTime]
|                    |<>--{0..*}-[Description]
|                    |<>--{1..*}-[Assessment]
|                    |<>--{0..*}-[Method]
|                    |            |<>--[AdditionalData]
|                    |                  |<>--[AttackPattern]
|                    |                  |<>--[Vulnerability]
|                    |                  |<>--[Weakness]
|                    |<>--{1..*}-[Contact]
|                    |<>--{0..*}-[EventData]
|                    |            |<>--[Flow]
|                    |            |     |<>--[System]
|                    |            |           |<>--[AdditionalData]
|                    |            |                 |<>--[Platform]
|                    |            |<>--[Expectation]
|                    |            |<>--[Record]
|                    |                  |<>--[RecordData]
|                    |                        |<>--[RecordItem]
|                    |                              |<>--[EventReport]
|                    |<>--{0..1}-[History]
|                    |<>--{0..*}-[AdditionalData]
|                    |            |<>--[Verification]
|                    |            |<>--[Remediation]
+--------------------+
```

This draft enables embedding structured cybersecurity information inside IODEF document

The draft uses IANA registry to maintain the list of cybersecurity information formats

Namespace	Specification Name	Ver.	Reference URI	Applicable classes
http://capec.mitre.org/observables	Common Attack Pattern Enumeration and Classification	1.6	http://capec.mitre.org/	AttackPattern
http://cce.mitre.org	Common Configuration Enumeration	5.0	http://cce.mitre.org/	Verification
http://cee.mitre.org	Common Event Expression	0.6	http://cee.mitre.org/	EventReport
http://cpe.mitre.org/dictionary/2.0	Common Platform Enumeration	2.3	http://scap.nist.gov/specifications/cpe/, http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7695	Platform
http://cve.mitre.org/cve/downloads/1.0	Common Vulnerability and Exposures	1.0	http://cve.mitre.org/	Vulnerability

Agenda

- Brief Overview of the extension

- Discussion issues

Discussion Issues that need to be confirmed

- MTI 1

- References to specifications 2

MTI issue

Issue

The draft needs to clarify what is mandatory to implement for implementers

Direction

1. The CVE SpecID value and related values (e.g., namespace) MUST be implemented (implementation is capable of sending and receiving well-formed CVE 1.0 XML documents without error)

2. The receiver MUST implement validation of received CVE 1.0 XML documents against the CVE 1.0 XML schema in order to detect invalid CVE documents

3. The receiver SHOULD validate all received CVE 1.0 XML documents as described in item #2

References to specifications

Issue

What resource is appropriate for the "Specification URI" field?

Web resource is subject to change. Then would it be enough?

Direction

1. Change the name from "Specification URI" into "Reference URI"
2. Multiple URIs could be embedded in the "Reference URI" field
3. Informational/Standard RFCs describing the specifications are recommended
4. As a reference, web URL could be used for the field: including the URL specifying the specification itself and the URL specifying its schema

Thank you