IODEF Data Model Status

<draft-ietf-inch-iodef-03>

tracked @ https://rt.psg.com : inch-dm queue

Roman Danyliw <rdd@cert.org>

Thursday, August 5. 2004

IETF 60, San Diego, USA

Summary of Work

1. Closed: No Action
   - Timestamps
   - Extension class typing
2. Closed: Adding to Draft
   - XML Schema, XML-Sig
   - Extension meta data
   - Simplified Representation
3. Open Issues
   - Flow support
   - Assigning IDs
   - Formalizing log data
4. Ok to add, but blocking on discussion
   - AS Number support

Summary of Work

1. Resolved -- No change required
2. Resolved -- Added to Draft
3. Open Issues
4. Ok to add, but blocking on discussion

#363: Timestamp formats

https://rt.psg.com/Ticket/Display.html?id=363

- Support more commonly used time formats
  - time-zones formats other than GMT+004, including day of the week, etc.

- STATUS: Closed
  - Properties of the date can be easily discerned mechanically from the existing UTC format.

#362: Unify type attribute of extensions

https://rt.psg.com/Ticket/Display.html?id=362

- Should the type attribute of the extension classes (i.e., AdditionalData, and Record Item) be identical?

- PROPOSALS
  - Since the enum list for RecordItem is a superset of AdditionalData, use the same for both
  - Since the classes represent different data, keep the attribute definitions different

- STATUS: Closed
  - These are semantically different – no change

Summary of Work

1. Resolved – No change required
2. Resolved -- Added to Draft
3. Open Issues
4. Ok to add, but blocking on discussion

#365: XML Schema Migration

https://rt.psg.com/Ticket/Display.html?id=365

http://www.uazone.org/demch/projects/iodef/

- Convert DTD to Schema

- STATUS
  - Release a DTD and Schema in v03 draft
  - v04 with full Schema

#364: XML-Sig and Encryption

https://rt.psg.com/Ticket/Display.html?id=364

- How to apply XML-Signature and XML-Encryption to IODEF documents?
- PROPOSAL
  - Examples of using XML-Signature
  - http://nic.surfnet.nl/scripts/wa.exe?A2=ind04&L=inch&F=&S=&P=2459
- STATUS:
  - Clearly will be used, but solution requires evaluation

#356: Standardize extensions

https://rt.psg.com/Ticket/Display.html?id=356

- Add a mandatory top-level container class to all extensions to allow an easy determination of which one is used
- PROPOSAL

```
<!ELEMENT IODEF-Extention (ANY)>
<!ATTLIST IODEF-Extention
          name     CDATA    #REQUIRED
          source   CDATA    #REQUIRED
          version  CDATA    #IMPLIED >
```

- STATUS:
  - Included in v03

#472: Representation Complex

https://rt.psg.com/Ticket/Display.html?id=472

- System class is too IDS/IDMEF centric and overly complex
- PROPOSAL
  - Create a more flow (i.e., communication between machines) view of the incidents
  - Drop <Process>, <FileList>, and <User> from <System>
  - Simplify <Address> to only IP addresses
- STATUS: proceeding with changes, last chance to comment

#472: Complexity (2)

- Information to drop:
  - Layer 7 (application) protocols fields
    - <SNMPService> and <HTTPService>
  - Running process at end-points
    - <Process>
  - Filesystem information at end-points (e.g., inodes)
    - <FileList>
  - Explicit netmask of an IP address (deal in CIDR blocks, IPs)
  - Merge <IncidentData> into <Incident> ** (consensus?)
- Information to Keep
  - User information at the end-point in <User>
  - All Layer-2 addresses
  - Non-IP Layer 3 protocols

Summary of Work

1. Resolved – No change required
2. Resolved -- Added to Draft
3. Open Issues
4. Ok to add, but blocking on discussion

#360: Flow Support

https://rt.psg.com/Ticket/Display.html?id=360

- Want a representation for:
  - flow data
  - statistics on these flows
- PROPOSAL
  - Add a way to represent stats via new <Counter>
  - Feedback has been not to over-engineer the solution: simple counts and summaries
  - http://nic.surfnet.nl/scripts/wa.exe?A2=ind04&L=inch&F=&S=&P=1576
- STATUS: proceeding with changes, comments?

#357: Assigning IncidentIDs

https://rt.psg.com/Ticket/Display.html?id=357

- How to assign incident identifiers?
- PROPOSALS
  - external registration, AS number, Domain name, Net handles
  - Interim Meeting: This is a policy problem solved by profiles?
- STATUS: further discussion needed

#551: Formalizing <RecordData>

https://rt.psg.com/Ticket/Display.html?id=551

- Add meta-information so that inlined logs snippets and those reference externally can be processed
- PROPOSALS
  - Add a way to specify filter patterns and offsets into text and binary log files
- STATUS: further discussion needed

Assorted Proposals

- Representing OS of <System>
- Representing Application providing <Service>
- <name> of <Node> not FQDN
- Formalize <Location> of <Node>
  - Specify country and timezone

Summary of Work

1. Resolved -- No change required
2. Resolved -- Added to Draft
3. Open Issues
4. Ok to add, but blocking on discussion

#359: Supporting AS Numbers

https://rt.psg.com/Ticket/Display.html?id=359

- Add AS numbers as another address type; needed for RID and providers
- STATUS: accepted, but contingent on any redesign (#360 already includes)

Moving Forward

- Release a v03 draft right after IETF 60 with
  - Schema support
  - Resolution to complexity and flow issues

Comments?