

IODEF update

TF-CSIRT 11, Madrid

Jan Meijer

`<jan.meijer@surfnet.nl>`

Jan. 16 2004



What is IODEF?

- Format for exchange of incident related data
- Development by the IETF-INCH wg with roots in the TF-CSIRT
- Used in eCSIRT.net, AirCERT, others underway (Japan, Korea, UK defense)

INCH status

- Requirements draft: WG last call soon now: can debate wording until the end of time ;)
- Datamodel draft: one major item left: xml-schema. Other small datamodel-nits. WG last call expected in march. Datamodel IS stable
- Usage-manual: no draft yet
- Interesting development: Kathleen Moriarty works on IODEF extension for DoS Handling

ICODEF, it works

- For a particular usage case
- Still (partly) experimental in eCSIRT.net but how to do it is known
- Operational in AirCERT but...CERT/CC controls all the end-points

ICODEF, how to use it

- You do not NEED to use every field in the datamodel
- The datamodel can hold 'anything', flexibility unfortunately gives ambiguity
- Follow the eCSIRT.net model: common language specifying which fields to use (profile) and define the exact semantics within your particular context
- Use it for initial reporting; still bits missing for total incident-lifecycle information exchange (meta-data)
- Current tools: AirCERT, LibIH, Greens Perl library, Helmes IHSH, work at JPCERT/CC

Activities

- Authoritative source for the eCSIRT.net IODEF profile and common language (maintenance)
- Implement an IODEF exchange protocol
- Offer support for the improvement of the current IODEF-exchange network (eCSIRT.net)
- Assist teams within the TF-CSIRT that want to join the IODEF-exchange network
- Promote the implementation of IODEF in other fora (presentations and other activities where and when appropriate)

Deliverables

- Working demo-bed for the exchange protocol
- Exchange protocol document
- HOWTO and FAQ for implementing IODEF in your operational environment and joining the IODEF-exchange network (TI)
- Standard webform package for reporting incidents that outputs IODEF
- 2 hr workshop on implementation (may, sep, ?)

Organisation

- Small (2/3 persons)
- Reporting to the TF-CSIRT (live at the meeting, email-report 1.5 weeks before the meeting)
- Announcements of cool things to the mailinglist

Where to look

Everything is/will be available on
<http://www.iodef.org/>

Proposal: (BIEN) Building Blocks for IODEF Exchange Network WG

The BIEN WG will concern itself with enabling the exchange of incident-related information between disparate incident handling systems of different CSIRTs in different administrative domains. The ultimate goal is to automate the exchange of incident-related information (data and meta-data) between incident handling systems as much as possible and at least terminate copy and paste by humans