

~~IODEF, it works~~ evaluation

Hamburg, 27 May 2004

Jan Meijer <jan.meijer@surfnet.nl>

Goal

The purpose of the Incident Data Exchange Format (IODEF) is to define data formats for information related to computer security incidents typically exchanged between collaborating Computer Security Incident Response Teams (CSIRTs).

- Define common data-format for incident-exchange
- Started 1999 within TF-CSIRT
- Continued in IETF as INCH since March 2002

Current usage

Very limited

- CERT/CC: stats gathering: production
- JPCERT/CC: incident reporting: development
- eCSIRT.net: incident reporting: experimental
- NOT in RTIR

Problem

IODEF usage is problematic, community pickup is minimal

- Datamodel complexity
 - used for many different problem spaces, linked by 'security incident related'
 - founding it on IDMEF adds to this
 - still unable to fully put current email content in easily
- Problems with implementation
 - no protocol for the workflow
 - no common notion of 'implementing iodef'

Moving forward

Do we want to?

Problem spaces:

- Incident handling data
- Statistics gathering
-

Option 1: continue on current path

- Contribute to INCH
- Continue to work on implementing IODEF
- Get IHS implementors and users to adapt their system and working methods to IODEF

Option 2: And now...

for something (completely) different: focus only on incident-handling data exchange within TF-CSIRT (TI)

Others may worry about the universe at large at this time

- Make usage in daily life possible: start with systems now available and data now available
- Incident handling protocol with very limited dataformat first, remember MPAA?
- Make it work; build on that, perhaps end up with IODEF but then implemented :)

So, what is BIEN to do?

Goal: Building blocks for an Incident-data Exchange Network, make life easier

- Continue on current IODEF path?
- Try something different?
- Nothing?
- Other?