IODEF Development

- What is it? (Incident Object Description and Exchange Format)
- History
- INCH is now a WG
- Requirements document revisited (Glenn Keeni, JPCERT/CC)
- datamodel doc: busy solving problems
- practical experience is needed!
- implementation: LIBIH (aircert, CERT/CC: http://aircert.sourceforge.net/)
- much interest from APCERTF
- eCSIRT.net is going to give lots of input :(
IODEF Pilot Project

- Aim: further the development of IODEF and implement it between Ukerna and CERT-NL
- Problems: IODEF is NOT an exchange protocol, it’s a format
- Making demonstrator: autoprobe-reporter a-la AusCERT
- Problem: IODEF not an exchange protocol