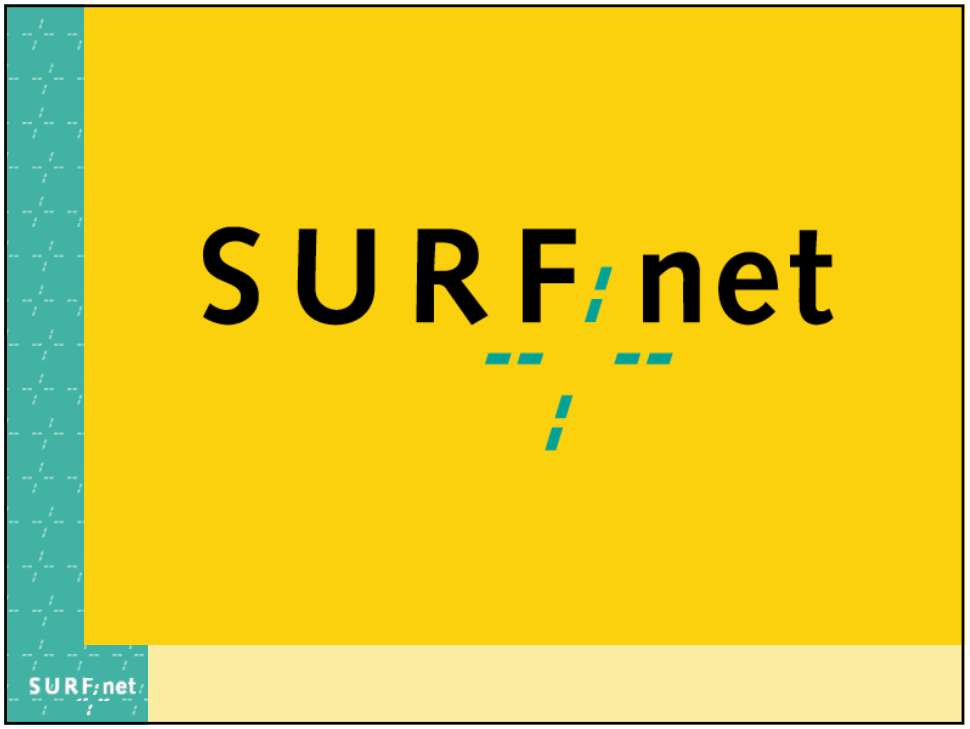


IODEF

Incident object description and exchange format

Developed within Terena's TF-CSIRT

This material is public :)

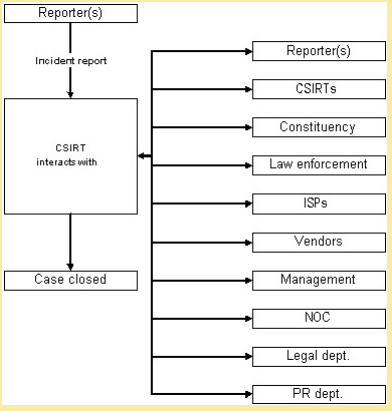
Jan Meijer <jan.meijer@surfnet.nl>

IODEF: what is it about?

Problem statement:

define a common data format for sharing information needed to handle an incident between different CSIRTs and to exchange incident related data between CSIRTs that allows both known and new types of incidents to be formatted and exchanged

Why is this needed?



And now the real, simple reason:

- Incident reporter *writes to*
- CSIRT A *writes to*
- CSIRT B *writes to*
- Constituent (attacker) *turnaround writes*

- **Lots of copy & paste**
- **Lots of rewriting of the same message**
- **Lots of effort in what you should not be doing**

SURFnet

Steps taken; short history

- BCP document on incident handling formats (june 2000)
- Requirements document (RFC 3067) (feb 2001)
- Datamodel and DTD (finalized last week, still buggy DTD though

Still to come (may 2002):
Management summary (why is iodef needed)
Users guide (what does this all mean)
Reality check (incident examples + xml)

SURFnet

Main requirements

- What, where, how, when, who
- Extensible
- Modular
- Internationalization
- Compatible with other standards, if feasable
- Access restriction to every element
- Degree of confidence
- Encrypt/sign

Datamodel: simple

- IODEF top level classes:
- Incident
  - **Attack**
  - ***Attacker***
  - ***Victim***
  - ***Method***
  - Evidence
  - **Assessment**
  - Authority
  - History
  - AdditionalData
  - CorrelationIncident

Datamodel: the whole monster

file://c:/Documents%20and%20Settings/meijer.ASFALT/My%20Documents/first-tc-london/draft-iodef-datamodel-005chart-final.gif

Example: original report

Naam aanmelder: Jan Meijer
E-mail adres aanmelder: jan.meijer@surfnet.nl
Organisatie aanmelder: SURFnet
Telefoonnr aanmelder: +31 302 305 305
Begin scan
(dd/mm/yy:hh:mm): 12/12/2001:9:54
Einde scan
(dd/mm/yy:hh:mm): 12/12/2001:11:42
Gescande machine(s): 192.87.108/24
Scannende machine: 193.62.83.151
Timezone: GMT +0100
Type probe/scan: slow ssh scan
Logfile: Dec 12 09:54:20 surroute.surfnet.nl 2506524: Dec 12 09:54:19: %SEC-6-IPACCESSLOGP: list 110 denied tcp 193.62.83.151(20) -> 192.87.108.50(22), 1 packet
Dec 12 09:56:32 surroute.surfnet.nl 2506605: Dec 12 09:56:31: %SEC-6-IPACCESSLOGP: list 110 denied tcp 193.62.83.151(20) -> 192.87.108.52(22), 1 packet
Dec 12 09:58:50 surroute.surfnet.nl 2506699: Dec 12 09:58:49: %SEC-6-IPACCESSLOGP: list 110 denied tcp 193.62.83.151(20) -> 192.87.108.54(22), 1 packet
Dec 12 10:13:08 surroute.surfnet.nl 2507231: Dec 12 10:13:07: %SEC-6-IPACCESSLOGP: list 110 denied tcp 193.62.83.151(20) -> 192.87.108.69(22), 1 packet
Dec 12 10:19:50 surroute.surfnet.nl 2507475: Dec 12 10:19:49: %SEC-6-IPACCESSLOGP: list 110 denied tcp 193.62.83.151(20) -> 192.87.108.75(22), Dec 12 11:32:44 surroute.surfnet.nl 2509981: Dec 12 11:32:43: %SEC-6-IPACCESSLOGP: list 111 denied tcp 193.62.83.151(20) -> 192.87.108.149(22), 1 packet
Dec 12 11:35:49 surroute.surfnet.nl 2510088: Dec 12 11:35:48: %SEC-6-IPACCESSLOGP: list 111 denied tcp 193.62.83.151(20) -> 192.87.108.152(22), 1 packet
Dec 12 11:42:49 surroute.surfnet.nl 2510285: Dec 12 11:42:48: %SEC-6-IPACCESSLOGP: list 111 denied tcp 193.62.83.151(20) -> 192.87.108.158(22), 1 packet

Example: XML

Is it:

- Perfect?
- Too complex?
- Usable?
- Used?
- Still under development?

Continuing development: IETF-INCH

- Version 2
- IETF WG
- http://www.terena.nl/inch/
- Terena Pilot Implementation Project

Terena Pilot Implementation project

- SURFnet (CERT-NL), Terena, Ukerna (JANET-CERT)
- Not an incident handling system
- Proof of concept
- Development of libiodef
- Want some schematics?

Future?

- The train is travelling at high speed
- Keep close watch, give real life input
- Validate!
- Lets make it simpler!
- Contribute@IETF
- Don’t let vendors/developers alone run it

SURFnet

URLS

- http://www.terena.nl/tf-csirt/iodef
- http://www.terena.nl/inch
- http://www.surfnetters.nl/meijer/ipp/
- http://www.terena.nl/tf-csirt/

SURFnet

Thank you |)