

JRA2 WI3

Operational Requirements

Claudio Allocchio

WI3 - Main Goals

- ❑ agree on a common set of severity classification of incidents;
- ❑ agree on response actions and response time for incidents;
- ❑ exchange electronic credentials;
- ❑ agree on a minimal format for incident information exchange;
- ❑ establish a common trouble ticket systems, or to be more realistic, make the existing TTSs interwork easily, with minimal human intervention;
- ❑ deploy and pilot in test-operational environment the set of tools developed by WI2;
- ❑ agree/disagree on how to handle IPR related incidents;

JRA2-WI3 Pilot phase 1

- IUCC, IL
- RENATER, FR
- HUNGARNET, HU
- ISTF, RO
- DANTE, EU
- GARR, IT
- REDIRIS, ES
- GRNET, GR
- SURFNET, NL
- SWITCH, CH

JRA2-WI3 Pilot phase 2 (Sep 2005)

- IUCC, IL
- RENATER, FR
- HUNGARNET, HU
- ISTF, RO
- DANTE, EU
- GARR, IT
- REDIRIS, ES
- GRNET, GR
- SURFNET, NL
- SWITCH, CH
- ARNES, SI
- CARNET, HR
- CESNET, CZ
- FCCN, PT

JRA2-WI3 End of GN2 Project

ALL GN2
participants!



Service Activity ?

JRA2-WI3 Possible operational Liaisons

- nsp-sec
- Esnet
- Abilene/I2
- REN-ISAC
- GRID-Sec (EGEE...)
- ...

Assumption:

- ❑ You can secure a domain ONLY if you are able to handle and resolve all incidents which originates from that domain or are targeted to that domain.

Approach:

- ❑ Shutting the door to incidents which originates from "outside" one owns domain is "minimal",... extending the domain or liaising with other domains is much better!

To join the party (draft checklist):

- ❑ clear definition of one owns constituency;
- ❑ provide reliable contact information, and adopted procedures (see Trusted Introducer)
- ❑ ability to handle and resolve incidents origination from one owns domain;
- ❑ provide well defined policies on how incidents are handled;
- ❑ agree on minimal incident severity classification;
- ❑ comply to agreed response times, actions and procedures;

To join the party (draft checklist, cont.):

- ❑ provide information to other partners about incidents which apparently originates within their own domain (according to their own disclosure procedures).
- ❑ keep track of incidents until they are solved
- ❑ join the "chain of trust" (Trusted Introducer, PGP and X.509 keys exchange, meet and make the human trust web start, ...)

Indeed...:

- ❑ it must provide benefits to the them in daily incident handling operations !
 - the new team provides information for incidents originating in other team members;
 - the new team acts to solve incidents spotted by other team members;
- ❑ Statistics, theoretical studies, etc... are not (yet) interesting!

QuickTime™ and a
TIFF (LZW) decompressor
are needed to see this picture.

Thank you,

□ Questions?

http://www.terena.nl/tech/index_security.html

<http://www.ti.terena.nl/>

<http://www.ist-transits.org/>

<http://www.terena.nl/tech/task-forces/tf-csirt/>