

GN2-JRA2
WI3
Pilot project for
Security Incident Handling
Claudio Allocchio

GN2-JRA2-WI3 Main Achievements

- ❑ agree on a common set of severity classification of incidents;
- ❑ agree on response actions and response time for incidents;
- ❑ agree on a minimal format for incident information exchange; a subset of IODEF could be what we need, but its an open decision yet;
- ❑ 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; if we do not find a common opinion on how to handle these, we could drop the item, as it is anyhow not strictly related to "a transport service";

GN2-JRA2-WI3 Timescale - draft

- ❑ Jan 2005: definition of incident severity and response times;
- ❑ Feb 2005: first use of incident severity and implementation of response times;
- ❑ Mar 2005: definition of minimal incident exchange format;
- ❑ Apr 2005: implementation of minimal incident exchange format;
- ❑ Apr 2005: first prototype of common TTS defined;
- ❑ Sep 2005: end of first pilot with a working prototype of all above elements.

GN2-JRA2-WI3 Timescale - revised

- ❑ Jan 2005: define the scope of Pilot One (today!);
- ❑ Feb 2005: definition of incident severity and response times;
- ❑ Feb 2005: exchange teams electronic credentials (digital signatures) and alert ML setup;
- ❑ Feb 2005: first use of incident severity and implementation of response times;
- ❑ Mar 2005: definition of minimal incident exchange format;
- ❑ Apr 2005: implementation of minimal incident exchange format;
- ❑ Apr 2005: first prototype of common/interoperable TTS defined;
- ❑ Jun 2005: define information exchange/interaction procedures with NOC/LAN teams;
- ❑ Sep 2005: end of first pilot with a working prototype of all above elements;
- ❑ Sep 2005: give recommendations back to tools developers;
- ❑ Sep 2005: define scope of Pilot Two.

GN2-JRA2-WI3 Possible operational Liaisons

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