

VEDEF Update

TF-CSIRT Workshop

Lisbon

Brief Description

- Vulnerability and Exploit Data Exchange Format (VEDEF)
 - Related to CVE/OVAL and CVSS but addresses different needs
 - Aims for “best of Breed” from candidates:
 - EISPP/CMSI
 - CAIF
 - VulDEF
 - Opensec ANML
 - OASIS AVDL and Web
 - Pick best elements and merge them

RoadMap

- Other DEFs
 - Incident Object (IODEF)
 - IETF lead with INCH WG and RFC3067
 - Intrusion Detection (IDMEF)
 - IETF lead based upon existing CIDF standard
 - Forensic Investigation (FIDEF)
 - NATO may lead through NC3A
 - Covers both static and dynamic Forensic gathering and analysis
 - Susceptibilities and Flaws (SFDEF)
 - No current lead, although investigating interest within AUS, CAN, NZ, UK, US military arena

Current Activity

- FIRST - a sidebar had been planned with CERT/CC and JPCERT/CC
- Meeting in Stuttgart on CAIF
- UK Government internal
 - Continuing to develop a software tool for WARPs, and the roadmap envisages alignment with any Standards that emerge
 - Investigating ways to include VEDEF (and some related other XML standards/ concepts, such as IODEF, IDMEF and the putative SFDEF and FIDEF) into the national XML standards work

Current Activity (Cont.)

- Standards
 - IETF – Ian and Dave had another exploratory discussion with Security Area (the Directors have changed), but still don't get a strong feeling this would be supported
 - The Security Forum of the Open Group has been identified as a possible alternate (we have ruled out OASIS, as they already have 2 competing initiatives internally, and W3C, who are not really active in this space).

Web Site

- A new web site is in the process of being created (www.secdef.org) which will subsume the existing VEDEF web site.
- The new web site will provide a wider access to all Security related DEF activities with the aim of fostering collaboration amongst the various DEF developers.