MILE Implementation Report

Chris Inacio, Carnegie Mellon University
Daisuke Miyamoto, The University of Tokyo
daisu-mi@nc.u-tokyo.ac.jp

Overview

- New proprietary software for IODEF
  - Collaborative Incident Management System
    - Contributed by Dandurand Luc, NATO
  - n6
    - Contributed by Pawel Pawlinski, NASK, CERT Polska
- New category for these software

Issues

- #1: MANTIS framework (section 4) close (IETF90)
- #2: Implementation Guide (section 6) close (IETF90)
- #3: CIMS (section 4) open
- #4: n6 (section 4) open
- #5: section title open

#4: CIMS

- CIMS stands for “Collaborative Incident Management System”
- CIMS is Developed for the Cyber Coalition 2013 (CC13) exercise organized by NATO.
- CIMS is Implemented based on Request Tracker (RT)
  - an open source software widely used for handling incident response by many CERTs and CSIRTs.
- The key features of CIMS are
  - ability to import and export IODEF messages in the body of emails.
  - send an email message containing an IODEF message whenever an incident ticket was created, modified or deleted

#5: n6

- n6 is a platform for processing security-related information, developed by NASK, CERT Polska.
- n6 exposes a REST-ful API over HTTPS with mandatory authentication via TLS client certificates.
- n6 uses an event-based data model for representation of all types of security information.
- N6 supports output data formats for keeping compatibility with existing systems – IODEF (and CSV)
  - Each event is represented as a JSON object with a set of mandatory and optional attributes.

#6: Section title

- Current category
  - Open source Implementations
  - Vendor Implementations
  - Vendors with Planned Support

- New category is preferable for CIMS/n6
  - Replace “Vendor” to “Proprietary”

  or

  - Add new section “Other Implementations”

Summary

- Update Status
  - Base: draft-moriarty-mileimplementation-report-00
  - Update in IETF90
    - 1. Vendor implementation (MANTIS in section 4.4)
    - 2. Implementation Guide (draft-daisuke-iodef-experiment-00, in section 6.1, 6.2)
  - (Envisioned) Update in IETF91
    - 3. CIMS (in section 4.5)
    - 4: n6 (in section 4.6)
    - 5: section category

Acknowledgement

- This work is materially supported by the Ministry of Internal Affairs and Communication, Japan, and by the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement No. 608533 (NECOMA).