draft-ietf-mile-iodef-guidance-07

Panos Kampanakis <pkampana@cisco.com>

Mio Suzuki <mio@nict.go.jp>

IETF97 Seoul

Overview

- This draft aims to provide guidelines for IODEF implementation
  - About representations of common security indicators
  - About use-cases so far
- Show updates from previous(-06) draft
- Show To-Do lists

Updates from Previous(-06) Draft

- Modify examples in "Appendix" to follow IODEFv2 schema
  - Currently the draft includes 4 examples
    - A.1. Malware and related indicators
    - A.2. Malware Delivery URL
    - A.3. DDoS traffic
    - A.4. Zeus Spear Phishing E-mail with Malware Attachment
  - All examples have passed IODEFv2 XML schema, but I don’t have much confidence that the examples are contextually correct.

To-Do Lists and Discussion

- Review

Could you please give me all sorts of comments or feedbacks?