

IODEF Usage Guidance

draft-ietf-mile-iodef-guidance

Berlin - July 2013

Panos Kampanakis

Goals for this draft

- Raise awareness about IODEF
- Point out that IODEF is used today and where
- Encourage faster IODEF adoption
- Educate implementers of IODEF
- Point out common problems and how to address them

Draft outline

[...]

3. Implementation Strategy

- 3.1. Recommended classes to implement
- 3.2. Decide what IODEF will be used for

4. IODEF considerations and how to address them

- 4.1. Unnecessary Fields
- 4.2. External References
- 4.3. Extensions
- 4.4. Logic for watchlist of indications
- 4.5. Externally defined Indicators
- 4.6. Restrictions in IODEF

← “Predicate logic”

5. Current uses of IODEF

- 5.1. Anti-Phishing Working Group
- 5.2. Collective Intelligence Framework
- 5.3. Other

← APWG, CIF,
CERTs etc

[...]

Status

- <http://tools.ietf.org/html/draft-ietf-mile-iodef-guidance-01>
- Draft is still in early stages, most sections need updates
- Some draft sections rely on the IODEF updates in draft-ietf-mile-rfc5070-bis (still early stage also)
- **Input, feedback, and discussion is welcome**