draft-ietf-mile-iodef-guidance-04

Panos Kampanakis
Mio Suzuki  mio@nict.go.jp

IETF94 Yokohama
Overview

• This draft aims to provide guidelines for IODEF implementation
  • About representations of common security indicators
  • About use-cases so far
• From this version (-04), I (Mio) have joined as a co-author of this draft
• Show updates from previous(-03) draft
• Show To-Do lists
Updates from Previous(-03) Draft

• Expanded on the “Extensions” section using Take's suggestion
  • Added external RFCs and related descriptions
• Moved future use-cases under the other section
• CIF and APWG were consolidated in one "Implementation" section
• Added abstract of RFC7495 to the "External References" section
• Added the Kathleen's example of malware delivery URL to "Appendix"
  • The other examples need to be converted from JSON to IODEF
• Added a little description to "Recommended classes to implement" section
To-Do Lists

• Add more to “Recommended classes to implement” section, “Decide what IODEF will be used for” section, “Unnecessary Fields” section, “External References” section, and “Restrictions in IODEF” section

• Convert and add Kathleen’s other examples to “Appendix”

• Modify examples in “Appendix” to follow the current schema
  • following IODEFv2 is better?

• Reflect Panos’s suggestions