draft-ietf-mile-iodef-guidance-05

Mio Suzuki <mio@nict.go.jp>
Panos Kampanakis <pkampana@cisco.com>

IETF95 Buenos Aires
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(-04) draft
• Show To-Do lists
Updates from Previous(-04) Draft

• Fixed some sentences according to Panos-san’s suggestion
• Changed section title from "Restrictions in IODEF" to "Disclosure level of IODEF" and added some description
• Mixed "Recommended classes to implement" section with "Unnecessary Fields" section into "Minimal IODEF document" section
• Added description to "Decide what IODEF will be used for" section, "Implementations" section, and "Security Considerations” section
To-Do Lists and Discussion

• Convert and add examples of spear phishing and watchlist/malware to "Appendix"
• Modify examples in "Appendix" to follow the current schema
  • Currently, only “Malware Delivery URL” sample follows IODEFv2 schema

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