draft-ietf-mile-iodef-guidance-06

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

IETF96 Berlin
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(-05) draft

• Show To-Do lists
Updates from Previous(-05) Draft

• Updated wording in various sections to make content clearer

• Updated Predicate Logic section to reflect the latest IndicatorExpression logic in IODEFv2

• Updated section to describe the difference between events and indicators and their use in IODEF v2
To-Do Lists and Discussion

• Modify examples in "Appendix" to follow IODEFv2 schema
  • Currently, only “Malware Delivery URL” sample follows IODEFv2 schema
• Review and review

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