Managed Incident Lightweight Exchange (MILE)

Overview and Particpation

Kathleen Moriarty
Global Lead Security Architect
EMC Corporate CTO Office

Agenda

- IETF's Managed Incident Lightweight Exchange (MILE)
  - Charter & documents
  - Data formats
  - Transport
- How can I help?

Overview

- Updated Charter:
  - http://datatracker.ietf.org/wg/mile/charter/
- Current list of documents:
- http://datatracker.ietf.org/wg/mile/
  - RFC5070-bis
  - IODEF Enumeration Reference Format
  - Structured Cybersecurity Information (SCI)
  - IODEF Guidance
  - RESTful indicator exchange using IODEF/RID

EMC²

MILE: Solving Interoperable Exchanges

- Share, consume, process, and amend indicator and incident data
  - Enable easy processing and use by
    - Incident Management Systems,
    - Security Information and Event Management systems (SIEM),
    - intrusion detection systems, etc.
  - Intelligence feeds for situational awareness
  - Enable risk-based prioritization for remediation and defensive actions
- Provide not only a common format, but also an architecture and protocol exchange

Interoperable Data Formats

Consistent Data Representations

Data exchanged, sent/received, with a consistent interpretation

- Well-defined data formats
  - RFC5070, Incident Object Description Exchange Format (IODEF) under revision for v2.0, participation encouraged
    - Sharing of indicator and incident information with context rich data for proactive and reactive remediation capabilities
  - RFC5070-bis is in an edit cycle
    - Outstanding issues tracked at: http://trac.tools.ietf.org/wg/mile/trac/report/1
    - Discussions on feedback, comments, changes, additions encouraged!
      - Fix internationaliztion
      - Add better reference (citation) to RecordPattern at type=regex
      - Review completeness of HistoryItem at action
      - Review completeness of @restriction
      - Review completeness of Impact at type
      - Add support for domain name meta data
      - Add geolocation representation to Node/System
      - Review completeness of recent additions in 5070-bis
      - Review implementation of extending enumerated values
      - Review all requirements key words (RFC 2119)
      - Harmonize the specification for Reference with other WG activity
      - Review completeness of NodeRole at category
      - Define clear scope for the core data model relative to other WG documents and future extensions

Incident Object Description and Exchange Format (IODEF)

Background

- Internet Engineering Task Force (IETF) Standard: RFC5070
- Provides a standard format to describe a security incident
- Effort led by the CERT Coordination Center (CERT/CC) out of Carnegie Mellon University, IODEF started by TERENA
- Computer Security Incident Response Teams (CSIRTs) globally contributed to the development and evaluation of the Extensible Markup Language (XML) schema

Assumptions

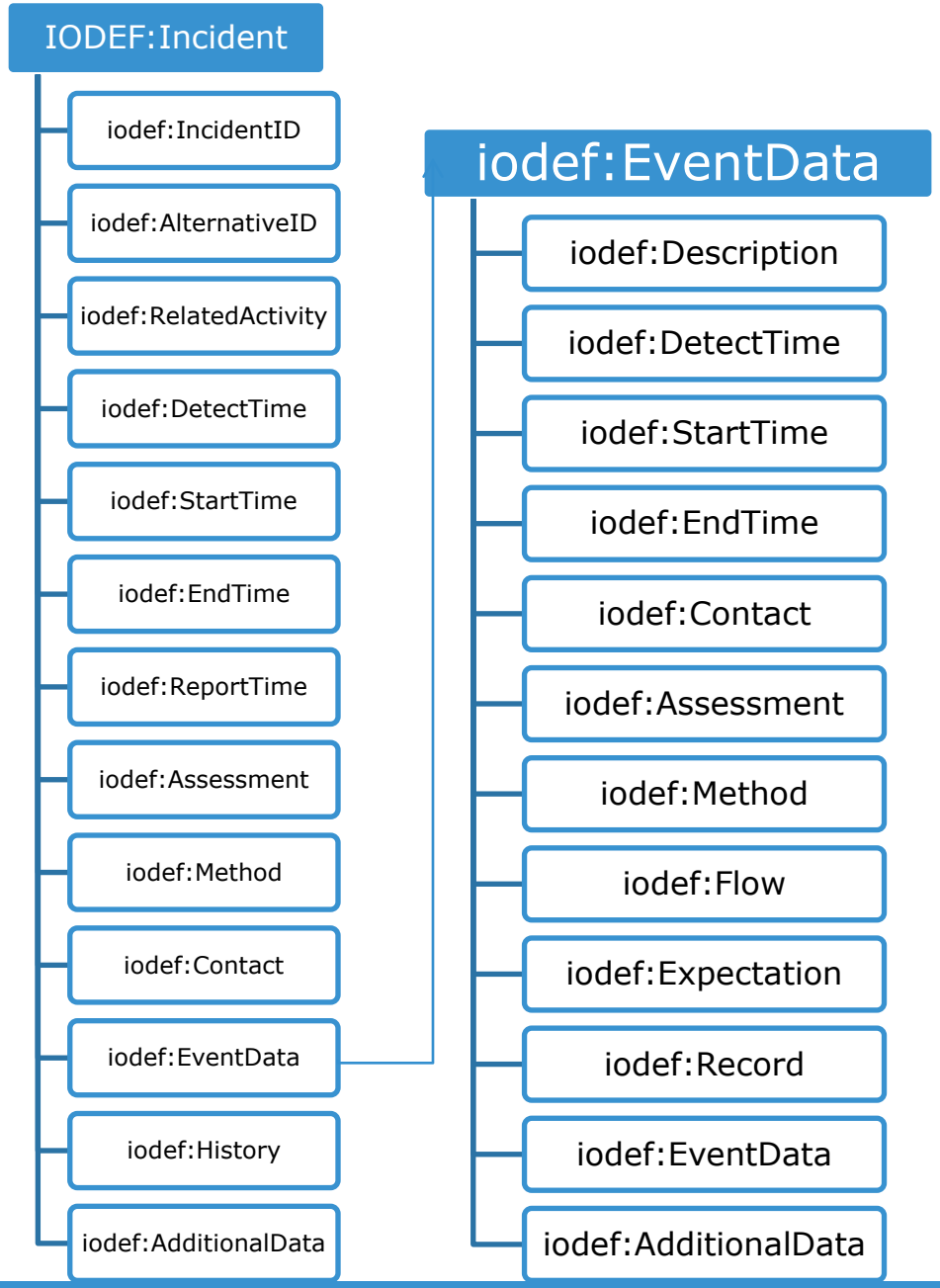
- Incidents are not IDS alarms
  - "Incidents are composed of events"
- Agnostic to specific incident taxonomies
  - "Your definition/threshold of an incident may be different than mine"
- Incidents are numbered and there is state kept about them
  - "Organizations assign incident IDs and have ticketing/handling/correlation systems that process them"
- Merely a wire format
  - "Sharing is different than storage and archiving"
- Incomplete information
  - "You may require more complete information than I need, can get, or have right now"

Some slide content from RSA Presentation: Roman Danyliw & Pat Cain

EMC²

IODEF Data Model

- CSIRT Operations
  - Incident identifiers
  - Contact Information
- Internationalization
  - Various Encodings
  - Translations
- Data handling labels
  - Sensitivity
  - Confidence
- Extensibility of attributes and adding new elements
- Timing information
- Enumeration of hosts or networks
  - e.g., IP addresses, ports, protocols, applications, etc.
- History and requested action
- Exploit and vulnerability references
- Impact expressed technically, financially, or by time
- Forensics information



EMC²

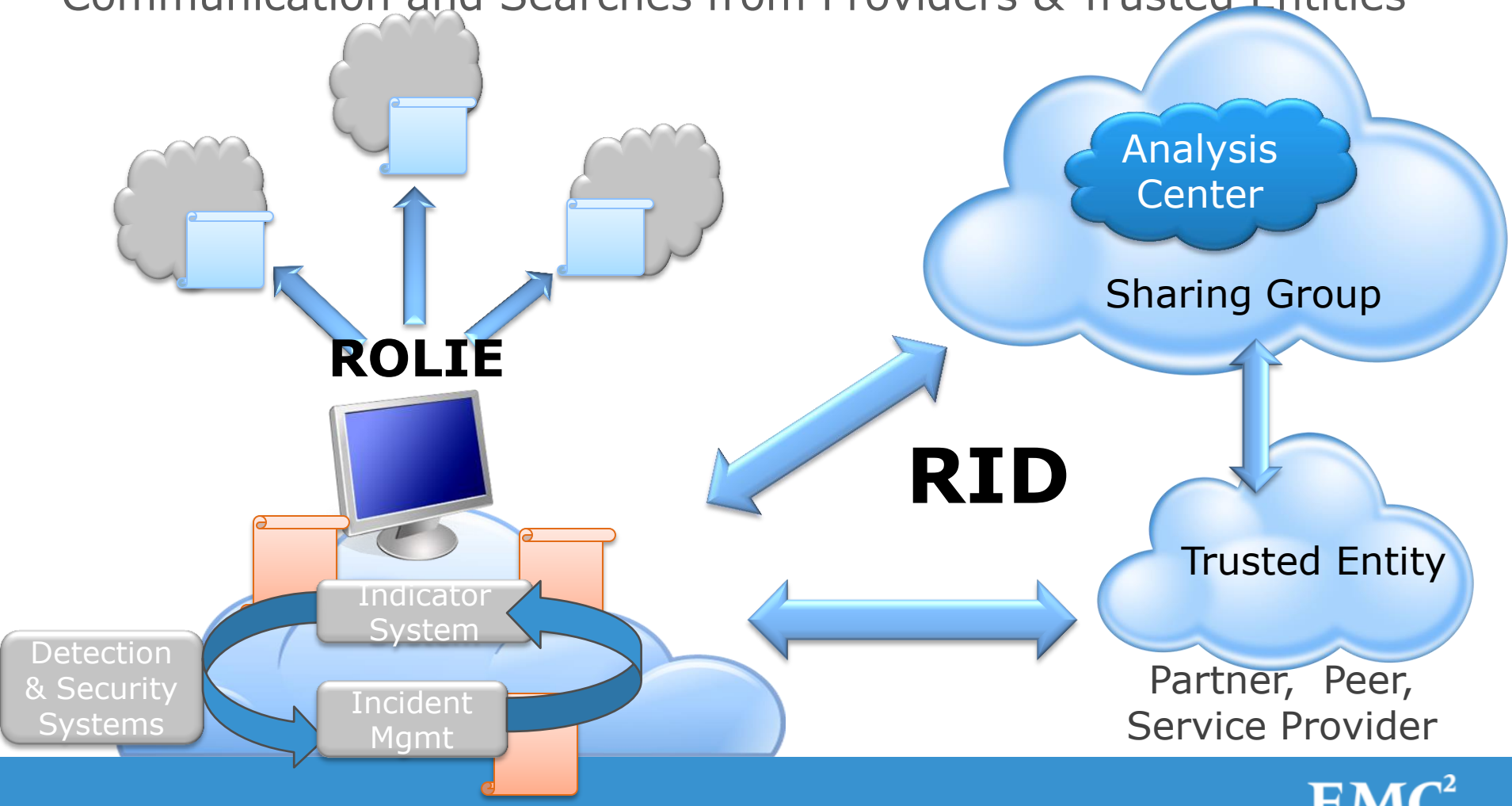
Feedback Requested

- Feedback encouraged on
  - RFC5070-bis
  - Structured Cyber Security draft
  - IODEF Enumeration Reference Format
- We will need to determine if the SCI draft should get folded into RFC5070-bis
- Additional extensions may be submitted soon for specific use cases

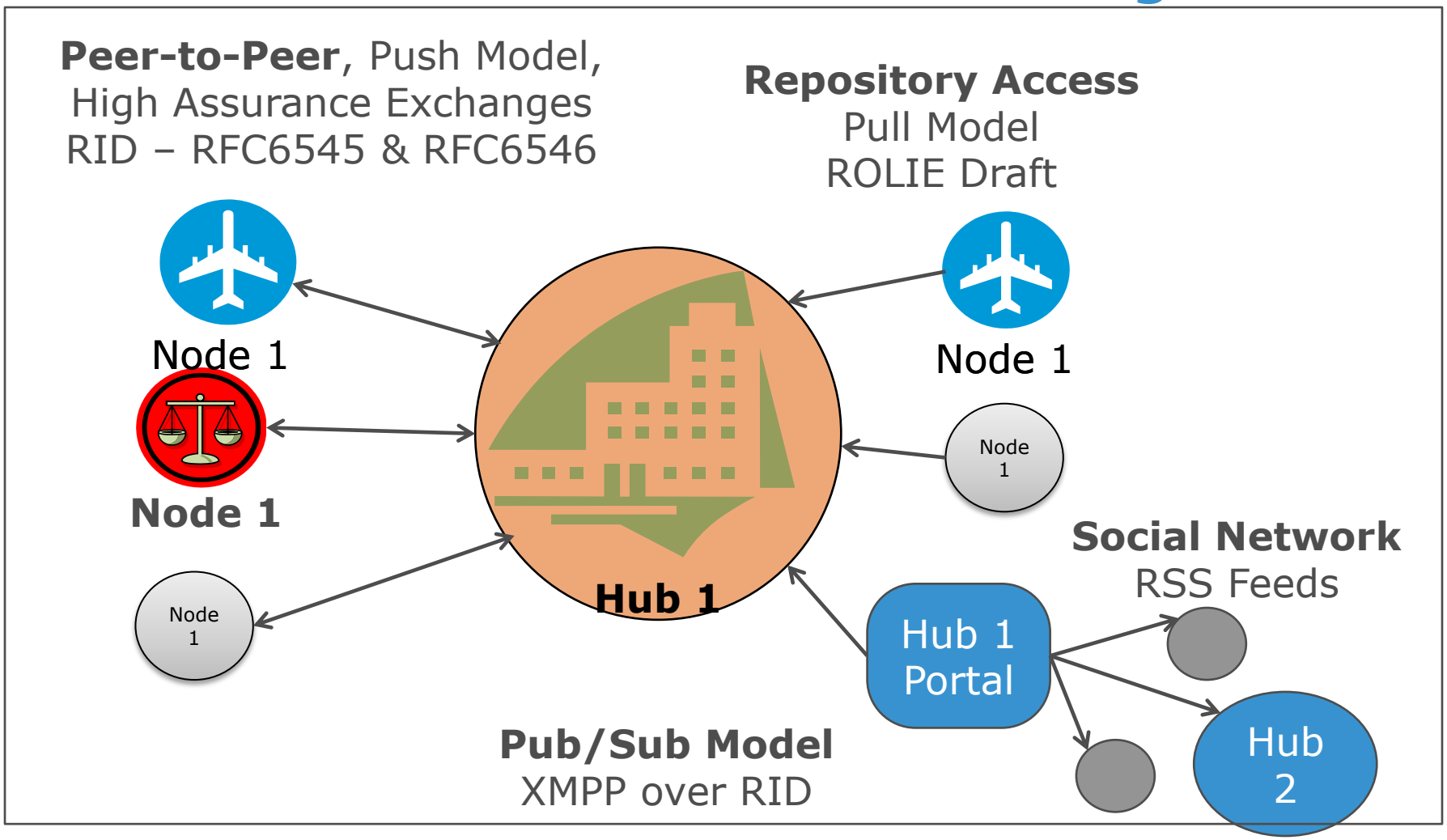
Transport

RID Incident and Indicator Exchanges

Communication and Searches from Providers & Trusted Entities



Protocols for Information Exchanges



Summary

- Taxonomy of cyber incident information is based on IODEF version 2 in the IETF
  - In revision from 1.0, participation encouraged
- Transport enables multiple exchange types
  - Peer-to-peer, push model
  - Hub and spoke pull model
  - Publish & subscribe
- Relies upon trust & assurance
  - Identity, access management, and federation
  - Secure collaboration with trusted entities at appropriate assurance levels

EMC²

How Can I help?

- Participate in the IETF MILE working group:
  - Meetings are held three times a year
    - Next meeting: Berlin, Germany – July 28 – Aug 2, 2013
    - Participation can be in person or remote via MeetEcho
    - All decisions are finalized on the mailing list
  - Join MILE@ietf.org mailing list
    - Participate in an existing thread
    - Start a thread on any questions based on review of a draft
    - Start a thread on work to be proposed related to MILE
- Contribute to open source code
  - https://github.com/RSAIntelShare
  - Provide feedback on code and associated RFCs and drafts

Thank you!

EMC²

Managed Incident Lightweight Exchange (MILE)

- Interoperable data exchanges
  - A data model alone is not enough
  - Consistent representations to ensure the recipient interprets the information as expected by the sender
  - Flexible and extensible data model:
    - Incident Object Description Exchange Format (IODEF)
    - IODEF + extensions using AdditionalData or RecordItem classes
    - IODEF + Structured Cybersecurity Information (SCI) registered data representations
- Flexible transports with consistent policy capabilities via Real-time Inter-network Defense (RID)
    - Secure peer-to-peer (RID + HTTP/TLS binding)
    - Hub-n-spoke (Resource Oriented Lightweight Indicator Exchange (ROLIE))
    - Federated access (RID + XMPP binding?)
    - Transports flexible to carry IODEF or any other data model