IACD Intra-Enterprise Message Fabric Community of Interest (COI)

August 4, 2016

Background

- **IACD has three pillars:**
  - **Automation to enable automated sensing, sense making, decision making, and response to provide near real-time network defense within an enterprise.**
  - **Information sharing to enable rapid sharing of indicators, analytics, and effective responses between enterprises, and coordinated response across the community.**
  - **Interoperability to allow commercial vendors to adapt existing interfaces to enable interoperability and integration of commercial tools, which in turn enables integration of new IACD capabilities into existing enterprise configurations.**

- **Interoperability and automation require common interfaces (Message Fabric) to integrate commercial tools within an enterprise**

Message Fabric - Definition

- A set of commonly understood application interfaces/descriptors usable by any tool or information source to 'plug in' to the fabric
- A standardized message set that establishes the contextual constructs and data formats
- A consistently defined set of message services (supporting control, configuration, publish/subscribe, etc.)
  - Define which services must be consistent across all users and which should be reserved to be enterprise-specific
  - Define a set of configurable trust and access services to ensure confidentiality, integrity, and availability
- A set of transport protocols
  - Decide to what degree the transport of messages must be standardized

Benefits of a Common Message Fabric

- **Provides secure and reliable intra-enterprise data exchanges**
  - **Facilitates interoperability, machine-speed information sharing, and automation in a dynamic environment**
  - **Bakes-in security and information sharing into the architecture**
- **Provides foundation necessary for:**
  - **Common data models**
  - **Abstraction of commands**
  - **Baked-in security and information sharing**
- **Simplifies integration of diverse sensors, actuators, analytics, orchestration/decision support products and network management tools**
  - **Eliminate the need for pairwise integration**
  - **Enables plug and play capabilities**

A common intra-enterprise message fabric enables multi-vendor ecosystems, flexible deployment of new tools, rapid and automatic exchange of security-relevant data and appropriate abstraction

Goals of the COI

- **Form a self-sustaining community**
  - **Achieve consensus on the required characteristics of this message fabric and the level at which interoperability specifications or standards should be established**
- **COI-developed message fabric interoperability specifications**
  - **Eventually to be transferred to a standards body selected by the COI**

Who should participate

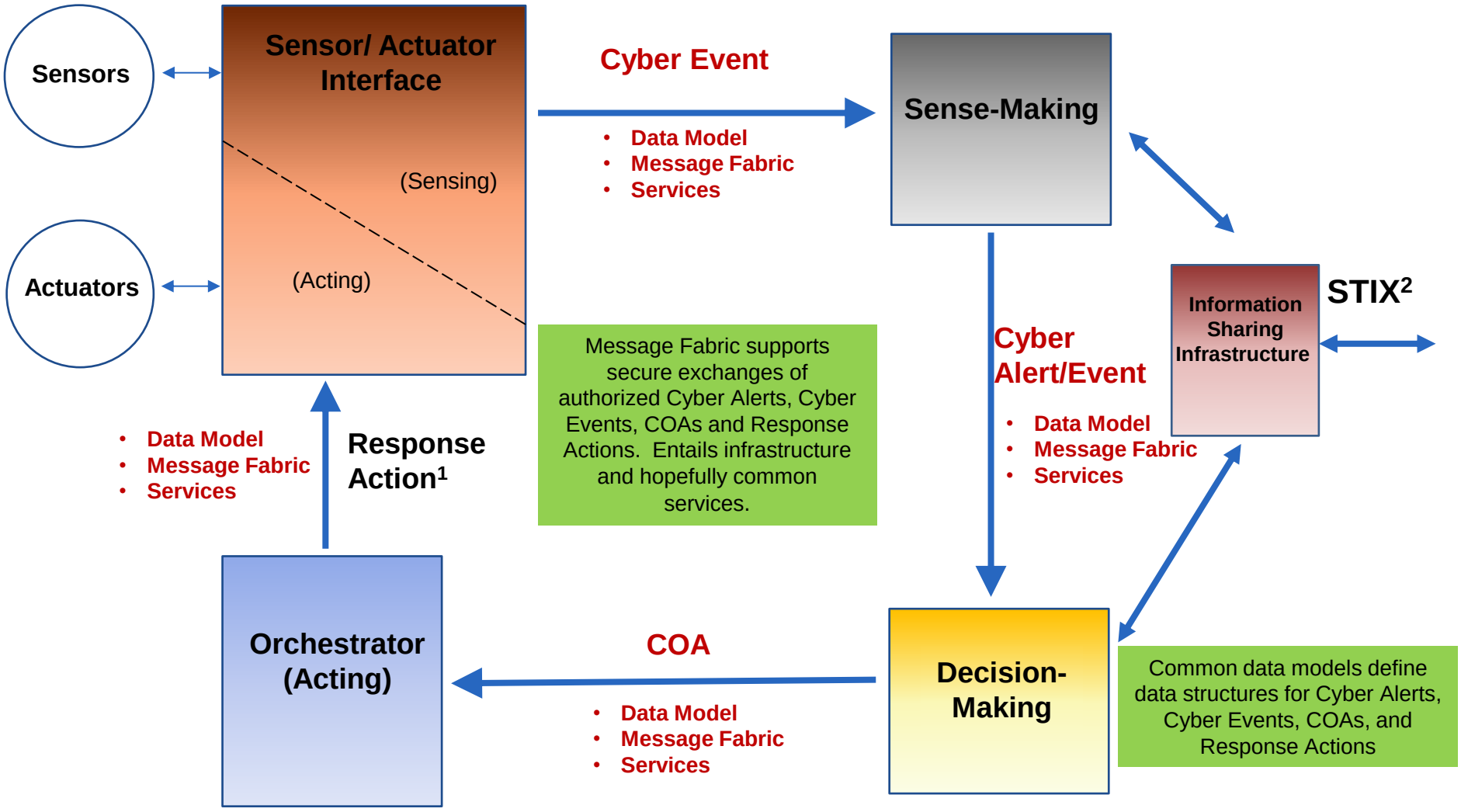
- **Vendors, government, academia, and CIKR members**
  - **Representing:**
    - **Cybersecurity and network management solutions providers**
    - **Messaging and orchestration providers**
    - **System integrators**
    - **Operators**
    - **Users/consumers**
    - **Acquisition programs**
  - **Interested in standardizing message fabrics and common data models to ensure interoperability between diverse commercial cyber security tools and network management products**

Future Interest

- **Points of Contact**
  - **Linda Harrell (Linda.Harrell@jhuapl.edu)**
  - **Cherie Mauck (Cherie.Mauck@jhuapl.edu)**

BACKUP

Key Interfaces and Initial Targets: OODA Loop View



[1]Work in progress by Open C2 Forum

[2]Established standards and specifications where possible