Messaging Lessons-Learned

16 February 2016

Kim Watson
Kimberly.Watson@jhuapl.edu
Message Fabric
Decentralized Service Orchestration Approach

Boundary Protections
Network Protections
Host Protections

Sensor Data
S/A Control/Data Channels
Actuator Cmds

Sensor/Actuator Interface
Secure Orchestration, Control
Response Actions

Sense-Making Analytic Framework
Secure Orchestration, Control
Cyber Events, Shared Analytics
Cyber Events

Presentation & Ops Services
Secure Orchestration, Control
Configuration Directives

Control Message Infrastructure
Message Bus

Response Actions, Information Sharing Actions
Course of Action
Shared Indicators
Shared COAs, Indicators, Analytics

Secure Orchestration, Control
Decision-Making Engine
Repositories
Log Data
Intel Configuration Blackboard

External Data
External Sharing I/F
Community Data Channel
Community Coordination Channel

Same interoperability requirements as in centralized approach

Trust Services: Security, Identity, Access Control
Sensors and actuators have translators and managers that bridge the proprietary interfaces (*Raw Sensor Data*) to the standard Control Message Infrastructure format (*Cyber Events*)
Integration of sensors to the message bus only required “shimming”

- Typical standard process for integration, nothing abnormal
- Transforms data between application native format and Common Event Format (CEF) if necessary
- Transports data in/out of the message bus

The Sensor Actuator Interface is the right level of abstraction
Lessons Learned

- **Message Fabric**
  - Products and applications did *not* need to know about each other or be pairwise integrated to be added into the environment.

- **Sensor/Actuator Integration**
  - Cybersecurity tools did not have a common interface, data model, or trust model.
    - The site or the vendors must perform the integration and associated management functions.
    - Significantly limits the products and applications that can be included in any enterprise.

**Message Buses support Scalability, Interoperability, and Simplicity**
Implications of Lessons Learned

- There is potential value in using a message bus when your environment includes:
  - Multiple consumers
  - Large scale integration
  - Dynamic environments
  - Extensive network connectivity

- **Sustainable** and **extensible** SRCE components need to have common or standardized connectors and data formats
  - Standards are not required internal to a single enterprise if the site is willing to be limited by vendor integration
Implications for SRCE

- Long Term Need: A common message fabric with standard message sets, services, and interfaces

  - Short Term: Common Connector
    - Products and applications come with at least one of a small set of ways to “plug” into message bus instances
    - May not need to be standardized as much as a small list where vendors must support at least one

  - Short Term: Initial common data model
    - Cyber Alerts and Response Actions

Standardization offers more flexibility and avoids significant custom integration
Message Fabric
Decentralized Service Orchestration Approach

Sensor/Actuator Interface
- Secure Orchestration, Control
- Sensor Data
- S/A Control/Data Channels
- Actuator Cmds
- Response Actions
- Cyber Events, Shared Analytics
- Cyber Events, Shared Indicators
- Cyber Alerts
- Content Analytics
- All Messages
- Configuration Directives

Sensor Data
- Actuator Cmds

Control Message Infrastructure
Message Bus
- Secure Orchestration, Control
- Decision-Making Engine
- Repositories
- Content
- Log Data
- Intel Configuration Blackboard
- COA Policy Mission Models
- COAs
- Shared COAs
- Shared Indicators
- Cyber Events
- Cyber Events, Shared Analytics
- Cyber Alerts
- Cyber Alerts, Shared Indicators
- Secure Orchestration, Control
- Information Sharing Infrastructure
- External Sharing I/F
- Community Data Channel
- Community Coordination Channel

Response Controller
- Response Actions
- Information Sharing Actions
- Course of Action
- Secure Orchestration, Control
- Response Controller

Course of Action
- Shared COAs
- Shared Indicators
- Cyber Events, Shared Analytics
- Cyber Events, Shared Indicators
- Cyber Alerts
- Cyber Alerts, Shared Indicators
- Secure Orchestration, Control
- Secure Orchestration, Control

Repositories
- Log Data
- Intel Configuration Blackboard
- Content
- COAs
- COA Policy
- Mission Models

Trusted Cyber Services
- Secure Orchestration, Control
- Cyber Events
- Shared Indicators
- Cyber Alerts
- Secure Orchestration, Control

Trust Services: Security, Identity, Access Control

External Data Feeds
- External Data Sharing I/F
- Community Data Channel
- Community Coordination Channel

Same interoperability requirements as in centralized approach

Enterprise Perimeter

Boundary Protections
Network Protections
Host Protections
Defense Services
