

Application of Message Fabrics to SRCE Systems

16 February 2016

DISTRIBUTION STATEMENT A APPROVAL FOR PUBLIC RELEASE: DISTRIBUTION IS UNLIMITED

Based on work funded by the Department of Homeland Security

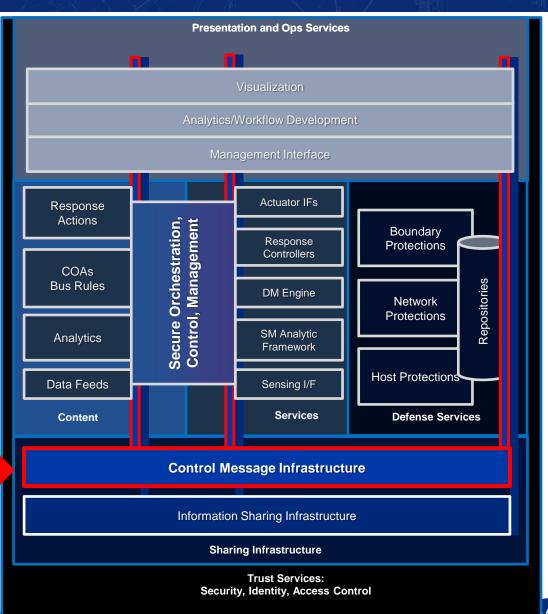
Gregg Tally @jhuapl.edu



Message Fabrics in SRCE Context

- Focus on the messaging within an enterprise in support of security operations automation and interoperability
- Enables secure, timely, and loosely coupled communication

Context



Challenges that Benefit from Message Fabric

- Enterprises will deploy components developed by vendors that may not have performed pairwise integration
- Vendor component capabilities will evolve independently over time
- Enterprises have diverse deployment topology and distribution requirements
- Sensor activity will occur at variable rates, with peaks, lulls

Implied SRCE Design Requirements

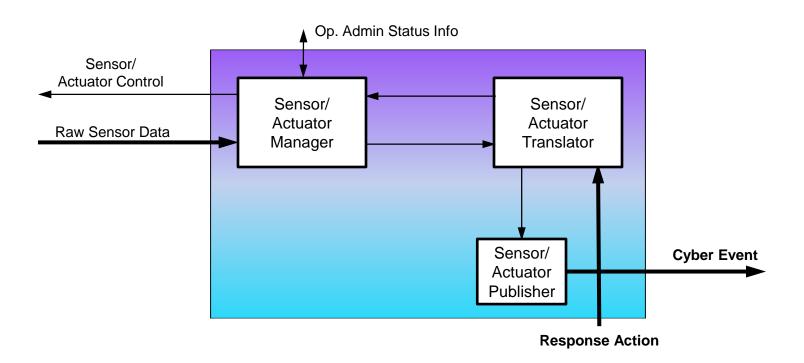
- Distributed, asynchronous message processing
 - Permits faster message producers to proceed without waiting for slower consumers
 - > Allows message consumers to catch-up during the lulls
- Minimal coupling between message producers and consumers
 - Rely only on common data representations and message bus interface
 - > Facilitate integration of components from independent vendors
- Backward compatibility of message formats
 - > Eliminate need for coordinated upgrades across components

Message Fabric Centralized Service Orchestration Approach Boundary Presentation & Sensor/Actuator Sense-Making **Protections** Interface Analytic **Ops Services** Interoperability Content Sensor Data **Framework** requires standardized: Network Analytics **Protections** Service definitions S/A Control/Data Message content Channels Host Message transport **Protections Actuator Cmds** Content formats **Defense Services** Status **Response Actions** Cyber Events, **Shared Analytics Control Message Infrastructure** Message Bus Configuration **Directives** Cyber Events Cyber Alerts Secure Orchestration, Control, Management Course of Action Shared Indicators Shared COAs, Indicators, Response Actions, **Information Sharing Actions Analytics** Enterprise **Cyber Alerts Shared COAs, Indicators** Cyber Events, Perimeter Course of Action Shared COAs Shared Indicators **Analytics** Repositories External **External Data** Sharing I/F Feeds Log Data Response **Decision-Making** Information Intel Controller **Engine** Sharing Community Configuration **Data Channel** Blackboard Infrastructure Content Community COAs Coordination **COA Policy** Channel Mission Models Trust Services: Security, Identity, Access Control

Message Fabric Decentralized Service Orchestration Approach Presentation & Sensor/Actuator Sense-Making Boundary **Protections** Interface Analytic **Ops Services** Same interoperability Content Sensor Data **Framework** requirements as in Network Analytics centralized approach **Protections** S/A Control/Data Channels Host **Protections Actuator Cmds** Secure Orchestration. Secure Orchestration, Secure Orchestration. Control Control Control **Defense Services** Response Actions Cyber Events, All Messages **Shared Analytics** Configuration Cyber Events Cyber Alerts **Directives Control Message Infrastructure** Message Bus Response Actions, Course of Action Shared Indicators Shared COAs, Indicators, Information Sharing Actions **Analytics** Enterprise Perimeter Shared COAs. Indicators Cyber Alerts Cyber Events, Shared COAs Course of Action Shared Indicators **Analytics** Secure Orchestration, Secure Orchestration, Repositories Secure Orchestration, External **External Data** Control Control Control Sharing I/F **Feeds** Log Data Response **Decision-Making** Information Intel Controller Sharing **Engine** Community Configuration **Data Channel** Blackboard Infrastructure rusted Information Sharing Content Community COAs Coordination **COA Policy** Channel Mission Models **APL** Trust Services: Security, Identity, Access Control

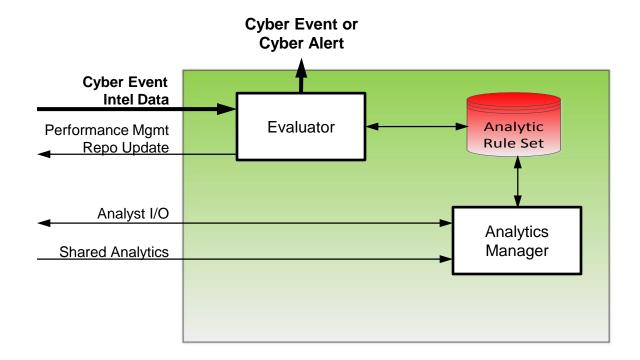
Message Content Sensor Actuator Interface

Sensors and actuators have translators and managers that bridge the proprietary interfaces (*Raw Sensor Data*) to the standard Control Message Infrastructure format (*Cyber Events*)



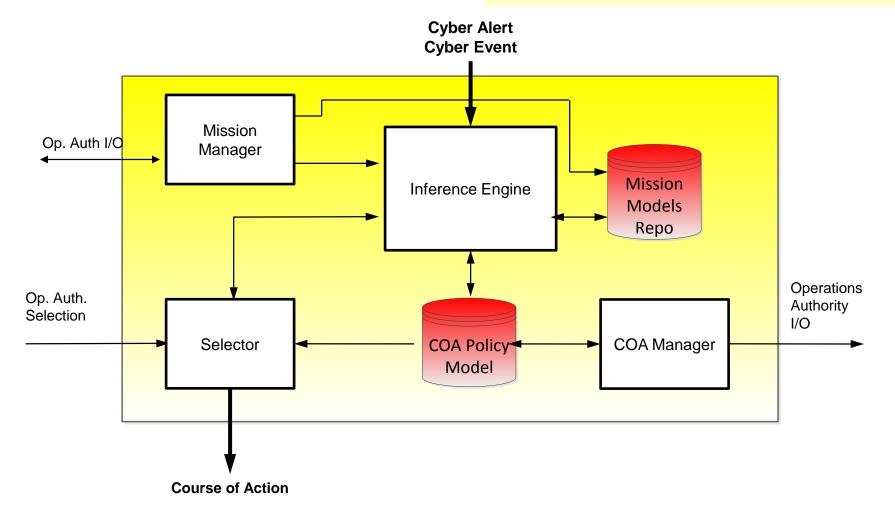
Message Content Sense Making Analytic Framework

Evaluators use analytics to assess *Cyber Events* against *Intel Data*, determine if a *Cyber Alert* should be generated or if the *Cyber Event* requires further analysis



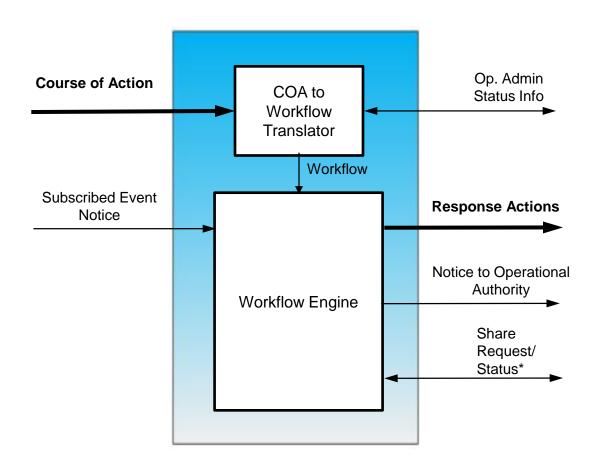
Message Content Decision-Making Engine

Given a *Cyber Alert* or *Cyber Event*, DM-Engine determines a course of action (*COA*) to minimize risk while considering mission impact of the alternative COAs



Message Content Response Action Controller

Selected COAs (*Couse of Action*), with parameters for targets and other options, converted to specific *Workflow*s containing *Sensor/Actuator Control Info* for execution



^{*} Incoming status includes Tip/Event/COA sharing notice



Messaging Attacks and SRCE

Attack Vectors	Example SRCE Outcome	Mitigation May Include
Message Replay	CoA enabled when not authorized, potentially causing network disruption	Signed messages with timestamp
Malformed Data (e.g. buffer overflow)	Response Controller could be affected by malformed data, allowing attacker undetected high privilege access	Whitelisting signed recipients, strong type/field checks
Man-in-the-Middle	A malicious party may intercept sensor data and replace it with recorded sensor output that appears normal, while actual abnormal sensor data is inaccessible to SRCE	Mutual authentication
Message flooding	Critical third party services may be rendered inaccessible if malicious party directs high bandwidth resources appropriately	Upstream high-speed dynamic filtering, use of efficient signing mechanisms (e.g., HMAC)
Spoofing	Malicious party receives sensitive analytics that can be used to develop stealth tactics	Use of strong key management or strong CA capabilities
Passive Eavesdropping	Indicators and COAs for a particular attack are learned by an adversary leading to changes in the attack vector to bypass the described mitigations	Use of strong confidentiality mechanisms

Potentially Relevant Standards Efforts

Message Transport

- Advanced Message Queueing Protocol (AMQP) from OASIS
- > Data Distribution Services (DDS) from Object Management Group

Message Content

- > Common Event Format (CEF) from HP ArcSight
- > Incident Object Description Exchange Format (IODEF) from MILE
- Reporting Formats in Security Content Automation Protocol (SCAP) from NIST
- > Open C2 from Open C2 Working Group

Security

- > DDS Security v1.0 Beta 1
- IETF Working Groups
 - Security Automation and Continuous Monitoring (SACM)
 - Managed Incident Lightweight Exchange (MILE)
 - DDoS Open Threat Signaling (DOTS)



Summary

- Interoperability requires standardized:
 - > Service definitions
 - > Message content
 - > Message transport
 - > Content formats
- Connects the core services supporting Sensing, Sense Making,
 Decision Making, and Acting
- Can support centralized, decentralized, or hybrid orchestration models

Specifications are to be determined



