AOS-16-0875
Aug 3, 2016

Enabling Adaptive and Interoperable Cyber Defense: Message Fabric Integration and Standardization

Release 1.0

Prepared for: Department of Homeland Security; Maryland Procurement Office

Prepared by: Linda Harrell, Wende Peters, Kim Watson, Gregg Tally, Laura Heath, Harold Zheng

Task No.: CYS05
Contract No.: H98230-14-D-0037 TTO 0042

EXEMPT FROM MANDATORY DISCLOSURE: This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA. Exemptions 3 and 5 apply.

Today's enterprise owners and operators, and the network defenders they employ, face a huge and continually evolving challenge: maintaining their core business and mission capabilities, and protecting their customer/user interests in the face of cyber-based threats, breaches, and attacks. Adversaries who are intent upon exploiting cyber vulnerabilities currently enjoy an asymmetric advantage; however, technology innovations, business prioritization, public policy developments, and cross-community partnerships are now converging to balance this equation. For example, the Department of Homeland Security (DHS), National Security Agency (NSA) Cyber Task Force (CTF), and several other organizations have come together to co-sponsor the Integrated Adaptive Cyber Defense (IACD) initiative, whose purpose is to define, mature, and prototype reference architectures and concepts that will enable operators and system owners to detect and respond to cyber threats and attacks in a cyber-relevant timeframe. IACD builds on several earlier initiatives, including the DHS Enterprise Automated Security Environment (EASE) and NSA's Active Cyber Defense (ACD).

The IACD operational environment is intended to include diverse government, commercial and critical infrastructure enterprises. IACD does not define a rigid specification or prescribe specific solutions. Rather it is intended to support a "bring your own enterprise" model with a product-agnostic plug-and-play architecture to enable enterprises to select the commercial components and products that best suit their needs. A goal is to expose interfaces to support interoperability between diverse vendor products, allowing the use of multi-vendor solutions tailored to each enterprise. The IACD initiative intends to provide guidance to both the supply and demand sides of the cybersecurity operations marketplace to achieve this goal. One important artifact that is created by the IACD initiative is an IACD reference architecture. This architecture can be applied to diverse Federal department and agencies infrastructures, and be aligned to Department of Defense (DoD) and intelligence community cybersecurity reference architectures.

The IACD initiative introduces three foundational activities into existing enterprises:

a. Automation to enable automated sensing, sense making, decision making, and response to provide near real-time network defense within an enterprise.

b. Information sharing to enable rapid sharing of indicators, analytics, and effective responses between enterprises, and coordinated response across the community.

c. Interoperability to enable integration of diverse commercial tools within existing enterprises, which in turn enables enterprises to incorporate new IACD capabilities.

Through concept development, prototyping, hardware demonstrations, research, and several Secure and Resilient Cyber Ecosystem (SRCE) workshops, the IACD project identified a need to define a message fabric that supports machine-speed information sharing between diverse commercial cyber security tools. A standardized message fabric is essential to establishing a secure, resilient cyber ecosystem that is equipped to face the current challenges while, more critically, providing the flexibility and adaptability to evolve to address future challenges. Based on our IACD experiences, the Johns Hopkins University Applied Physics Lab (JHU/APL) recommends that the community shift from proprietary tool sets to an open interface ecosystem that enables integration of diverse, specialized tools in accordance with each organization's policies.

The purpose of this paper is to:

- Broadly scope the characteristics of an emerging cyber ecosystem, particularly within an enterprise.
- Outline a construct for an interoperable, vendor-agnostic message fabric that enables adaptive cyber defense capabilities within an enterprise.
- Establish an initial set of use cases and representative requirements as a common reference point for defining a sustainable, industry-supportable path towards integration and standardization while supporting continued innovation.
- Describe the formation of a self-sustaining Community of Interest (COI) to define message fabric specifications.

The Challenge

Currently, cyber defense capabilities and processes are insufficient for rapidly responding to cyber threats and attacks; organizations are highly dependent upon security and cyber-operations teams who struggle to manage ever expanding business demands and a continually evolving threat space. To improve efficiency and effectiveness, many organizations have invested in an array of cybersecurity and enterprise management tools, threat intelligence sources, and situational awareness solutions. These investments, however, too often present their own challenges; the analysts are awash in data from disparate information sources without context or a cohesive integration of the data. Often, organizations expend precious resources performing this integration ourselves in an ad-hoc manner. In other cases, we lock ourselves into narrow stacks of solutions in the interest of providing integration, but sacrifice the flexibility to adjust or expand the suite of tools available.

Meanwhile, industry solution providers face the cost, complexity, and liability of managing a continually expanding set of backward-compatible interfaces, or face telling some customers that they cannot access the most innovative options available without jettisoning long-established investments.

Every organization has unique operational, threat, and risk environments supported by different policies, procedures, and resource profiles. They must be equipped with solutions adaptive to their needs, instead of having to sacrifice their specifications or business priorities to the constraints of network and security solutions.

The Vision

To address these challenges, we require the ability to:

- ***Integrate and automate*** across a diverse and changing set of sensing, sense-making, decision making, and response capabilities.
- Execute mission operations and cyber defense capabilities at the ***speed and scale*** needed to provide real-time network defense within an enterprise.
- Leverage the expanding tools for inter-organizational ***information sharing*** and extending that ***inside our enterprises*** for actionable response.

- ***Maintain the operational freedom*** to reconfigure, repurpose, or replace solutions in innovative and unanticipated combinations, thus enabling each mission owner the ability to tailor to their needs.

A common standardized intra-enterprise message fabric provides the foundation to accomplish these goals by:

- Supporting secure and reliable intra-enterprise data exchanges that facilitate interoperability, machine-speed information sharing, and automation in a dynamic environment.
- Baking-in security and information sharing into the enterprise architecture
- Supporting common data models and abstraction of commands
- Simplifying integration of diverse sensors, actuators, analytics, orchestration/decision support products and network management tools

Figure 1 highlights some of challenges experienced in today's environment and the desired end-state.

Bringing Together a COI for Common Message Fabric Specifications

Achieving the vision requires a common standardized secure message fabric with application programming interfaces (APIs), if necessary, to interconnect diverse commercial cybersecurity devices and tools. Defining the characteristics of this fabric, the level at which interoperability specifications should be established, and the amount of flexibility needed by individual enterprises is fundamental to achieving a secure, resilient cyber ecosystem**.**

Together, a community of cybersecurity and network management solutions providers, messaging and orchestration providers, system integrators, operators, users/consumers, and acquisition programs from across the commercial marketplace, government, academia, and Critical Infrastructure and Key Resources (CIKR) sectors are asked to scope and define the message fabric needs and identify how and to what degree each component interoperates. This community should define message fabric specifications at the appropriate level of detail, while providing vendors the freedom to develop innovative solutions. Our goal is to form a self-sustaining community to define common message fabrics and data models to facilitate interoperability between commercial cyber security devices/products and network management tools. The desired end-state is COI developed message fabric interoperability specifications that enable enterprises to easily adopt and securely integrate diverse sensors, actuators, analytics, orchestration/decision support products and network management tools to enable enterprises to respond to dynamic cybersecurity threats in a timely manner. It is envisioned that the specifications will eventually be transferred to a standards body selected by the COI.

The community that emerges to address this topic will ultimately need to develop and execute a plan to realize message fabric specifications. For example, some candidate next steps for this community are:

- Document a consensus view of the problem to be addressed and define the characteristics of a successful outcome.

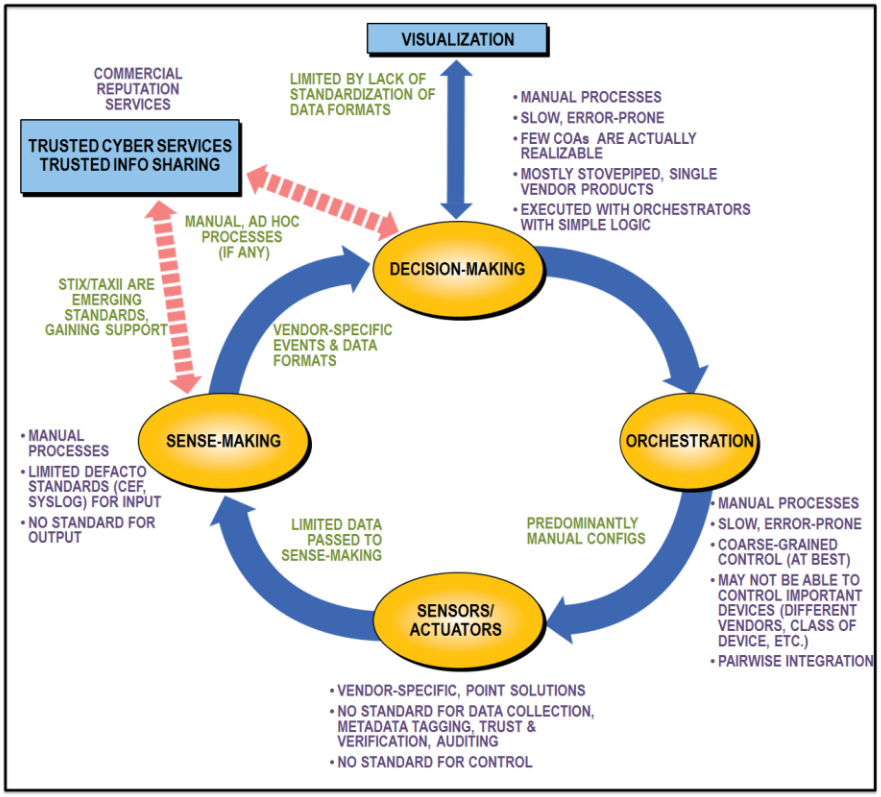

VISUALIZATION
COMMERCIAL REPUTATION SERVICES
LIMITED BY LACK OF STANDARDIZATION OF DATA FORMATS
TRUSTED CYBER SERVICES TRUSTED INFO SHARING
• MANUAL PROCESSES
• SLOW, ERROR-PRONE
• FEW COAs ARE ACTUALLY REALIZABLE
• MOSTLY STOVEPIPED, SINGLE VENDOR PRODUCTS
• EXECUTED WITH ORCHESTRATORS WITH SIMPLE LOGIC
MANUAL, AD HOC PROCESSES (IF ANY)
DECISION-MAKING
STIX/TAXII ARE EMERGING STANDARDS, GAINING SUPPORT
VENDOR-SPECIFIC EVENTS & DATA FORMATS
SENSE-MAKING
ORCHESTRATION
• MANUAL PROCESSES
• LIMITED DEFACTO STANDARDS (CEF, SYSLOG) FOR INPUT
• NO STANDARD FOR OUTPUT
• MANUAL PROCESSES
• SLOW, ERROR-PRONE
• COARSE-GRAINED CONTROL (AT BEST)
• MAY NOT BE ABLE TO CONTROL IMPORTANT DEVICES (DIFFERENT VENDORS, CLASS OF DEVICE, ETC.)
• PAIRWISE INTEGRATION
LIMITED DATA PASSED TO SENSE-MAKING
PREDOMINANTLY MANUAL CONFIGS
SENSORS/ ACTUATORS
• VENDOR-SPECIFIC, POINT SOLUTIONS
• NO STANDARD FOR DATA COLLECTION, METADATA TAGGING, TRUST & VERIFICATION, AUDITING
• NO STANDARD FOR CONTROL

Figure 1 (a) Existing Situation

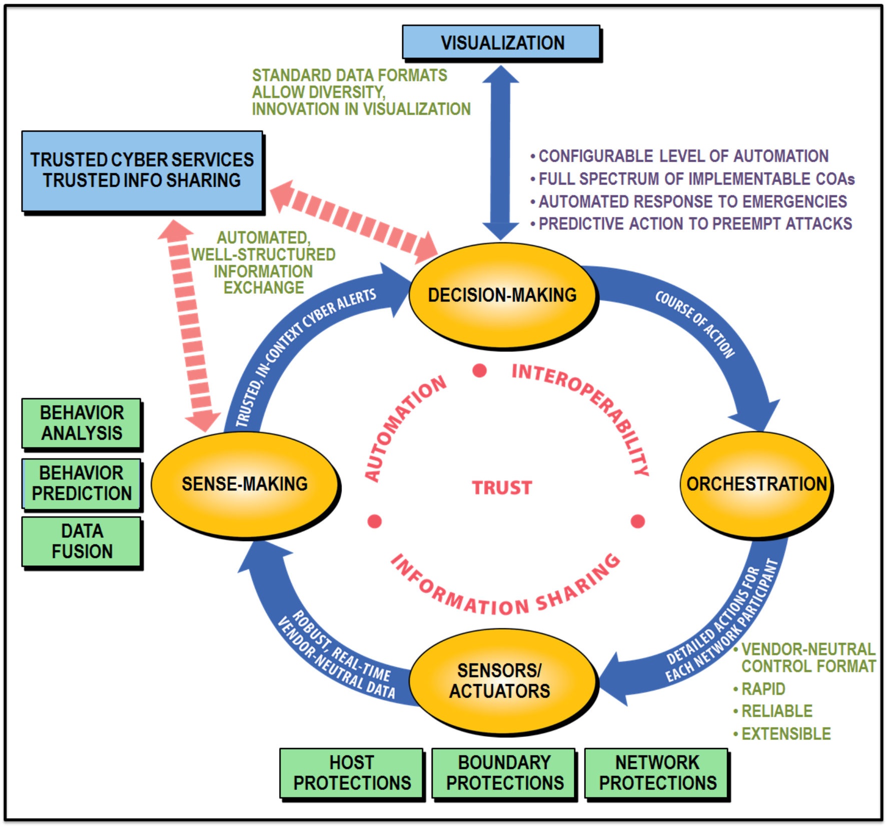

VISUALIZATION
STANDARD DATA FORMATS ALLOW DIVERSITY, INNOVATION IN VISUALIZATION
• CONFIGURABLE LEVEL OF AUTOMATION
• FULL SPECTRUM OF IMPLEMENTABLE COAs
• AUTOMATED RESPONSE TO EMERGENCIES
• PREDICTIVE ACTION TO PREEMPT ATTACKS
TRUSTED CYBER SERVICES TRUSTED INFO SHARING
AUTOMATED, WELL-STRUCTURED INFORMATION EXCHANGE
DECISION-MAKING
TRUSTED, IN-CONTEXT CYBER ALERTS
COURSE OF ACTION
AUTOMATION
INTEROPERABILITY
TRUST
INFORMATION SHARING
BEHAVIOR ANALYSIS
BEHAVIOR PREDICTION
DATA FUSION
SENSE-MAKING
ORCHESTRATION
ROBUST, REAL-TIME VENDOR-NEUTRAL DATA
DETAILED ACTIONS FOR EACH NETWORK PARTICIPANT
SENSORS/ ACTUATORS
• VENDOR-NEUTRAL CONTROL FORMAT
• RAPID
• RELIABLE
• EXTENSIBLE
HOST PROTECTIONS
BOUNDARY PROTECTIONS
NETWORK PROTECTIONS

Figure 1 (b) Desired End-state

- Identify how to bring together the right individuals and organizations to form this community.
- Scope the effort by further refining the framework presented in this document, including identifying what components require definition and standardization.
- Further develop use-cases and requirements for each layer of the message fabric (message set, services, and transport), and define interfaces and interactions among them.
- Define message fabric specifications.
- Identify candidate message fabric solutions and evaluate those solutions, validating with lab experiments and demonstrations.
- Recommend a path forward and create a roadmap.

A high-level process of community collaboration is depicted in Figure 2.

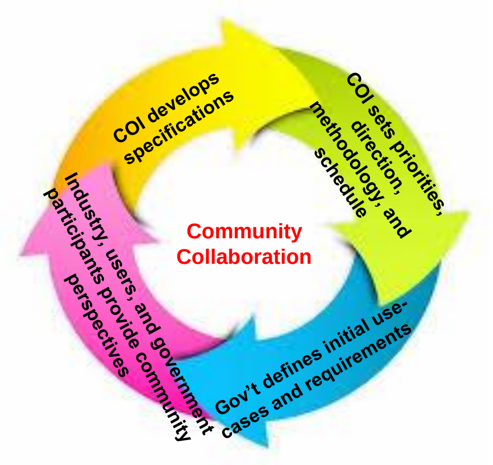

COI develops specifications
COI sets priorities, direction, methodology, and schedule
Community Collaboration
Gov't defines initial use-cases and requirements
Industry, users, and government participants provide community perspectives

Figure 2. Community Collaboration Model

Business Case for Standardization of Message Fabrics

Standardization of the message fabric for the exchange of security-relevant data among discrete cybersecurity and network management products can enable compelling business cases at the enterprise level:

- **Multi-vendor ecosystem.** An organization can incorporate multiple tools from diverse vendors and they all plug and play together seamlessly.

- **Flexible deployment and support for future migrations.** An organization can deploy a new application or product without having to redesign the existing enterprise, perform custom integration with multiple existing products/interfaces, or use vendor proprietary pairwise integration. They may maintain their existing message fabric capabilities (transport, services, message sets, and APIs/descriptors) with minimal, easily managed configuration updates. An organization may choose to procure and install a different vendor's Sense-Making (SM), Decision-Making (DM), or acting module and only require minimal reconfiguration of connections or services.

- **Rapid and automatic exchange of security-relevant data.** Secure and reliable intra-enterprise data exchanges facilitate interoperability, machine-speed information sharing, and automation in a dynamic environment. For instance, the identification of a cyber threat can be immediately shared across multiple orchestration products and those products can send commands to multiple types of actuator managers for action. The orchestration technologies and actuator managers can be from different vendors and support different types of endpoints (e.g., mobile, virtualized), but can expect to communicate using a common message set and commonly understood message services.

- **Baked-in security and information sharing into the architecture.** A message fabric with capabilities tailored to the intended environment and application provides an ideal foundation for secure and reliable message exchanges and support for common data models.

- **Appropriate abstraction.** An organization can utilize their choice of secure orchestration solutions without tying abstract cyber defense courses of action to a specific underlying message fabric instantiation.

Hence, a common intra-enterprise message fabric enables multi-vendor ecosystems, flexible deployment of new tools, rapid and automatic exchange of security-relevant data, baked in security and information sharing, and appropriate abstraction of commands.

Representative Message Fabric Components

The COI that comes together will define the desired message fabric that provides the necessary interoperability. A notional concept is depicted in Figure 3 and explained below:

- A set of commonly understood application interfaces/descriptors usable by any tool or information source to plug-in to the fabric [Technical Interoperability]
- A standardized message set that establishes the contextual constructs and data formats to understand the message in the intended way [Semantic Interoperability]
- A consistently defined set of message services (supporting control, configuration, publish/subscribe, etc.)
  - Requires an understanding of which services must be consistent across all users and which should be reserved to be enterprise-specific in their configuration
  - Includes a set of configurable trust and access services that enables secure communications with confidentiality, integrity, and availability.
- A set of transport protocols

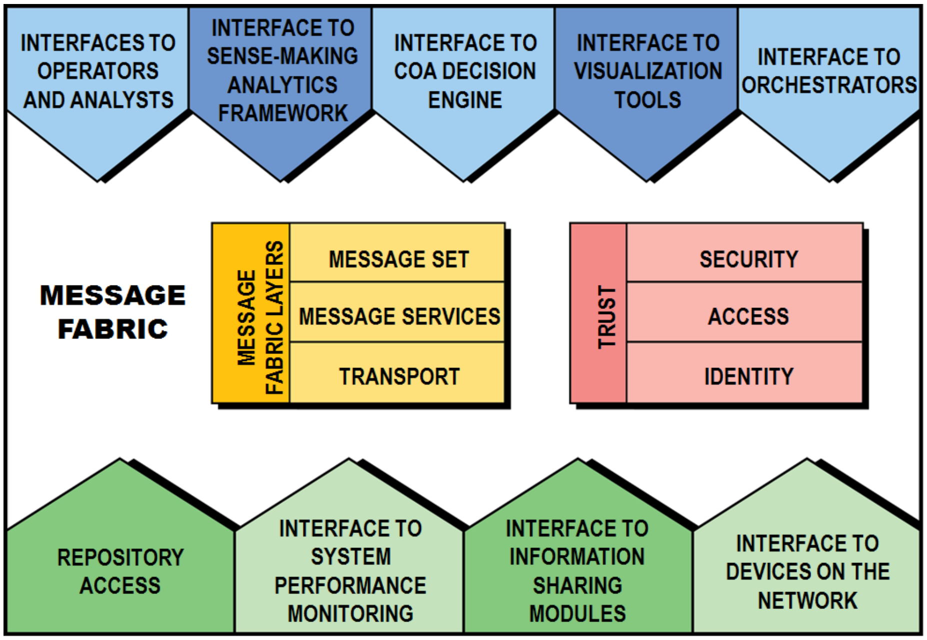

INTERFACES TO OPERATORS AND ANALYSTS
INTERFACE TO SENSE-MAKING ANALYTICS FRAMEWORK
INTERFACE TO COA DECISION ENGINE
INTERFACE TO VISUALIZATION TOOLS
INTERFACE TO ORCHESTRATORS
MESSAGE FABRIC
MESSAGE FABRIC LAYERS
MESSAGE SET
MESSAGE SERVICES
TRANSPORT
TRUST
SECURITY
ACCESS
IDENTITY
REPOSITORY ACCESS
INTERFACE TO SYSTEM PERFORMANCE MONITORING
INTERFACE TO INFORMATION SHARING MODULES
INTERFACE TO DEVICES ON THE NETWORK

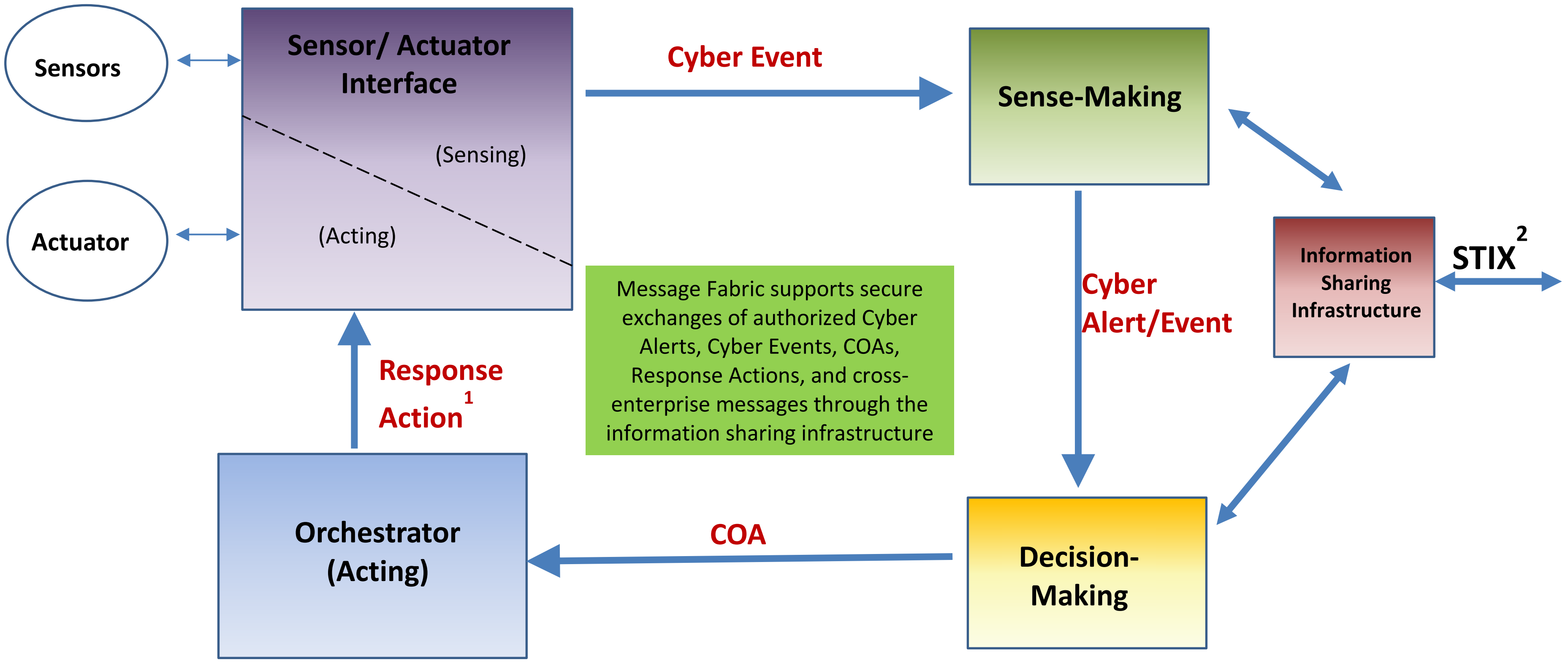
Figure 3. Representative Components of a Message Fabric

The message fabric components should be logically distinct and support a layered architectural approach such that an abstract layer can be compatible with multiple concrete supporting layers. As an example, Open-C2 has defined an abstract language to express the command and control response actions using a layered approach. This layered approach provides flexibility, supports a wide range of deployment environments, and minimizes the engineering required to support a new implementation layer. The same approach should be considered for the message fabric in general so that vendor products can more easily support a broad range of deployment environments and requirements.

Initial Use Cases

An initial set of integration and automation use-cases/scenarios were defined to describe representative messages and elicit capability needs and standards drivers for the message fabric. These scenarios involve interconnecting sensing, sense-making, decision-making, acting, and cross-enterprise information sharing, while leveraging automation wherever possible. Figure 4 shows how the message fabric fits into this notional cybersecurity enterprise containing a sensing, sense-making, decision-making, and acting loop with connectivity to an external messaging infrastructure. In Figure 4:

- “Sensor/Actuator” interface generates cyber events and passes them to the SM module.
- Sense-Making module generates cyber event and cyber alert messages and passes them to a Decision-Making module.
- Decision-Making module generates Course of Action (COA) messages and passes them to an orchestrator (or acting) module. While not explicitly shown, orchestrators may also send COAs or workflows derived from COAs to other orchestrators.



Message Fabric supports secure exchanges of authorized Cyber Alerts, Cyber Events, COAs, Response Actions, and cross-enterprise messages through the information sharing infrastructure

[1] Work in progress by Open C2 Forum

[2] Established standards and specifications

Figure 4. Primary Use for the Message Fabric

- The orchestrator generates response actions to the sensor/actuator interface in order control the sensors and actuators.
- The message fabric supports all of the above data exchanges, as well as connectivity to an external (outside of enterprise) data-message transport infrastructure.
- While not explicitly shown, human operators may also generate IACD message flows through human interface translators contained within the SM, DM, and orchestration components.

Use-Cases Fully Contained within a Single Enterprise

- **Adding new sensors, actuators, response actions, and COAs:** Updates the sense-making, decision making, and response capabilities as needed.
- **Adding new sense-making, decision-making, and response capabilities.** Add new tools to analyze sensor data, determine a course of action, or execute a course of action. Configure authentication and authorization policy for new tools.
- **Compliance checking and automated return to compliant state**. Assess the network and automatically remediate non-compliant system. Appendix A provides additional detail on the specific case of a Compliance Scan and Automatic Remediation.

Use-Cases Involving Collaboration with External Enterprises

- **Indicator/tipping or COA received from external source and initiation of automated cyber response.** Automatically update internal sensors and sense-making processes based on indicators received from external sources. Evaluate a proposed COA to understand the impact on the network and missions.
- **Generation and sharing of Indicators/Tips for Sharing/Direction.** Automatically generate host and network indicators, analytics, and mitigation strategies for a specific threat and share them with the situational awareness centers and the community using appropriate privacy safeguards.
- **Auto-enrichment of troubleshooting/analyst activity.** Automatically obtain additional information about initial indicators of a potential cyber event. Appendix A provides additional detail on the specific case titled “Enrichment After Finding a New File on the Network”
- **Detection and mitigation of risks.** Automatically detect risk conditions; select a course of action; execute course of action to mitigate vulnerability, threat, or impact, and share any indicators of compromise with the community. Mitigations include, but are not limited to, increased passive monitoring, deployment of signatures, removal of files, access restrictions, and mitigating configurations. Appendix A provides additional detail on the specific case titled “Malware Detection and Remediation”.
- **Continuity of operations and regeneration in support of mission assurance.** Automatically respond to major cyber incidents that degrade enterprise operation. Automatically determine a course of action to repair or replace degraded or unavailable cyber resources, and provide situational awareness to other enterprises.
- **Third party service support.** Enable third party services to implement sensing, sense-making, decision-making, and /or orchestrator functions.

Initial Representative Requirements for the Message Fabric

The scenarios and associated use-cases will identify the interfaces and underlying message system and transport characteristics that must be standardized to achieve interoperability. Some of these, such as network capacity, latency, reliability, and quality of service requirements will derive from the operational characteristics of the computing environment. For example, representative message fabric requirements could include:

- **Support sensing, sense-making, decision-making, and orchestration functions.** The message fabric needs to support the intended applications in the intended operational environment.
- **Message/data buffer and storage.** At times, some components will receive high data volumes that need to be managed. For instance, the volume of sensing data often fluctuates significantly.   Although the peak data volumes may be higher than the receiving component can process, it is important not to drop the data at any time. The message fabric should be able to support high speed data buffer and storage capabilities to handle high data volumes during peak times.
- **Message/data exchange priority treatment.** Some data exchanges may be considered to have a higher priority than other data. The message fabric should be capable of delivering the data in an order consistent with established priorities.
- **Message/data distribution and load-balancing.** Sometimes, components work in parallel to process similar data. For example, more than one Sense-Making component may receive cyber events. When required, the message fabric should be capable of distributing the data based on pre-defined load balancing schemes.
- **Guaranteed message delivery.** The message fabric should support delivery guaranteed to a pre-defined level, handling packets that arrive out of order or are duplicated. It also needs to enable recovery and retransmit of lost messages.
- **Maximum throughputs and latency.** The message fabric should support various throughputs and latencies to pre-defined levels.
- **Transport service monitoring and management.** The message fabric should be capable of managing and monitoring message transport utilization, message loss rate, delay, jitter, and out-of-order message delivery to support auditing, configuring, and repair/replacement as needed.
- **Transport performance reporting.** The performance of the transport layer should be able to be provided to human operators.
- **Compatibility with an external cross-enterprise infrastructure.** The message fabric transport layer should enable transferring of messages within the enterprise and to/from the external message fabric infrastructure with minimal translation required. External (outside of enterprise) indicators, cyber events, cyber alerts, and defensive measures are transported via an external data-message transport infrastructure utilizing Structured Threat Information eXpression (STIX) and Trusted Automated eXchange of Indicator Information (TAXII) formats.
- **Distributed enterprise over wider area network.** The message transport should be capable of delivering data and messages across a distributed network topology with potentially high packet loss rates and long latencies, consistent with established message priorities.

The COI will need to define other requirements, such as those associated with secure data exchanges, authorization mechanisms, authorization policy, and access control. There may also be a need to capture unique requirements for different computing environments, such as traditional on-premises computing, extended enterprises, industrial control systems, cloud computing, and security as-a-service.

Conclusion and Next Steps

This paper establishes an initial framework to enable cross-community discussion, exploration, and collaboration on message fabric interoperability and standardization. Our goal is the formation of a self-sustaining community of vendors, government, academia, and CIKR members representing a community of cybersecurity and network management solutions providers, messaging and orchestration providers, system integrators, operators, users/consumers, and acquisition programs who will come together to define common message fabrics and common data models to ensure interoperability between diverse commercial cyber security tools. The desired end-state is COI-developed message fabric interoperability specifications that enable enterprises to easily adopt and securely integrate diverse sensors, actuators, analytics, orchestration/decision support products and network management tools to enable enterprises to respond to dynamic cybersecurity threats in a timely manner.

The community that emerges to address this topic will ultimately need to develop and execute a plan. Some candidate next steps for this community are:

- Document a consensus view of the problem to be addressed and define the characteristics of a successful outcome.
- Scope the effort by further refining the framework presented in this document, including identifying what components require definition and standardization.
- Identify how to bring together the right individuals and organizations to form this community.
- Further develop use-cases, derive requirements for each layer of the message fabric (message set, services, and transport), and define interfaces and interactions between the message fabric layers.
- Define message fabric specifications
- Identify candidate message fabric solutions and evaluate those solutions, validating with lab experiments and demonstrations
- Recommend a path forward and create a roadmap.

Appendix A. Additional Detail for Representative Use-Cases.

1.0 Compliance Scan and Automatic Remediation

An administrator elects to perform a compliance scan on the network. Through the management interface, the operator selects the Compliance Scan COA. The acting component of IACD receives the COA and issues Response Actions to scanners. Scanners return compliance reports to Sense-Making (SM). SM raises a non-compliance cyber alert to Decision-Making (DM). DM recommends a COA for remediation to the administrator, who then authorizes the COA. Acting receives the COA and sends Response Actions to multiple actuators to change the host configurations. The actuators return the resulting configuration changes through the Sensor/Actuator Interface, which are published to the Configuration Repository and SM. SM determines that the non-compliance issues are resolved.

2.0 Enrichment After Finding a New File on the Network

A sensor discovers a new file on the network. SM is unable to make a determination about the file from the initial sensor data. DM elects a COA for automated enrichment. The enrichment COA has two parallel activities, requesting information from an external service (e.g., VirusTotal) about the file and detonating the file locally for analysis (e.g., FireEye). The external service and detonation both provide results back to Sense-Making.

3.0 Malware Detection and Remediation

Sensors detect a process that violates specifications. After auto-enrichment of the initial cyber event, SM sends a cyber alert to DM. DM recommends a COA with actions to quarantine the infected host and develop signatures for the unknown malware. Acting issues response actions to quarantine the host and issues a ticket to an analyst to develop the malware signatures. The analyst develops the new signature; an operator issues commands to deploy the signature and share it with the community. Acting executes a workflow to deploy the signature and share it with the community. The new signature is deployed to sensors, including those on the infected host. The host's anti-malware sensors and actuators remove the malware and generate a cyber-event. SM determines that the host is no longer infected and issues another cyber event. DM receives the cyber event and determines that the quarantine can be lifted on the host.