JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

11100 Johns Hopkins Road • Laurel, Maryland 20723-6099

Integrated Adaptive Cyber Defense (IACD) Baseline Reference Architecture

Version 1.0

CHANGE LOG

This table summarizes the changes made with each release of this document.

Document	Date	Description
Release 1.0	January 2016	Initial graphical and functional views.
Version 1.0	December 2016	Create a baseline architecture document based upon Release 1.0 and updated to include orchestration services, use cases, spiral mapping to architecture and glossary.

CONTENTS

FIGURES

TABLES

1. INTRODUCTION

The Integrated Adaptive Cyber Defense (IACD) project was initiated in 2014 by the Department of Homeland Security (DHS) and the National Security Agency (NSA) in response to malicious cyber threats against government, commercial, and academic enterprises. Such threats are increasingly sophisticated yet surprisingly easy to act upon given the widespread availability of shared malware information. Current cyber defense practices rely heavily on the speed and skill of human cyber defenders. Unfortunately, these human-centered practices cannot keep pace with the speed and volume of current threats. IACD addresses the problem of cyber defense in two key areas: 1) it automates cyber defense tasks currently performed by human defenders; and 2) it shares threat information with other enterprises. Automation reduces the time to detect and respond to cyber threats. Information sharing across enterprises limits the reusability of such threats against other enterprises.

1.1 Purpose of this Document

The purpose of this document is to provide an updated description of the concept, general functions, and architectural construct for IACD. It reflects recent research, analysis, and experimentation. It is not a traditional systems engineering document, but rather a framework with which vendors, users, and stakeholders can consider the critical components of IACD to determine what is necessary to integrate a variety of products to meet the specific needs of a given enterprise. The document presents the tenets of IACD and describes the evolving concept and elements of IACD. It describes the use cases examined and lists the commercial products employed thus far in IACD development and research. Finally, it identifies the anticipated minimum set of specification and standards necessary to ensure IACD interoperability.

1.2 IACD Tenets

IACD has three driving tenets that have influenced the architecture, capability definitions, and operations concepts:

- Bring your own enterprise. IACD acknowledges that enterprises have different missions, business process rules, and resources and therefore may implement IACD differently.
- Product-agnostic plug-and-play architecture. IACD must be flexible enough to support a range of enterprise environments, technologies, resources, and levels of sophistication.
- Interoperability. Proprietary products must function together via non-proprietary methods.

The challenge posed by the "bring your own enterprise" model is that each enterprise brings its own unique collection of heterogeneous defense mechanisms (e.g. perimeter protections, internal network protections, host-based protections), security information systems, and management systems. IACD must meld these components into an automated cyber defense system. If this challenge can be met, research indicates that the automation of cyber defense tasks can dramatically reduce detection and response times. As in many other fields, shifting human labor away from voluminous, repetitive tasks is an opportunity to better employ human talent and raise productivity.

1.3 IACD Concept: Operationalizing the OODA Loop for Cyber Defense

IACD was conceived with the idea that we could dramatically improve the timeliness and effectiveness of cyber defenses by:

- Addressing speed and scale via automation and integration
- Providing dial-able levels of automation to support operational priorities and gradual development of trust in automation
- Ensuring trusted, secure control driven by network owner rules
- Enabling flexible, affordable solutions via commercial products that leverage existing and emerging interoperability standards

Essentially, IACD seeks to adapt a traditional control and decision approach from the physical world and apply it in cyberspace. The OODA Loop (Observe-Orient-Decide-Act) can, if implemented at speed and scale, drive cyber operations timelines from months to minutes to milliseconds.

The IACD concept transforms the OODA Loop activities into sensing, sense-making, decisions making, and acting and envisions the sharing of information across these activities through a common messaging system. This messaging system likewise shares information with other entities to achieve shared situation awareness. Figure 1 illustrates an early approach to the transformation of the OODA Loop to the IACD concept.

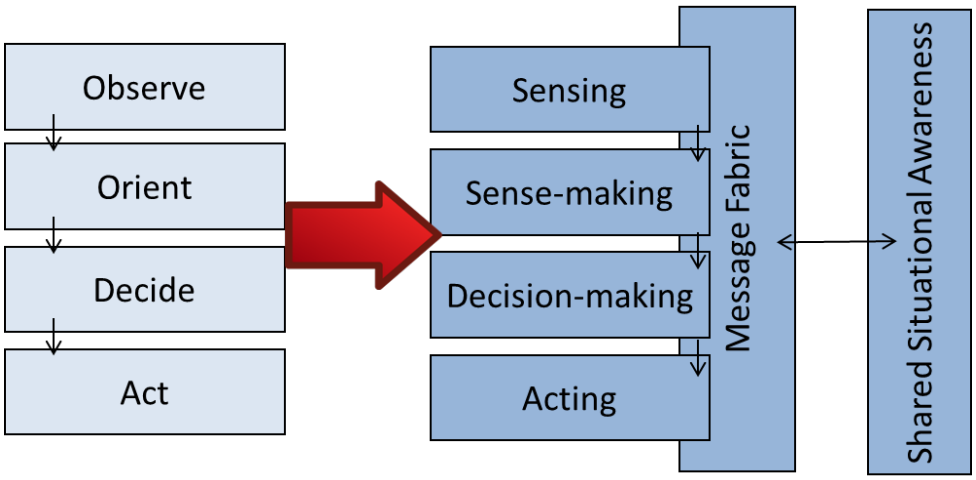

Figure 1. OODA Loop to IACD Concept

1.4 Evolution of IACD Architecture

The IACD project used a series of agile development spirals to identify and implement the capabilities needed for automated cyber defense. These efforts focused on the integration of commercial products. As a result of experimentation and testing, the IACD architecture has

evolved over time into the description that follows. **Figure 2** illustrates the basic flow and timeline of this evolution.

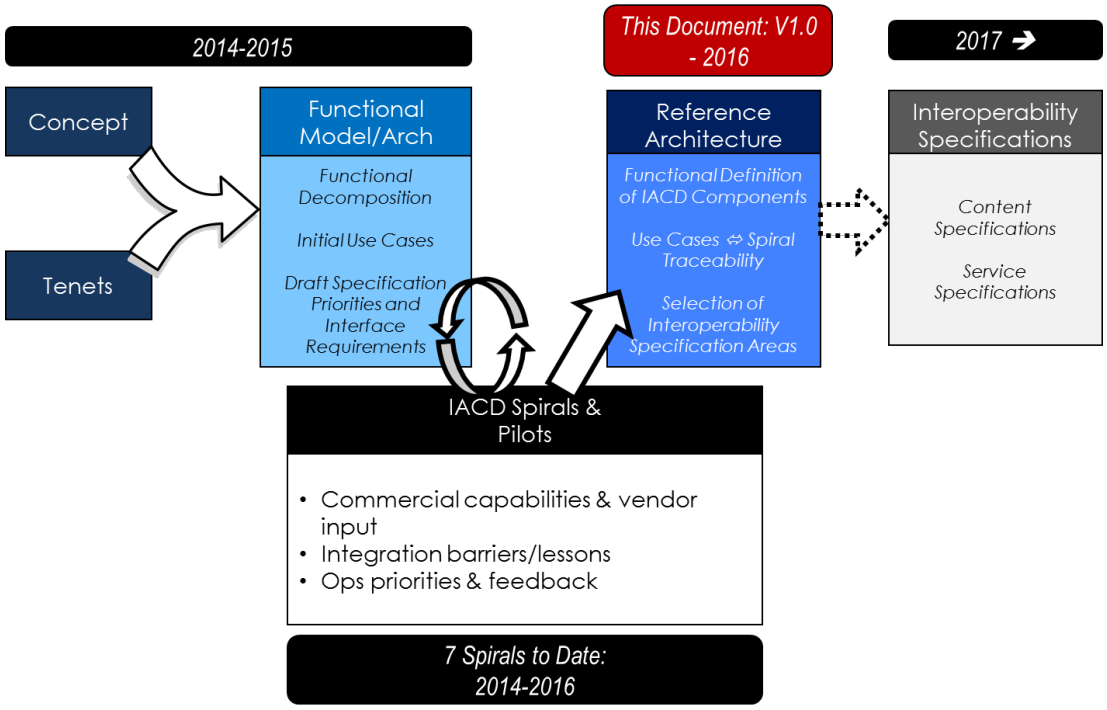

Figure 2. Evolution of IACD

The initial IACD concepts and tenets led to a functional model that identified the major IACD components and interfaces. Thereafter, development spirals and pilot projects employed a number of use cases to refine the functional model. The functional model was documented in two IACD publications in September 2015 and January 2016 (see References). While some may find these documents useful for background information, their chief purpose was defining the core components of IACD and identifying the **minimal set of commonly needed capabilities**.

2. IACD REFERENCE ARCHITECTURE COMPONENTS

This IACD Reference Architecture transforms the IACD conceptual model to the set of components depicted in **Figure 3**. This figure illustrates how the elements of IACD fit within an enterprise and work with existing infrastructure, defensive, and management elements. Subsequent sections decompose this figure and describe how the interfaces among these capabilities may drive emerging interoperability specifications.

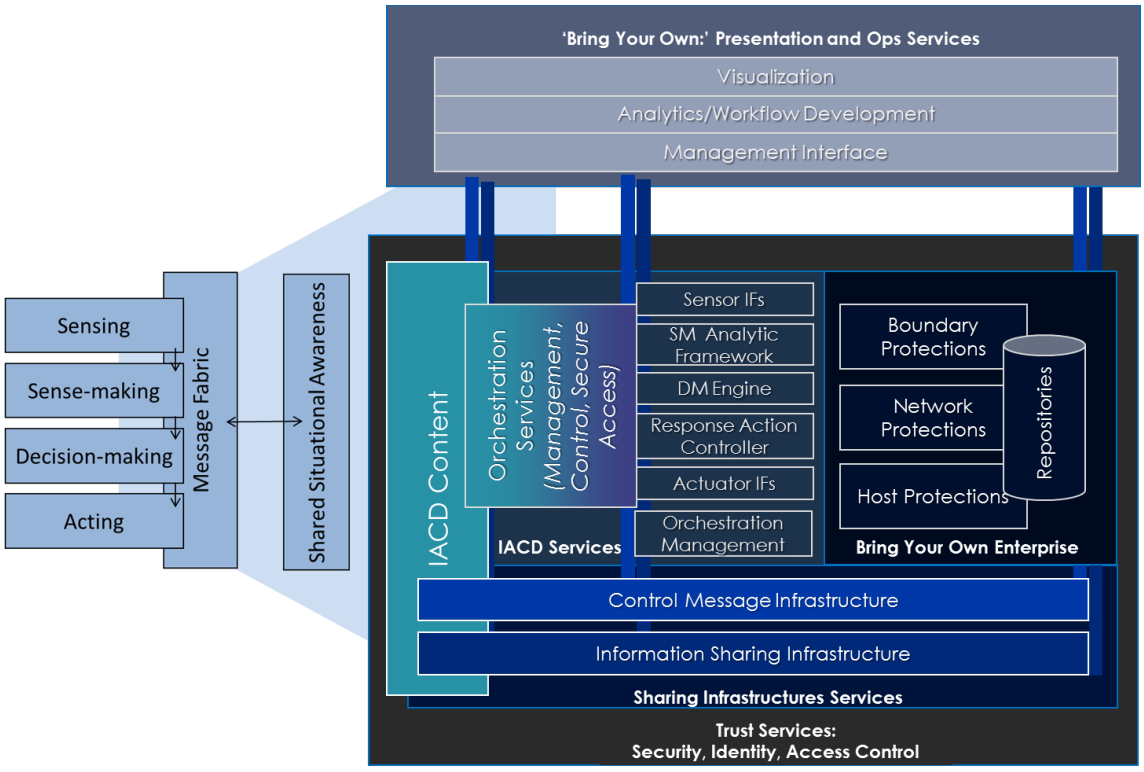

Figure 3. Enterprise View of IACD Reference Architecture Components

2.1 IACD Key Logical Components

The key components of IACD can be logically described as either **services** or **content**. **Services** are components that perform specific IACD functions. The use of the term, services, supports the concept of "plug and play" components that either perform these functions within an enterprise or provide them externally through some form of subscriber service. **Content** is the information entering or exiting IACD services. Both services and content are necessary to perform IACD. Understanding their structure and interactions is the key to achieving interoperability between "plug and play" components.

The **IACD Services** depicted are:

Orchestration Services
Including managing the integration and automation of these functions:
- Sensor and Actuator Interfaces
- Sense-Making Analytic Framework
- Decision-Making Engine(s)
- Response Action Controllers
- Orchestration Management

Sharing Infrastructure Services
- Control Message Infrastructure - message Services executed over designated transport
- Information Sharing Infrastructure - exchange Services executed over designated transport

Trust Services

- Security, Identity, Access Control, and Policy Enforcement services

The **IACD Content** includes:

- Cyber Events entering the IACD services
- Response Actions exiting the IACD services
- Alerts created by IACD services
- Courses of Action (COAs) implemented via the IACD services
- Indicators/Shared Cyber Defense Information into and out of shared situational awareness

Section 5 in this document introduces the approach to interoperability specifications derived from this IACD architecture.

2.2 Orchestration Services

Logically, **orchestration services** refer to the managed automation and integration of the OODA Loop-derived activities: sensing, sense-making, Decision-Making, and acting. There are five discrete services that make up orchestration services in IACD: Sensor/Actuator Interface, Sense-Making Analytical Framework, Decision-Making Engine, Response Controller, and Orchestration Management. The combination of sensor and actuator interfaces recognizes the dual role of components that both sense and respond to cyber events. An example would be a firewall that can both sense malicious penetration efforts and, under the direction of IACD, respond against them. **Figure 4** depicts the set of orchestration services in the form of an OODA loop and illustrates the basic flow of content between them.

The basic **content** categories are: cyber events, alerts, alert actions, COAs (courses of action), workflows, and response actions. These content categories are further described below.

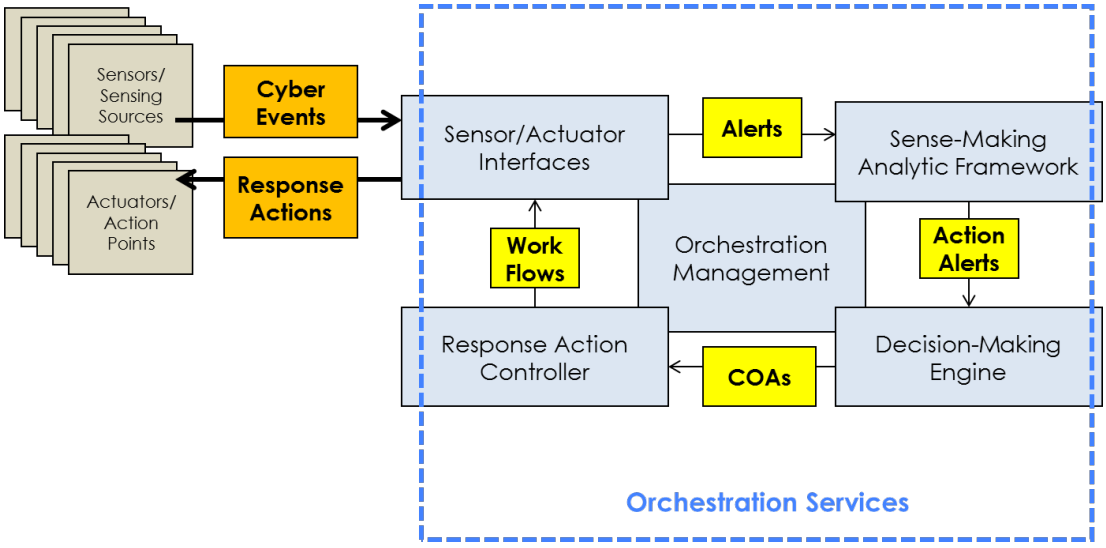

Figure 4. Orchestration Services

2.2.1 Sensor/Actuator Interface (Sensing)

The first step in the IACD OODA loop is sensing. It occurs when the Sensor/Actuator Interface receives notification of a ***cyber event*** from enterprise sensors. Based on enterprise-defined policies and processes, the Sensor/Actuator Interface will determine that either the ***cyber event*** requires further action or it does not. If further action is required, it will pass the ***cyber event*** information to the Sense-Making Analytic Framework as an ***alert.*** Otherwise, it will simply log the ***cyber event***.

2.2.2 Sense-Making Analytic Framework

If the Sense-Making Analytic Framework receives an ***alert***, it will—based on enterprise policies and processes—perform a number of operations (i.e. a particular analytic workflow) to enrich the alert information. It will query internal or external data sources for sightings of similar behavior, file hashes, etc. In the case of a malware file, it may send the file to a file detonation service. Based on the enriched information and enterprise policies and processes, the Sense-Making Analytic Framework will determine whether further action is required or not. If further action is required, it will pass the enriched information as an ***action alert*** to the Decision-Making Engine. If no further action is required, it will simply log its activities.

2.2.3 Decision-Making Engine

Upon receipt of an ***action alert***, the Decision-Making Engine will determine—based on enterprise policies and processes—what Course of Action (COA) is appropriate. For example, a selected COA might block all traffic from a specific internet address or quarantine a specific host system. A number of COAs may be appropriate. It is possible that enterprise policies and processes require the notification and involvement of a human decision maker. It is also possible that no enterprise COA exists for a given action alert and the Decision-Making Engine may seek possible COAs from an external source. Once a COA is selected, the Decision-Making Engine will pass the selected ***COA(s)*** to the Response Controller.

2.2.4 Response Action Controller

The Response Controller translates the ***COA*** into a machine translatable ***execution workflow***, which it sends to the Sensor/Actuator interface.

2.2.5 Sensor/Actuator Controller (Acting)

Upon receipt of an ***execution workflow***, the Sensor/Actuator Interface translates the workflow into device-specific response actions that it sends to the appropriate enterprise sensors and actuators.

2.2.6 Orchestration Management

Orchestration management marshals the configuration and flow of information across the other orchestration services. It also provides the mechanism for both operator and electronic interface to orchestration services.

2.2.7 Interface Points

IACD Orchestration Services are not complete until interface points allowing for use and control of the services are provided. The two general interface point types are the Information Interface and the Management Interface, as shown in **Figure 5**. They mimic a standard network management view of capabilities, acknowledging that both information/data flow as well as management flow are needed to and from a component.

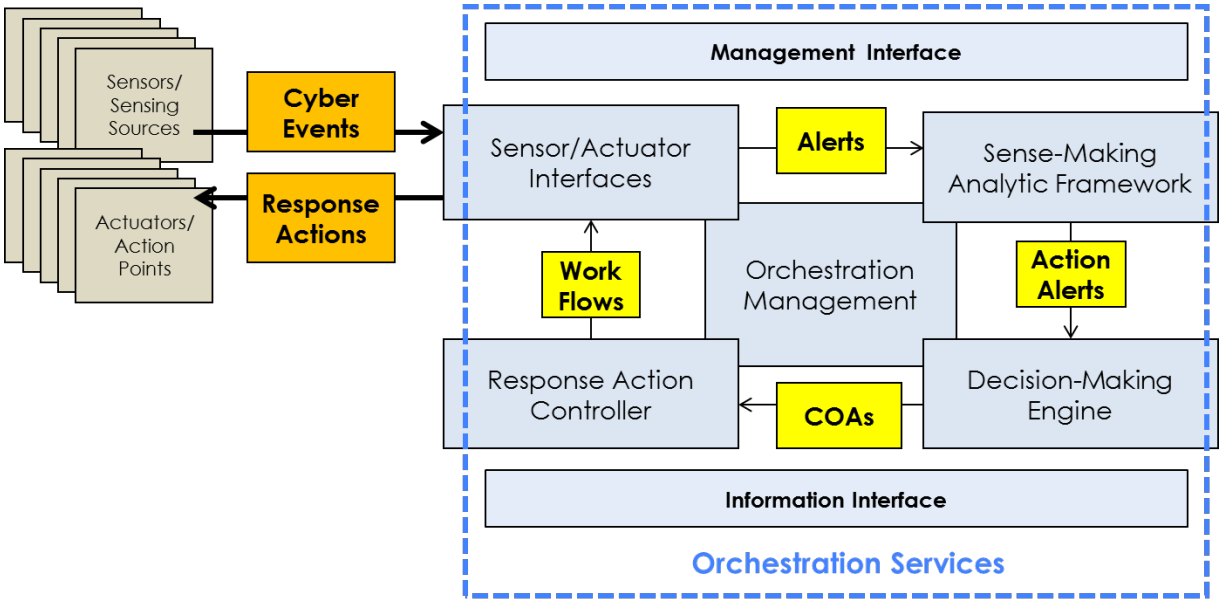

Figure 5 Orchestration Services with Interface Points

2.2.7.1 Information Interface

The Information Interface enables ingest and output of information external to the IACD Orchestration Services. It provides the logical data or information handling capabilities necessary to interface in the broader enterprise. At a minimum, the information interface must provide the mechanism to connect to the native information layer in the enterprise it is serving. It could, however, expand to include activities such as data marshaling, normalization, etc. The minimal commonly needed set of information interface functionality is still evolving, and will be updated in future iterations of the IACD architecture.

2.2.7.2 Management Interface

The Management Interface is the means by which the enterprise monitors, assesses, and controls IACD. It is the conduit for implementing and enforcing enterprise policies and processes in the form of workflows and decision criteria within workflows. It is also the means for defining and collecting analytics which can affect changes as necessary to enterprise policies and processes. The interface, at a minimum, must be able to integrate with existing presentation services, but could expand to include features such as workflow validation and policy enforcement. The

minimal commonly needed set of information interface functionality is still evolving, and will be updated in future iterations of the IACD architecture.

2.3 Sharing Infrastructure Services

The IACD Message Infrastructures provide and support IACD messaging *within* and *external* to the defended enterprise. There are two message/sharing infrastructure elements: Control Message Infrastructure and Information Sharing Infrastructure, as shown in Figure 6. Each infrastructure element consists of three parts: the underlying transport, the message service carried by the transport, and the content carried by the service. Current IACD specification activities will focus on the commonly needed content and service features. To date, experimentation and research has not identified a driver to specify transport layer details. However, experimentation and operational implementation will continue and may point to specific features and properties that need to be called out.

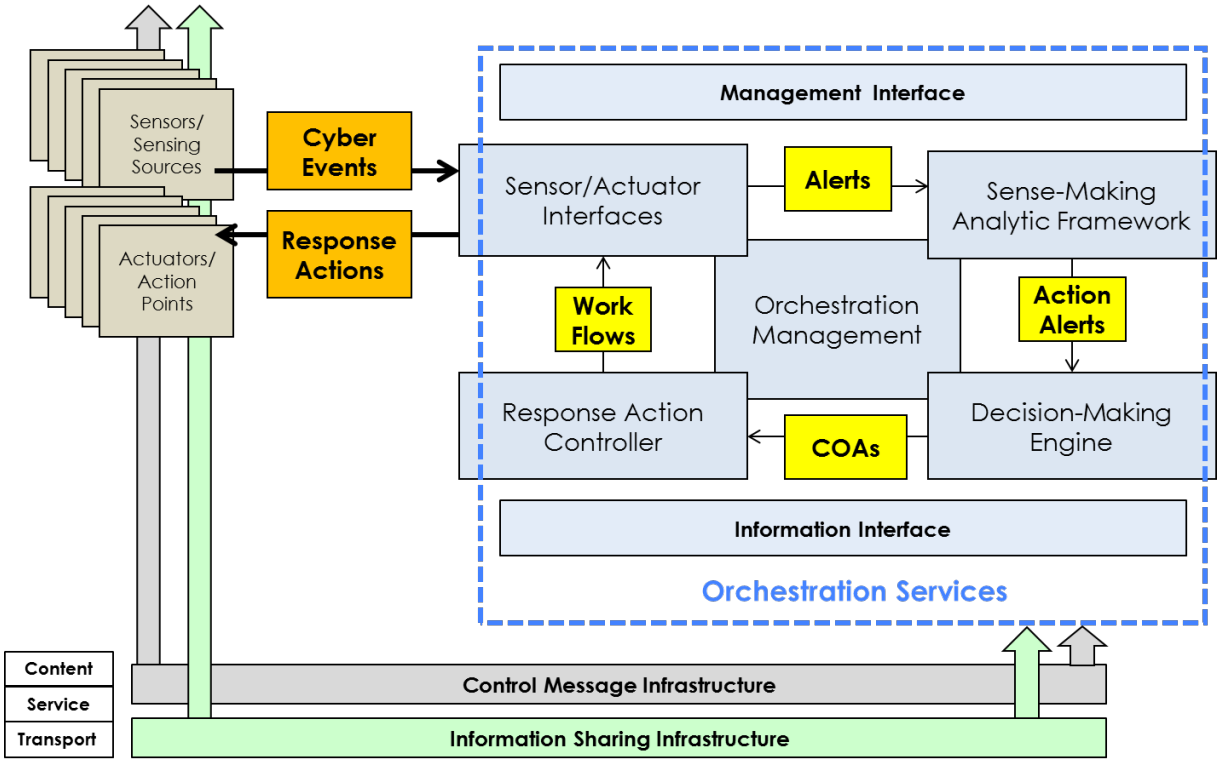

Figure 6. Sharing Infrastructure Services

2.3.1 Control Message Infrastructure

The Control Message Infrastructure enables high-reliability control and signaling of orchestration services and the components being orchestrated. The intent of separating this interface from the information infrastructure is to allow for the need to levy different latency, reliability, and availability constraints on the control messaging. As trust services and policy management/enforcement are further explored it is anticipated that there will specific messaging relevant to these services.

2.3.2 **Information Sharing Infrastructure**

In addition to the signaling required for control functionality within an IACD implementation, there is essential content/information that will flow within a defended enterprise ***as well as*** among multiple participants in sharing communities. The evolving information sharing infrastructure specifications will describe the commonly needed information management services intra-enterprise, as well as the inter-enterprise information sharing services required for machine speed ingest and output. These capability needs draw extensively from the Information Sharing Architecture developed under the Enhance Shared Situational Awareness initiative, and the Automated Indicator Sharing service.

At a minimum, an information sharing infrastructure must be able to accept Indicators and Course of Action (or shared defensive actions) and convey those as input into IACD, and to accept internal IACD items as output to enable their sharing outside of IACD. However, it is also clear that IACD implementations will generate information to include orchestration management and status information that may also need to be shared. The minimum set of information to be shared is still evolving, hence interface functionality will be updated in future iterations of the IACD architecture. As information sharing evolves, it may further expand to additional information such as known vulnerabilities, workflows, configuration guidance, etc.

2.4 Trust Services

A critical element to all IACD operations, content, and interfaces is the concept of trust. In Figure 7, this feature is portrayed in a very simplified manner as Trust Services, which must address all information exchanged among IACD components, enterprise elements, and non-enterprise elements. Cyber events, alerts, alert actions, indicators, COAs, workflows, response actions, etc. must be trusted by elements that receive them and act on them. Information related to orchestration management must also be trusted. Since IACD will be a pivotal point in enterprise cyber defense, it will be a high-value target of malicious cyber threats that may seek to penetrate and subvert it, cause it to automatically block or quarantine legitimate enterprise activities, or in general use its functionality for malicious purposes. Preliminary research has not yet revealed a minimal set of trust services; nonetheless research is ongoing and trust service functionality will be updated in future iterations of the IACD architecture.

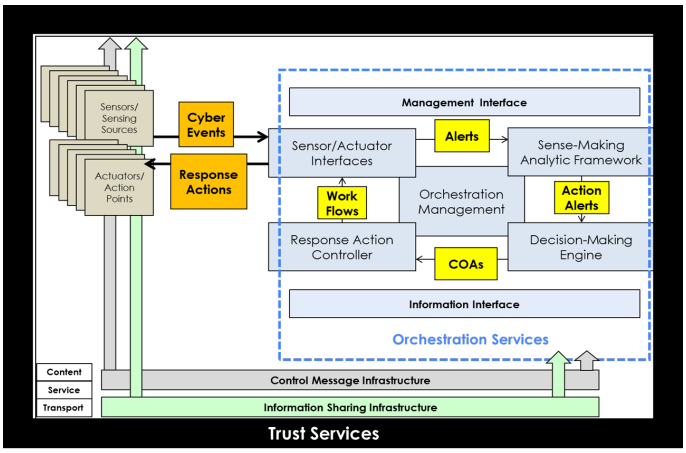

Figure 7. Addition of Trust Services

3. ORCHESTRATION USE CASES

Use cases are high-level descriptions of IACD functionality in terms of how actors (human or machine) use the system to achieve operational goals. The development of the IACD Reference Architecture has been heavily influenced by the analysis and demonstration of multiple use cases. As the IACD Reference Architecture evolves and matures, these use cases have at times been updated, replaced, or rendered obsolete by emerging discoveries. Table 1 summarizes the current set of use cases representative of IACD orchestration services. Appendix A contains more detailed use case descriptions and figures. For historical reference purposes, the aggregated list of prior IACD Use Cases is included in Appendix B.

Table 1. IACD Orchestration Use Cases

#	Use Case Name	Flow Orchestrated
1	Detection and mitigation of vulnerabilities	Query->Response produces identifier. Obtain vulnerability information from community and translate. Sense-Making (Identifier)-> Decision-Making (Triage) -> Response (COA)
2	Detection and mitigation of malware	Obtain threat information from community and translate. Sensing (File) -> Sense-Making (Detonate) -> Decision-Making (Results) -> Response (COA)
3	Detection, tipping, and mitigation of anomalous behaviors	Sensing -> Sense-Making -> Decision-Making (Triage)-> Response (COA). Create indicator for sharing.
4	Indicator received from external source and initiation of IACD response	Query->Response produces indicator. Obtain threat information from community and translate. Sense-Making (Indicator) -> Decision-Making (Triage) -> Response (COA)
5	Generation of Indicators/Tips for Sharing/Direction to other enterprises	Sensing ->Sense-Making. Create indicator for sharing.
6	Adding new sensing sources	
7	Adding new actuators	
8	Adding new response actions / COAs	

Future IACD development will look toward more advanced use cases that explore IACD detection and response to more advanced threats and/or require more complex responses.

4. IACD REFERENCE IMPLEMENTATIONS

To operationalize the IACD concepts, a series of prototype/experimental/assessment spirals have integrated real-world, commercial products into IACD reference implementations.

NOTE: The use of specific products in these spirals does not constitute endorsement of those products, nor does it imply that those products do not or could not perform IACD functions other than as depicted in the specific exercises. In general, products were selected based on feature set, availability, interoperability, and the objectives of a particular spiral, supporting the targeted use cases. **Appendix B** contains tables listing the products used during development spirals.

5. FUTURE EVOLUTION: INTEROPERABILITY SPECIFICATIONS AND STANDARDS

The IACD Reference Architecture defined in this document will continue to evolve based on lessons learned from experimentation, implementation, and prototyping and based on community feedback, research and feedback, and innovation. The intent of the reference architecture is to provide a common basis from which ***interoperability specifications*** can be derived or developed. The goal is to capture the least-constraining set of commonly needed services and content that enable the tenets of IACD (bring your own enterprise, plug-and-play, and interoperability). Over- specification risks the loss of interoperability, limits the design or employment of innovative solutions and may be counter to a level commercial playing field.

Figure 7 shows the service and content/data portions of the IACD Architecture that have been targeted to document candidate interoperability specifications. Where communities and/or standards bodies already exist, those will provide the conduit for IACD-related discussions. Where an existing community cannot be identified, interoperability can be ensured through continued engagement with commercial vendors and integrators, operational users, and researchers to transfer the knowledge gained and lessons learned from IACD activities to emerging efforts.

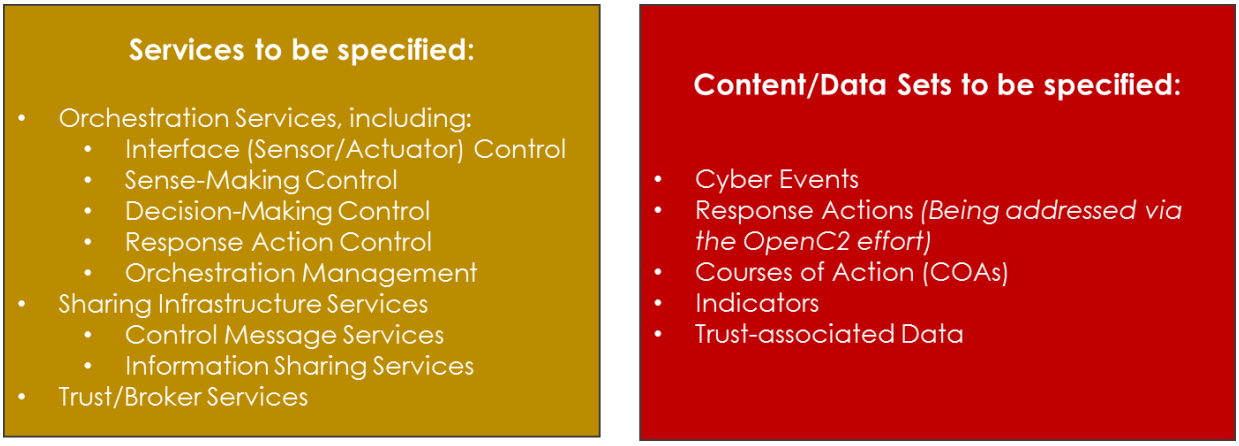

Figure 8. IACD Interoperability Specification Targets

Development of specifications for IACD content has the advantage of building on the significant work already underway as part of the OpenC2 program, which has been used in IACD experimentation to transmit commands. As noted above, the development of specifications for shared information has the advantage of building on the significant work underway by the AIS program.

The tables in Appendix A include candidate orchestration requirements, and posit candidate specifications associated with those requirements.

6. SUMMARY

This document is a baseline reference architecture for IACD. It includes a brief explanation of how IACD has evolved to its current form, which is based on the experiments and analysis of six development spirals and the integration of commercial products to perform IACD functions. A key theme throughout the development of the reference architecture has been the concept of minimum specification in the belief that over-specification will limit innovation, flexibility, and adoption. This document is not a traditional systems engineering document, but rather a framework for automated cyber defense. Significant work remains in the areas of trust, product integration, policy enforcement, and in refining the anticipated minimum set of specification and standards necessary to ensure IACD interoperability. Future updates will expand on these points.

7. REFERENCES

1. Integrated Adaptive Cyber Defense (IACD) Architecture and Functional Description Document, JHU/APL, AOS-15-0948, September 2015.

2. Integrated Adaptive Cyber Defense (IACD) Architecture Description and Graphical Views, AOS-16-0097, January 2016.

APPENDIX A. COMBINED USE CASES

1. Use Case Name: Detection and Mitigation of Vulnerabilities

Preconditions: Partner has identified new vulnerability			
Actors: Partner enterprise, Actuators			
Step	**Process**	**Orchestration Requirement**	**Specification**
1	Poll information sharing infrastructure. Queries the information sharing architecture to determine if any new messages have arrived.	poll information sharing architecture	query message format
2	Information sharing sends query response. If response is that there are new messages, information sharing sends messages. Parses the messages to separate the indicators and metadata.	receive and interpret polling response from information sharing architecture	response format
3	Vulnerability information sent to Sense-Making. Pass indicators and associated information to Sense-Making	-receive and parse indicator message -send indicator message to Sense-Making	indicator message format
4	Sense-Making processes the indicators and associated information		
5	Triage indicators sent to Decision-Making	Send triage indicator to Decision-Making	Triage indicator message format
6	Decision-Making applies logic and returns a decision whether vulnerability must be responded to. - Decision-Making Engine chooses COA based on decision.		
7	COA sent to Response Controller. Response controller receives COA and develops a workflow for actuators to carry out.	Send COA to response controller	COA message format
8	Workflow sent from Response Controller and sends to Actuators	Receive and forward workflow	Workflow message format

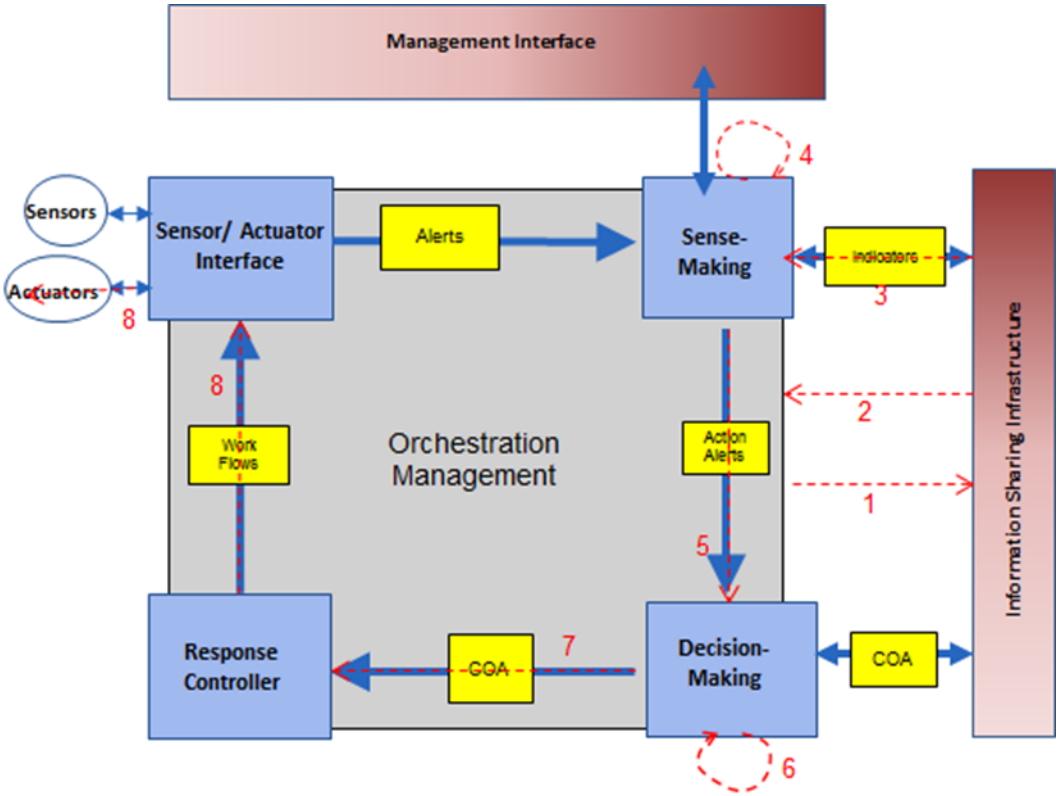

Figure 9. Detection and Mitigation of Vulnerabilities Use Case Flow

2. Use Case Name: Detection and Mitigation of Malware

Preconditions: Sensor has collected data that indicates a risk			
Actors: Sensors, actuators			
Step	**Process**	**Orchestration Requirement**	**Specification**
1	Alert and associated sensor data (e.g. file) is passed from sensor to sensor/actuator interface		
2	Alert and associated sensor data (e.g. file) sent to Sense-Making	Receive alert and associated sensor data, pass to sense-making	Alert message format Sensor data message format
3	Auto-enrichment Sense-making requests data. Data returns. Sense-making creates message indicating identified condition and associated risk.	Receive request for data from sense-making and pass to management interface. Receive data response from management interface and pass to sense-making.	Data request format Response data message format
4	Identified condition / risk sent to decision-making	Receive message indicating identified condition from sense-making and send to Decision-Making.	Identified condition / risk message format
5	Make decision Use identified condition and risk message to choose a COA to carry out.		
6	Send COA from decision-making to response controller. Response controller receives COA and develops a workflow for actuators to carry out.	Receive COA from decision-making and send to response controller	COA message format
7	Workflow sent to sensor/actuator interface	Receive and forward workflow	Workflow message format

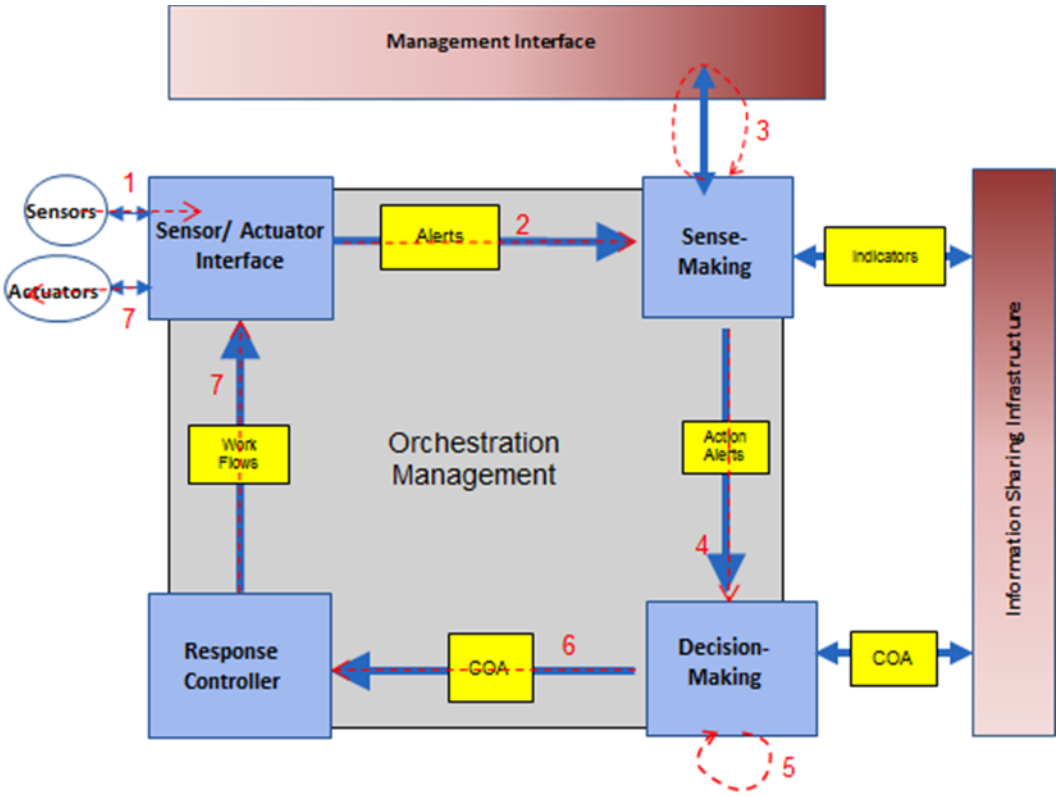

Figure 10. Detection and Mitigation of Malware Use Case Flow

3. Use Case Name: Detection, Tipping, and Mitigation of Anomalous Behaviors

Preconditions: Sensor has collected data that is an alert of anomalous behavior			
Actors: Sensors, actuators			
Step	**Process**	**Orchestration Requirement**	**Specification**
1	Alert and associated sensor data (e.g. file) is passed from sensor to sensor/actuator interface		
2	Alert and associated sensor data (e.g. file) sent to Sense-Making	Receive alert and associated sensor data, pass to sense-making	Alert message format Sensor data message format
3	Auto-enrichment Sense-making requests data. Data returns. Sense-making creates message indicating identified condition and associated risk. Sense-making creates alert to send to the community.	Receive request for data from sense-making and pass to management interface. Receive data response from management interface and pass to sense-making.	Data request format Response data message format
4	Triage indicators sent to Decision-Making	Send triage indicator to Decision-Making	Triage indicator message format
5	Make decision Use identified condition and risk message to choose a COA to carry out.		
6	Send COA from decision-making to response controller. Response controller receives COA and develops a workflow for actuators to carry out.	Receive COA from decision-making and send to response controller	COA message format
7	Workflow sent to sensor/actuator interface	Receive and forward workflow	Workflow message format
8	Send alert to community through information sharing infrastructure	Receive alert message and send to information sharing infrastructure	Alert message format

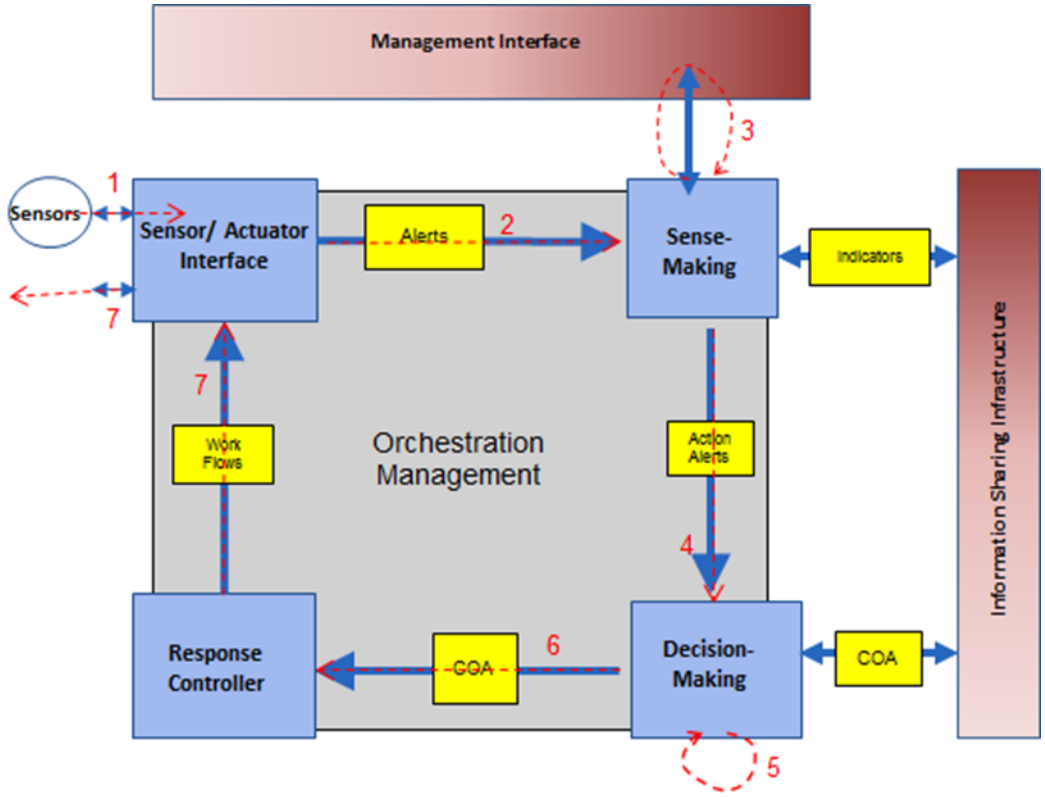

Figure 11. Detection, Tipping, and Mitigation of Anomalous Behaviors Use Case Flow

4. Use Case Name: Indicator Received from External Source

Preconditions: Partner has received new indicator			
Actors: Partner enterprise, Actuators, Analyst			
Step	**Process**	**Orchestration Requirement**	**Specification**
1	Poll information sharing architecture. Queries the information sharing architecture to determine if any new messages have arrived.	poll information sharing architecture	query message format
2	Information sharing sends query response. If response is that there are new messages, information sharing sends messages. Parses the messages to separate the indicators and metadata.	receive and interpret polling response from information sharing architecture	response format
3	Vulnerability information sent to Sense-Making. Pass indicators and associated information to Sense-Making	-receive and parse indicator message -send indicator message to Sense-Making	indicator message format
4	Sense-Making processes the indicators and associated information and sets up new analytic rule		
5	Human review of new analytic rule		
6	Recommendation for sensor update sent to decision-making	Receive recommendation message from sense-making and send to decision-making	Recommendation message format
7	Decision-Making applies logic and returns a decision whether sensor will be updated with new analytic rule		
8	COA sent to Response Controller. Response controller receives COA and develops a workflow for actuators to carry out.	Send COA to response controller	COA message format
9	Workflow sent from Response Controller and sends to Actuators	Receive and forward workflow	Workflow message format

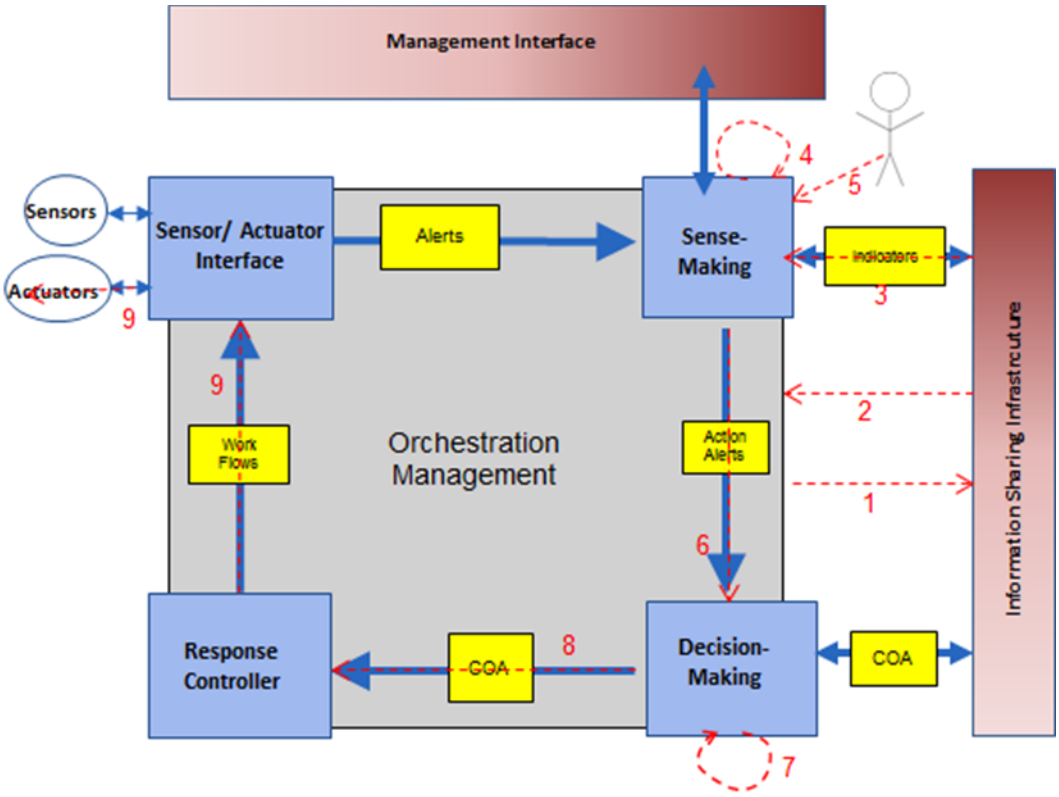

Figure 12. Indicator Received from External Source Use Case Flow

5. Use Case Name: Generation of Indicators/Tips for Sharing to other Enterprises

Preconditions: Analyst has discovered new indicator			
Actors: Analyst, sensors			
Step	**Process**	**Orchestration Requirement**	**Specification**
1	Alert and associated sensor data (e.g. file) is passed from sensor to sensor/actuator interface		
2	Alert and associated sensor data (e.g. file) sent to Sense-Making	Receive alert and associated sensor data, send to sense-making	Alert message format Sensor data message format
3	Analyst creates indicator		
4	Sense-Making processes the indicators and associated information and sets up new analytic rule		
5	Indicator shared with community	Receive indicator from sense-making and send to information sharing infrastructure	Indicator message format

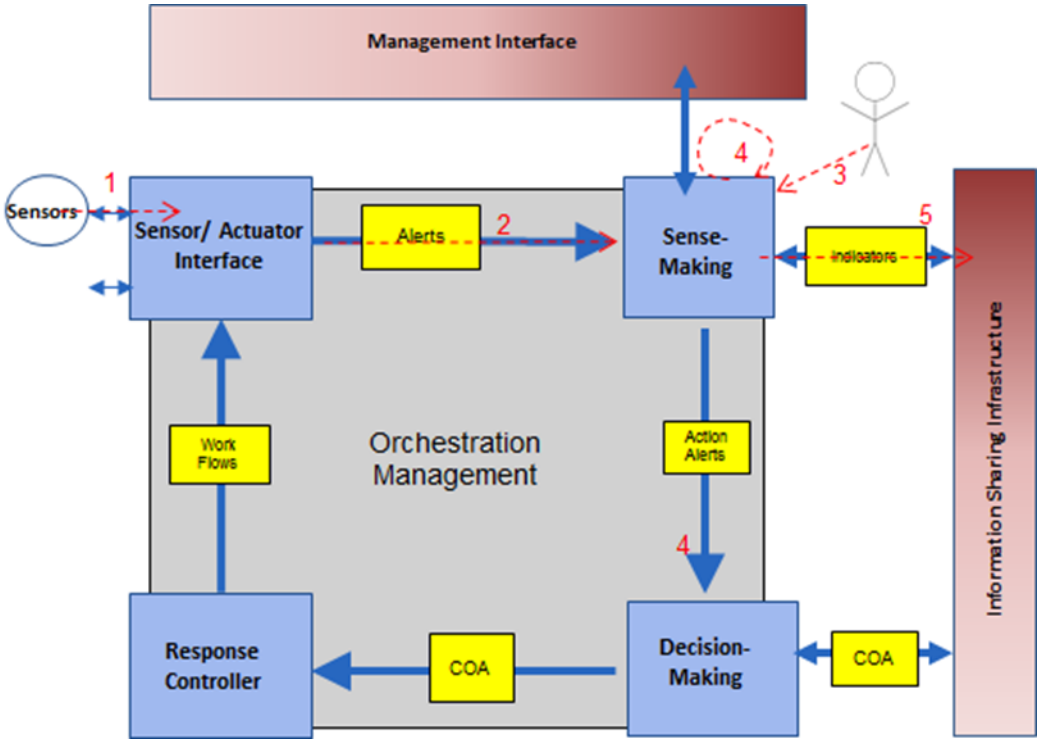

Figure 13. Generation of Indicators/Tips for Sharing to other Enterprises Use Case Flo

6. Use Case Name: Adding New Sensing Sources

Preconditions: New sensor added to enterprise			
Actors: Sensors			
Step	**Process**	**Orchestration Requirement**	**Specification**
1	New sensor configuration sent to sensor/actuator interface		
2	Sensor/actuator interface updated to receive input from new sensor		
3	New sensor information sent to sense-making	Receive new sensor data information from sensor/actuator interface and send to sense-making	New sensor data information message format
4	Sense-making sets up new rules so it can receive and interpret data from new sensor		

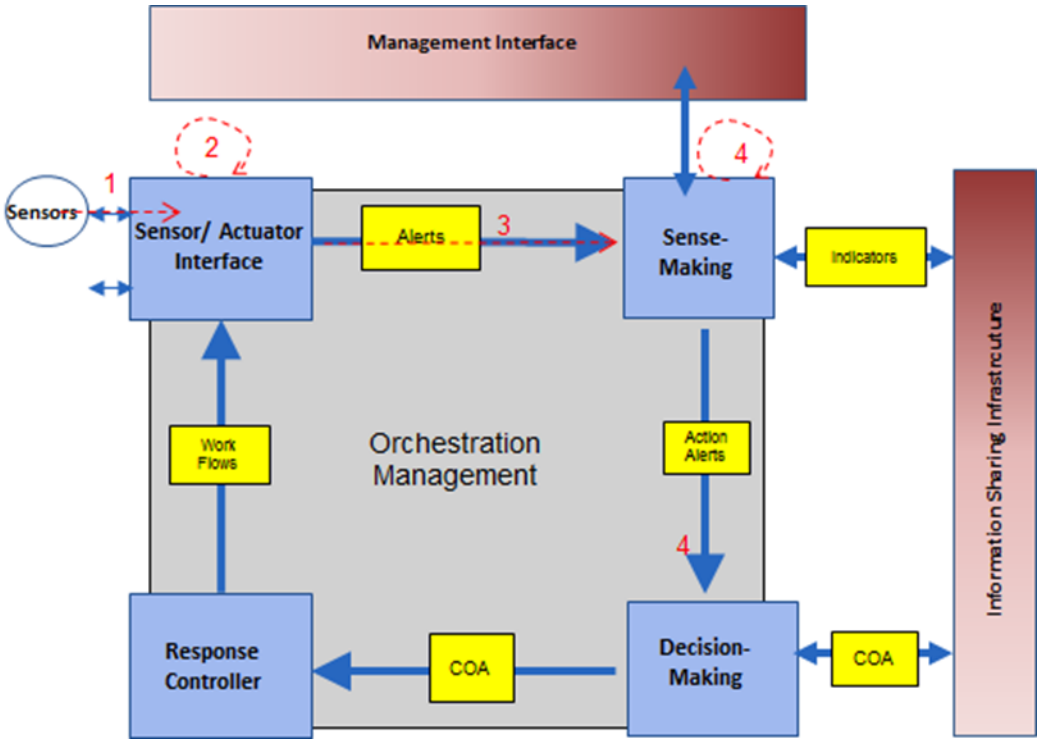

Figure 14. Adding New Sensing Sources Use Case Flow

7. Use Case Name: Adding New Actuators

Preconditions: New actuator added to enterprise			
Actors: Actuators			
Step	**Process**	**Orchestration Requirement**	**Specification**
1	New actuator configuration sent to sensor/actuator interface		
2	Sensor/actuator interface updated to send workflow to actuator		
3	New acting point information sent to sense-making	Receive new acting point information from sensor/actuator interface and send to sense-making	New acting point message format
4	Sense-making sets up new rules so it can set up new rules for acting point		

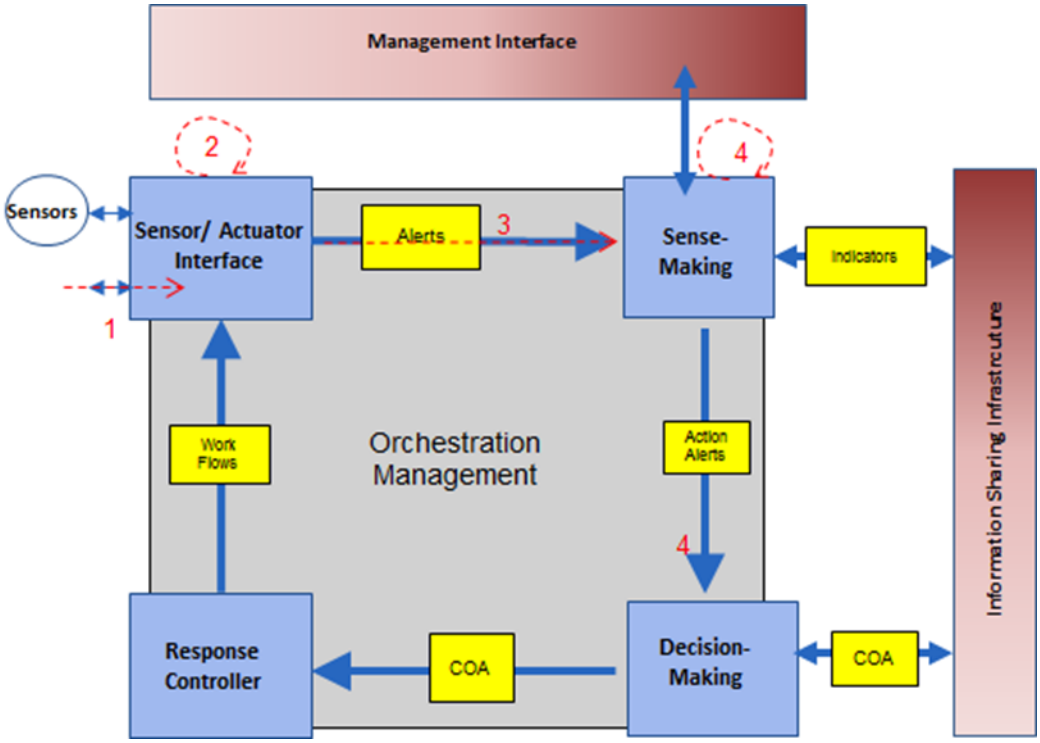

Figure 15. Adding New Actuators Use Case Flow

8. Use Case Name: Adding New Response Actions/COAs

Preconditions: Partner enterprise shares new COA			
Actors: Partner enterprise, analyst			
Step	**Process**	**Orchestration Requirement**	**Specification**
1	New COA received through information sharing interface and sent to decision-making	Receive new COA from information sharing infrastructure and send to decision-making	COA message format
2	User examines COA and determines whether it adversely affects mission		
3	User approves or disapproves of COA		
4	New COA is added to decision-making		

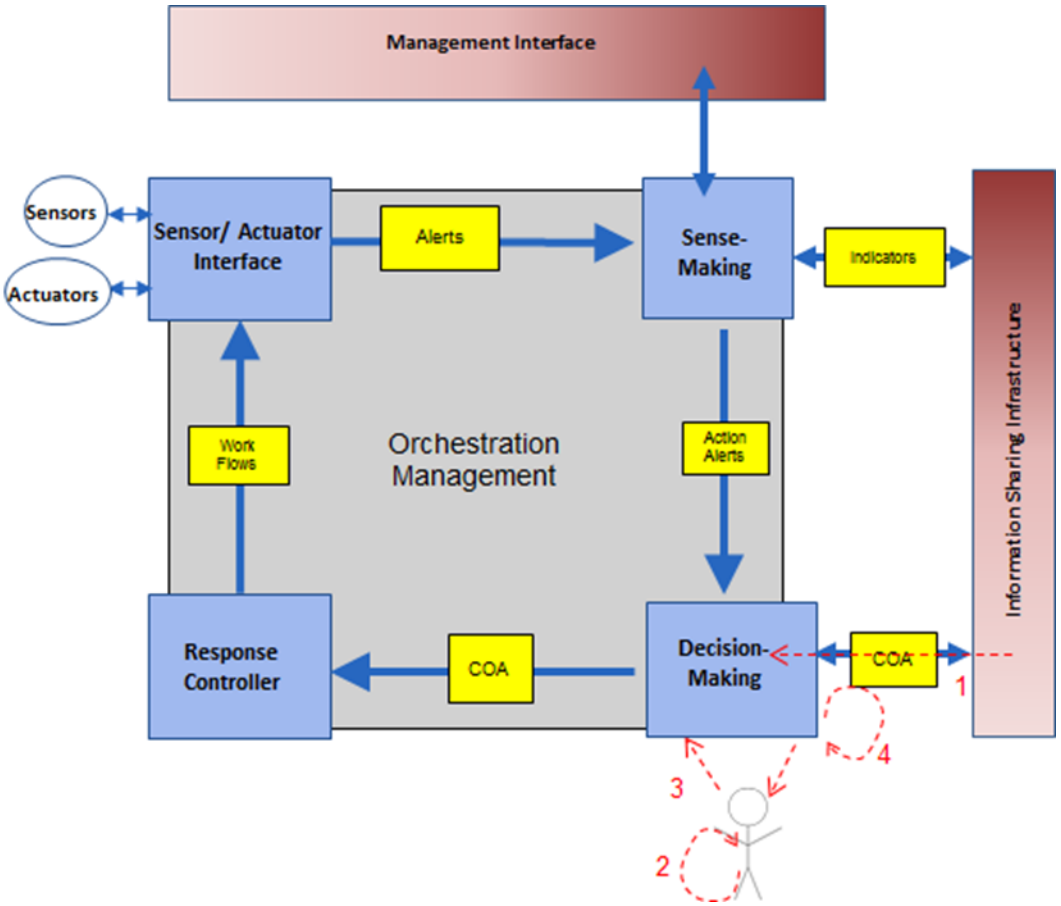

Figure 16. Adding New Response Actions/COAs Use Case Flow

APPENDIX B. SPIRAL MAPPING TO ARCHITECTURE

This appendix provides a summarized description of IACD spiral activity and aligns those spirals to the IACD architecture in this document. The summary charts on the following pages provide:

- Theme of the spiral
- Identification of IACD Use Cases exercised in spiral
- Classification of the architecture components exercised in the spiral, as well as the specific tools, solutions, and interface mechanisms that were implemented
- Description of areas of customization that were required to integrate – these in turn were used to drive interoperability mechanisms to reduce customization in the future
- Summary of how the given spiral influenced or impacted the IACD Architecture

As reference, the following table presents an aggregated set of use cases that have been applied over the evolution of the architecture. As noted in Section 3 of this IACD Reference Architecture, a combined, updated set of use cases represent the current state of the architecture, and should be used moving forward. The list below provides both the older reference numbers (IACD #) of the use cases that were active during the development of prior spirals in comparison to the combined use cases (Combined #) for easy reference.

Table 2. Use Case/Spiral Alignment

IACD #	Combined #	Use Case Name	Spirals	Share	Detect Event	Maintain System CS	Upgrade System CS
1		Compliance checking and automated return to compliant state.				X	
2		Auto-enrichment of troubleshooting/analyst activity	1, 2, 4				X
3	**1**	**Detection and mitigation of vulnerabilities**					**X**
4	**2**	**Detection and mitigation of malware**	**1, 2, 3, 4**		**X**		
5	**3**	**Detection, tipping, and mitigation of anomalous behaviors**	**3**		**X**		
6	**4**	**Indicator received from external source and initiation of IACD response**	**1, 2, 3**	**X**			
7	**5**	**Generation of Indicators/Tips for Sharing/Direction to other enterprises**	**1, 2, 3, 5**	**X**			
8		Passive sensing and cross-enterprise IACD	5	X			
9	**6**	**Adding new sensing sources**					**X**
10	**7**	**Adding new actuators**					X
11	**8**	**Adding new response actions / COAs**	**3**				**X**
12		Validation/checking of new COA	3				X
13		Continuity of Operations				X	
14		Regeneration in support of mission assurance				X	
15		Equity adjudication				X	

Spiral 0: Orchestration & Automation Intra-Enterprise – "Make It Real"

IACD Architecture Use Cases Exercised:

#2: Auto-enrichment of troubleshooting/analyst activity
#4: Detection and mitigation of malware
#7: Generation of Indicators/Tips ➔ Directions to other enterprises (created and formatted, not sent/shared until spiral 1)

Tools/Solutions Integrated

Sensors	*SAIF*	*SM*	*DM*	*RAC*	Orchestration Tools/Services
Bit9 (Host/endpoint protect, whitelist) Splunk (Event history) FireEye (Sandbox/Detonation) VirusTotal, IPVoid, URLVoid , Herd Protect (Reputation Services)	Custom	Custom	Custom	Custom	Invotas Security Orchestrator (Now FireEye SO) TIBCO Streambase Python Scripting
Actuators					
Bit9 (Host/endpoint mgmt) Cisco, Juniper (Firewall) Snort (IDS) TAXII-Yeti (Info Exchange Svc)					

Control Message Infrastructure	Information Sharing Infrastructure	Trust Services	Content Specs/Stds Examined
Not exercised	*TAXII Service*	Not exercised	*STIX 1.1 Indicators*

Drivers/Influencers on IACD Evolution:

- Established initial 'orchestration' characteristics and categorization criteria
- Normalized early workflows – auto-enrichment and auto-block
- First implementation of auto-generation of STIX formatted messaging

Spiral 1: Scalability and Automated Indicator Sharing

IACD Architecture Use Cases Exercised:

#2: Auto-enrichment of troubleshooting/analyst activity
#4: Detection and mitigation of malware
#6: Indicator Received from External Source ➔ Initiation of IACD Response
#7: Generation of Indicators/Tips ➔ Directions to other enterprises

Tools/Solutions Integrated

Sensors	*SAIF*	*SM*	*DM*	*RAC*	Orchestration Tools/Services
Bit9 (Host/endpoint mgmt.) Splunk (Event history) FireEye, Cuckoo (Sandbox/Detonation) VirusTotal, IPVoid, URLVoid, Herd Protect, ESSA Storefront (Reputation Services) Bro (Netflow interface) TAXII-Yeti (Info Exchange Svc)	Some vendor-sourced connectors Custom	Custom	Custom	Custom	Invotas Security Orchestrator (Now FireEye SO) TIBCO Streambase Microsoft Security Center Orchestrator Python Scripting
Actuators					
McAfee ePO (Host/endpoint mgmt) Cisco, Juniper (Firewall) Cuckoo (Sandbox/Detonation) Snort, Suricata (IDS) TAXII-Yeti (Info Exchange Svc) RTIR (Ticketing Service)					

Control Message Infrastructure	Information Sharing Infrastructure	Trust Services	Content Specs/Stds Examined
Not exercised	TAXII Service	Not exercised	STIX 1.1 Indicators

Drivers/Influencers on IACD Evolution:

- Validated auto-information sharing via STIX/TAXII – drove initial trade-space questions for control message infrastructure
- Derived common command categories for multiple actuator and sensor types ➔ inform OpenC2 definitions and evolution
- Established workflow format for human-in-the-loop/dial-able automation scenarios
- Integrated orchestration service with Government-provisioned reputation source – ESSA Storefront

Spiral 2: Risk- and Mission-based Decision Complexity					
IACD Architecture Use Cases Exercised:					
#2: Auto-enrichment of troubleshooting/analyst activity #4: Detection and mitigation of malware #6: Indicator Received from External Source ➔ Initiation of IACD Response #7: Generation of Indicators/Tips ➔ Directions to other enterprises					
Tools/Solutions Integrated					
Sensors	*SAIF*	*SM*	*DM*	*RAC*	Orchestration Tools/Services
Splunk (Event history) VirusTotal, IPVoid, URLVoid, Herd Protect, Alexa, WhoIs.net (Reputation Services) Bro (Netflow interface) TAXII-Yeti (Info Exchange Service) DIB Indicator Sharing (Info Ex Service) Tripwire (Host/endpoint mgmt.) *RSA Archer (Host/endpoint mgmt)**	Some vendor-sourced connectors Custom	Custom	Custom	Custom	TIBCO Streambase
Actuators					
Cisco, Juniper (Firewall) Windows Utilities (Host, User Mgmt) Security Onion (IDS) Best Practical (Ticketing Service)					
Control Message Infrastructure	Information Sharing Infrastructure			Trust Services	Content Specs/Stds Examined
Not exercised	TAXII Service			Not exercised	STIX 1.1, DIB Indicators
Drivers/Influencers on IACD Evolution:					

- Developed reference algorithms for implementing scoring/risk prioritization ➔ inform CDM, commercial implementations
- Derived additional common command categories for multiple actuator and sensor types ➔ inform OpenC2 definitions and evolution
- Added 'audit trail' logging via tickets of decision criteria – drives orchestration service and decision-making engine requirements

<table>
<tr><td colspan="6">Spiral 3: Anomalous Behavior Mitigation & COA Sharing</td></tr>
<tr><td colspan="6">IACD Architecture Use Cases Exercised:</td></tr>
<tr><td colspan="6">#4: Detection and mitigation of malware
#5: Detection, tipping, and mitigation of anomalous behaviors
#6: Indicator received from external source ➔Initiation of IACD Response
#7: Generation of Indicators/Tips ➔ Directions to other enterprises
#11: Adding new response actions/COAs
#12: Validation/checking of new COAs</td></tr>
<tr><td colspan="6">Tools/Solutions Integrated</td></tr>
<tr><td rowspan="2">Sensors</td><td colspan="5"></td></tr>
<tr><td>SAIF</td><td>SM</td><td>DM</td><td>RAC</td><td>Orchestration Tools/Services</td></tr>
<tr><td>Snort (IDS)
VirusTotal (Reputation Service)
Cuckoo (Sandbox/Detonation)
Bro (Netflow Interface)

Soltra Edge (TAXII - Exchange Svc)
McAfee ePO (Host/endpoint mgmt)</td><td rowspan="3">Increased # vendor-sourced connectors

Custom</td><td rowspan="3">Custom</td><td rowspan="3">Custom</td><td rowspan="3">Custom</td><td rowspan="3">Phantom Cyber
Invotas Security Orchestrator (now FireEye SO)</td></tr>
<tr><td>Actuators</td></tr>
<tr><td>Snort (IDS)
Windows Utilities (Host, User Mgmt) Cuckoo (Sandbox/Detonation)
Bro (Netflow Interface)

Soltra Edge (TAXII - Exchange Service)
McAfee ePO (Host/endpoint mgmt)
Best Practical (Ticketing Service)</td></tr>
<tr><td>Control Message Infrastructure</td><td colspan="2">Information Sharing Infrastructure</td><td>Trust Services</td><td colspan="2">Content Specs/Stds Examined</td></tr>
<tr><td>Not exercised</td><td colspan="2">TAXII Service</td><td>Not exercised</td><td colspan="2">Experimental STIX 1.1 Adaptation – draft COA exchange formats</td></tr>
</table>

Drivers/Influencers on IACD Evolution:
• Informed future specifications for Courses of Action content, drove information sharing service definitions • Derived COA interoperability/import-export requirements for orchestration services

Spiral 4: Message Fabric Interoperability/Interchangability						
IACD Architecture Use Cases Exercised:						
#2: Auto-enrichment of troubleshooting/analyst activity #4: Detection and mitigation of malware						
Tools/Solutions Integrated						
Sensors	*SAIF*	*SM*	*DM*	*RAC*	Orchestration Tools/Services	
Snort (IDS) Splunk (Event History)	Vendor-sourced connectors	Custom	Custom	Custom	Phantom Cyber Invotas Security Orchestrator (now FireEye SO)	
Actuators						
Snort (IDS) Splunk (Event History)						
Control Message Infrastructure	Information Sharing Infrastructure				Trust Services	Content Specs/Stds Examined
TIBCO EMS Informatica ActiveMQ	Not Exercised				Not exercised	
Drivers/Influencers on IACD Evolution:						
• Drove selection of content abstraction levels, content types to go onto IACD specification roadmap, including response actions (OpenC2), events, Courses of Action • Drove more precise definition of 'message fabric' to instead emphasize a stack of ***Control Message Infrastructure*** components: Transport, Services, and Content • Initial capture of draft Trust Service requirements						

Spiral 5 (1 of 2) : Response Action Interoperability

IACD Architecture Use Cases Exercised:

#2: Auto-enrichment of troubleshooting/analyst activity
#4: Detection and mitigation of malware
#5: Detection, tipping, and mitigation of anomalous behaviors

Tools/Solutions Integrated

Sensors	*SAIF*	*SM*	*DM*	*RAC*	Orchestration Tools/Services
Snort (IDS) Splunk (Event History) VirusTotal (Reputation Service) Cuckoo (Sandbox/Detonation) McAfee ePO, Carbon Black (Host/endpoint B–22gmt.)	Standards-based custom library (to represent future vendor svc) Limited vendor-sourced beta	Custom	Custom	Standards-based custom library (to represent future vendor svc)	Phantom Cyber
Actuators					
Cuckoo (Sandbox/Detonation) McAfee ePO, Carbon Black (Host/endpoint B–22mgmt) Netfilter/iptables (Firewall)					

Control Message Infrastructure	Information Sharing Infrastructure	Trust Services	Content Specs/Stds Examined
Active MQ	TAXII Service	Not exercised	OpenC2 version 0.5 – common Response Action specification

Drivers/Influencers on IACD Evolution:

- Extensive reference implementation of draft OpenC2 specification ➔ direct feedback to community for refinement, additional specification
- Derived interface boundaries for IACD specification roadmap, to include services and content specs

Spiral 5 (2 of 2) : Automated Support to Hunt Operations

IACD Architecture Use Cases Exercised:

#2: Auto-enrichment of troubleshooting/analyst activity
#6: Indicator Received from External Source ➔ Initiation of IACD Response
#7: Generation of Indicators/Tips ➔ Directions to other enterprises
#8: Passive sensing and cross-enterprise IACD

Tools/Solutions Integrated

Sensors	*SAIF*	*SM*	*DM*	*RAC*	Orchestration Tools/Services
Soltra Edge (TAXII – Exchange Service) RiskIQ, VirusTotal, PassiveTotal (Reputation Services) Splunk (Event history) Tanium (Host/endpoint B–23gmt.)	Custom (reuse)	Custom	Custom	Custom	Microsoft System Center Orchestrator
Actuators					
Splunk (Event history) Cuckoo (Sandbox/Detonation) Tanium (Host/endpoint B–23gmt.) FireEye (IDS/IPS) PostFix (Email queue ➔ Ticketing)					

Control Message Infrastructure	Information Sharing Infrastructure	Trust Services	Content Specs/Stds Examined
Not exercised	TAXII Service (Soltra Edge)	Not exercised	STIX 1.1 Indicators

Drivers/Influencers on IACD Evolution:

- Initial private sector pilot implementation – drove format, content of IACD Implementation Packages
- Derived format for object specification documentation of IACD workflows
- Captured input to STIX evolution to increase indicator utility
- Drove key capability requirements for indicator parsing automation

APPENDIX C. LIST OF ACRONYMS AND ABBREVIATIONS

COA	Course of Action
DHS	Department of Homeland Security
DM	Decision-Making
IACD	Integrated Adaptive Cyber Defense
IDS	Intrusion Detection Systems
IPS	Intrusion Prevention System
JHU/APL	The Johns Hopkins University Applied Physics Laboratory
NetFlow	Network Flow
NSA	National Security Agency
OODA	Observe, Orient, Decide, Act
RAC	Response Action Controller
SAIF	Sensor/Actuator Interface
SM	Sense-Making
STIX	Structured Threat Information eXpression; XML-based file that stores threat information.
TAXII	Trusted Automated eXchange of Indicator Information; The protocol that transports STIX messages.