JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

11100 Johns Hopkins Road • Laurel, Maryland 20723-6099

AOS-17-0258
August 2017

Integrated Adaptive Cyber Defense (IACD) Orchestration Thin Specification

Version 2.0

Prepared for: Department of Homeland Security

Prepared by: Beth Hoenicke, Alexander Lee, Jenna Stiling, Brett Waldman

Task No.: XXXXX; CYS05101

Contract No.: XXXXXXXXXXXXXXXXXXXX

15-407

CHANGE LOG

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

Document	Date	Description
Draft 0.8	February 2017	**Draft Limited Distribution -** Orchestration Thin Specification for early input
Version 1.0	March 2017	Pre-Decisional Draft release for comment.
Version 2.0	August 2017	Updated draft to refine sections describing orchestration services, playbooks and workflows.

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. 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.

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

The IACD concept transforms the construct of OODA Loop activities into sensing, sense-making, decision making, and acting. It envisions the sharing of information across these activities and with other entities to achieve shared situation awareness. Orchestration services provide the managed automation and integration of the OODA Loop-derived activities.

1.1. Purpose

The purpose of this document is to provide the minimum requirements necessary for security orchestration services in the Integrated Adaptive Cyber Defense (IACD) framework. This thin specification does not overly prescribe or dictate difficult to achieve requirements, but presents the minimum functionality needed to successfully perform security orchestration services.

While some requirements are specific, other requirements are general by design to avoid unnecessary constraint and numerous requirements. This document will not describe how to achieve or implement these requirements, but rather acknowledge they need to be considered for effective implementation.

One of the main considerations for implementation of security automation and orchestration (SA&O) services will be an organization's inclination to trust automated response actions including defining both human and non-human roles. This thin specification is not intended to address minimum requirements for trust, trustworthiness, or risk tolerance since that may be different for every organization. The latest information about orchestration, interoperability, playbooks, and more can be found on the IACD website: https://secwww.jhuapl.edu/IACD.

2. Orchestration Service Descriptions

IACD can be summarized the set of **orchestration services** needed to: *integrate* across multiple, disparate sources of information; *automate* the determination of risk and the decision to act; *synchronize* those machine actions to align with an organization's business rules and operational priorities, as captured in **playbooks**; and *inform* communities of trust via **secure automated cybersecurity information exchange** so that other IACD-capable partners can rapidly act on that information. This basic component framework is shown in Figure 1.

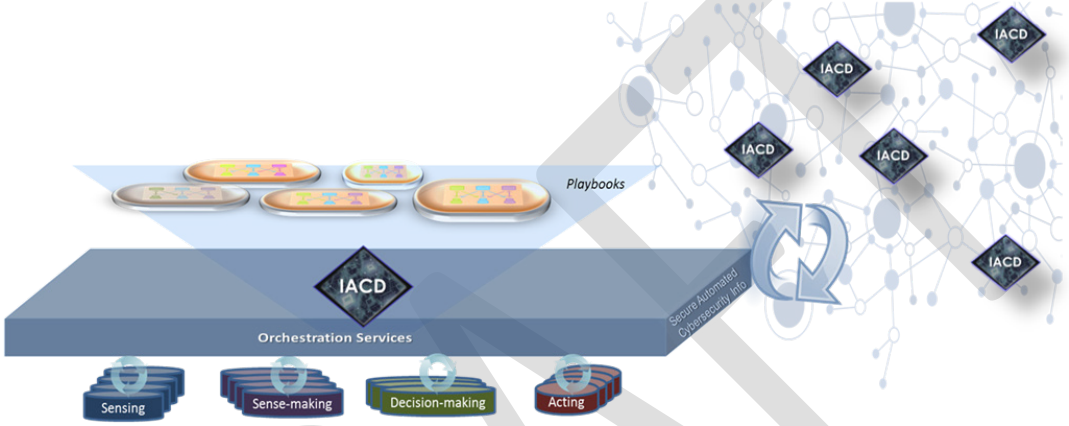

Figure 1: Basic IACD Component Framework

In the IACD architecture, the Orchestration Services block in Figure 1 is decomposed into a set of orchestration capabilities based on the previously described OODA loop. This is necessary to adequately define the minimum requirements for orchestration services. Figure 2 illustrates the basic architecture of IACD. The blue boxes are orchestration capabilities, which are further described below. The yellow boxes indicate the type of information that passes between the capabilities as part of the OODA construct.

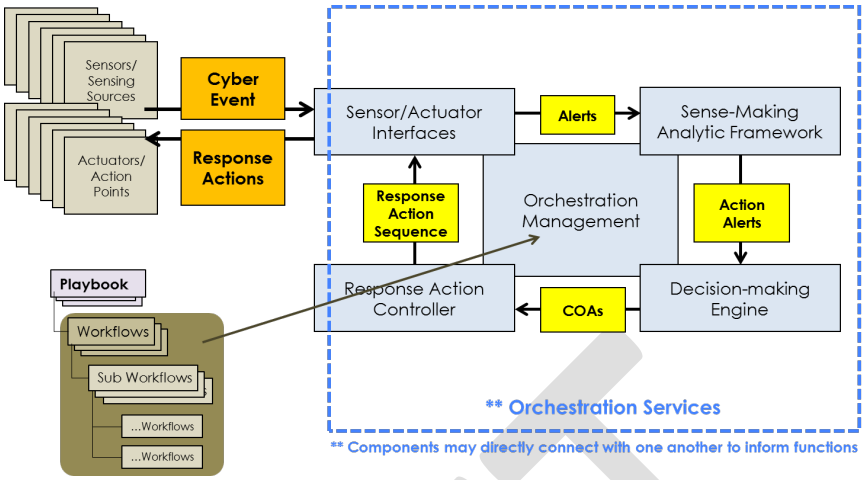

Figure 2: Orchestration Services

Orchestration workflows are rarely as simple and direct as a single OODA loop. Often the process from initiation of a workflow to its completion involves multiple sub-workflows that require more information from sensing, sense-making, and decision-making sources (including humans) at key points. As Figure 2 denotes, components may directly connect with one another. There are two types of communication that are allowed even though they are not explicitly enumerated in the architecture: Query and Response. They are both accounted for in the requirements and enable orchestration capabilities to query other capabilities via a workflow executed by Orchestration Management and respond directly as appropriate. For example, during the processing of an Alert, an analytic in the Sense-Making Analytic Framework may need to query a Sensor Manager for certain data, and that data may be passed directly to a process accessible by the analytic with only a status response being sent to the Orchestration Management capability. This is acceptable communication between components.

The orchestration capabilities in Figure 2 are defined as follows, to include the basic OODA loop information flow that must be supported.

2.1. Sensor/Actuator Interface

The sensor/actuator interface enables communication with heterogeneous collections of sensors and actuators within an enterprise. 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. Sense-Making Analytical Framework

If the Sense-Making Analytic Framework receives an alert, it will—based on enterprise policies and processes—perform a number of operations 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. Whether action or no action, it will log its activities.

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. Once a COA is selected, the Decision Making Engine will pass the selected COA(s) to the Response Controller.

2.4. Response Action Controller

The Response Controller translates the COA into a sequence of response actions, which it sends to the appropriate Sensor/Actuator interface.

2.5. Sensor/Actuator Interface

Upon receipt of a Response Action Sequence, the Sensor/Actuator Interface translates the sequence into device-specific response actions that it sends to the appropriate enterprise sensors and actuators.

2.6. Orchestration Management

Orchestration management is responsible for maintaining the configuration and monitoring other orchestration capabilities. It also provides the mechanism for both operator and electronic interface to orchestration services. Orchestration management should provide some capability for rollback and recovery with the understanding that all actions may not be reversible. Given that orchestration management capabilities continue to evolve, Section 4.4 requirement OM-07 captures only those actions that are currently deemed feasible and appropriate.

3. Playbooks, Workflows, and Local Instances

Playbooks are a set of process oriented steps that enable an organization to meet the requirements specified in their policies and procedures. They are a set of human understandable actions that document an organizational process which is initiated in response to a cyber-event or other defined trigger condition (e.g., a compromised device is detected).

Workflows are the machine understandable codification of playbooks to enable repeatable and auditable automation of the procedures. Orchestration services execute workflows, interfacing with the other orchestration services and humans as necessary. To ensure proper execution of the workflow, the orchestration services must maintain sequence and state of the individual tasks to any component as well as the workflow as a whole.

A local instance of a workflow is one that has been tailored to a particular environment, executing specific actions on specific devices and applications in response to specific conditions or events. Local instances are meant to be machine-to-machine shareable.

Figure 3 is a summary of the three levels of security automation abstraction from the highest to lowest detail level.

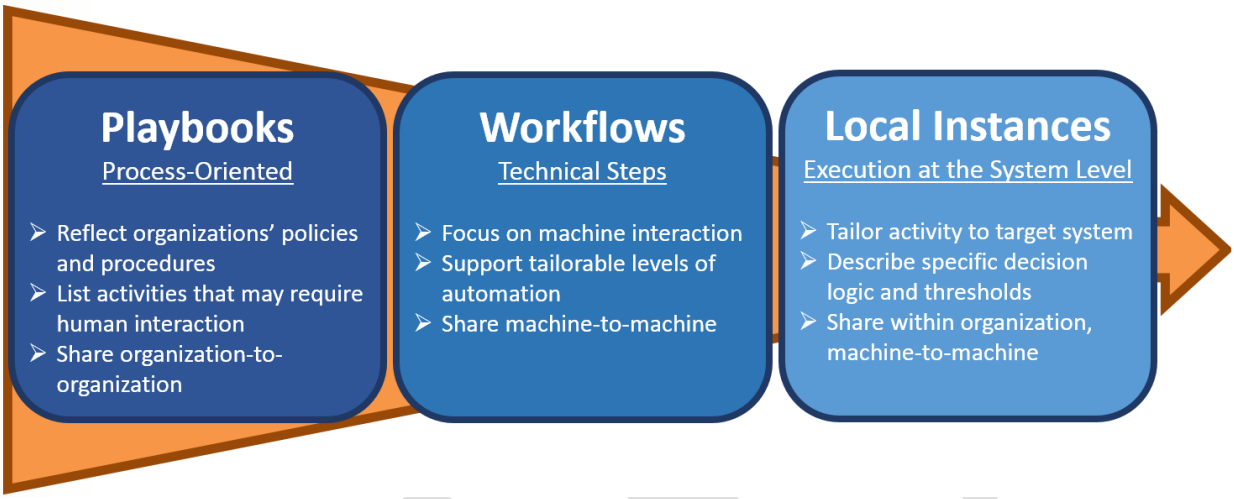

Figure 3: Detail at the Three Levels of Security Automation Abstraction

In simplified terms, the execution of a playbook is initiated by a cyber-event trigger. Playbooks may invoke other playbooks, operate either serially or in parallel, or initiate a workflow depending on the situation or conditions facing the system. Workflows are the instantiations of playbooks in IACD, and orchestration services are responsible for the coordination and execution of those workflows. The workflow may be as automated as desired, allowing for human interaction as required to support organizational policies and procedures.

More information regarding playbooks can be found at the IACD website here: https://secwww.jhuapl.edu/IACD/PlaybookSpecification

4. Minimum Orchestration Requirements

The following tables list the minimum requirements for orchestration services.

Products or services intended to provide orchestration services must either:

1) Fulfill these requirements;
2) Fulfill these requirements through an interface with other products or services that meet these requirements; or
3) Be part of an implementation in which these requirements are fulfilled elsewhere by other products and services.

For example, within an environment implementing IACD recommendations, the Sensor/Actuator Interface should maintain awareness of sensors and actuators (Requirement SA-01) or interface

with a product or service that offers the awareness and connectivity or be part of an implementation in which this requirement is fulfilled elsewhere in the implementation.

4.1. General Orchestration Requirements

GO-01	Logging. All orchestration actions shall be logged and include the provenance of information and decisions.
GO-02	Human involvement. There shall be an accommodation through user interfaces and APIs for human involvement to support automation that is consistent with enterprise policies and procedures.
GO-03	Error handling. There shall be provisions for error handling.
GO-04	Service recovery. As a minimum, there shall be provisions for recording the state of Orchestration services at the time of a service interruption or system shutdown.
GO-05	Scaling. There shall be a provision for scaling, load balancing, and failover.
GO-06	Backup. There shall be a mechanism for backup.
GO-07	Multiple orchestration services. There shall be the ability for independent workflows to be executed by different orchestration services in the same enterprise. This can be multiple nested workflows executed as part of a large-order workflow, or individual workflows initiated from the same trigger, but intended to execute independently.
GO-08	Policies. Policies and procedures shall be enterable and editable.
GO-09	Performance. Orchestration services should have the ability to provide performance information.
GO-10	Processing. Orchestration services shall support workflow execution with batch and real-time processing.

4.2. Security

S-01	Platform administration and security. There shall be capabilities that enable platform security, administering users, auditing platform access and utilization, optimizing performance and ensuring high availability and recovery.
S-02	Mutual authentication. Protected mutual authentication between orchestration and users as well as between orchestration capabilities shall be provided.
S-03	Secure protocols. Orchestration services will accommodate one or more existing secure protocols.
S-04	Least privilege. Orchestration services shall adhere to the principle of least privilege.
S-05	Patch management. Patch management shall be provided for orchestration services.
S-06	Credential storage. Orchestration services must be able to provide or take advantage of protected credential storage.

4.3. Workflows

WF-01	Workflow management. Orchestration services shall provide user interface for creating, editing, and cataloguing workflows.
WF-02	Schedule. Workflows shall be able to be scheduled.
WF-03	Catalog. Workflows shall be cataloged and version controlled.
WF-04	Interconnection and nesting. There shall be a capability to interconnect and nest

	workflows.
WF-05	Conditional logic. Workflows shall be able to include conditional logic.
WF-06	Define end state. Workflows shall be capable of being defined to achieve a particular state (e.g. compliance) without having to list all actions that will achieve that state.
WF-07	Storage. Workflows should be stored in a mechanism that allows for recovery.

4.4. Orchestration Management

OM-01	Triggers. There shall be the ability to kick off a workflow as a result of a trigger.
OM-02	Thresholds. Orchestration management shall set thresholds for action, e.g. define a default timeout for responses.
OM-03	Workflow State and Sequence. Orchestration management shall maintain awareness of state and sequence of workflow.
OM-04	Course of Action (COA) management. Orchestration management shall have the ability to create, edit, and catalogue COAs.
OM-05	Query. All Orchestration capabilities shall have the ability to query other capabilities.
OM-06	Input. All Orchestration services shall accept input in the form of: triggers, polling and response.
OM-07	Rollback. Orchestration management shall, as necessary, feasible and appropriate, have the ability to reverse the actions of a previous workflow.

4.5. Sensor/Actuator Interface (SAI)

SA-01	Maintain awareness of sensors and actuators. The SAI shall maintain awareness of enterprise sensors and actuators.
SA-02	Receive trigger. The SAI shall receive cyber event trigger from sensors.
SA-03	Send Alert. The SAI shall send an alert to the Sense-Making Analytic Framework (SMAF) if it exceeds threshold set in orchestration management.
SA-04	Receive response action sequences. The SAI shall receive response action sequences from the response action controller (RAC).
SA-05	Translate response action sequences. The SAI shall translate response action sequences into device - specific response actions and send to actuators.
SA-06	Add and remove sensors and actuators. Shall have the ability to add or remove sensors and actuators from a catalog of available sensors and actuators.

4.6. Sense-Making Analytic Framework (SMAF)

SM-01	Receive alerts. The SMAF shall receive alerts from the SAI.
SM-02	Enrich alert information. The SMAF shall enrich information about the alert by querying and receiving additional information from internal or external sources.
SM-03	Alert status. The SMAF shall maintain awareness of alert status.
SM-04	Determine further action. The SMAF shall determine whether further action is required in accordance with the workflow. Examples include: initiating enrichment queries, performing detonation, sending an action alert to the Decision-Making Engine, or determining that no further action is required.

SM-05	Send an action alert. If an action alert is needed, the SMAF shall send an action alert to the Decision-Making Engine.

4.7. Decision-Making Engine (DME)

DM-01	Policies and procedures. Decision making engine shall maintain association between policies and procedures and workflows.
DM-02	Receive action alerts. The DME shall receive action alerts from the Sense Making Analytic Framework.
DM-03	Catalog of COAs. The DME shall have access to the catalog of COAs for the organization.
DM-04	Selection of COA(s). The DME shall select COAs appropriate for the action alert received.
DM-05	New COAs. The DME shall be able to accept new COA(s) consistent with enterprise policies and procedures.
DM-06	Export. The DME shall be able to export COAs.
DM-07	Send COA(s). The DME shall send selected COAs to the Response Action Controller.

4.8. Response Action Controller (RAC)

RA-01	Receive COAs. The RAC shall receive the selected COAs from the DME.
RA-02	Translate COAs. The RAC shall translate COAs into sequences of response actions.
RA-03	Receive status of response action execution. The RAC shall receive status of response action execution, including erroneous conditions and states.
RA-04	Send status of response action execution. The RAC shall send status of response action execution to the appropriate orchestration service as defined in the workflow.