Integrated Adaptive Cyber Defense (IACD) Security Orchestration, Automation, and Response (SOAR) Product Thin Specification

Capabilities Engineering and Data Analysis (CEDA)
March 1, 2019
Version 1.0

CHANGE LOG

Version	Date	Description
1.0	1 March 2019	Initial Public Release

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. 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 respects by: (1) integrating and automating cyber defense tasks currently performed by human defenders, and (2) sharing threat information with other enterprises.

2. PURPOSE

This document provides the minimum requirements necessary for security orchestration, automation, and response (SOAR) services, which support the IACD framework. This document does not address any minimum requirements for trust, trustworthiness, or risk tolerance because those levels may be different for every organization. The requirements are implementation-independent and describe "what," rather than "how." Contrary to overly prescribing or dictating difficult-to-achieve requirements, this thin specification presents the minimum functionality needed for a well-conceived SOAR product to be successful.

The latest information about orchestration, interoperability, playbooks, and more can be found on the IACD website: **https://www.iacdautomate.org**.

3. ORCHESTRATION SERVICES

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 activities can, if implemented at speed and scale, drive cyber operations timelines from months to minutes to milliseconds. In terms of IACD, the OODA Loop translates to the equivalent activities of Sensing, Sense-making, Decision-making, and Acting. Orchestration services provide the managed automation and integration of these OODA Loop-derived activities.

IACD can be summarized as the set of **orchestration services** needed to:

- *integrate* across multiple, disparate information sources;
- *automate* risk determination and the decision to act;
- *synchronize* these 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**, thereby enabling other IACD-capable partners to rapidly act on that information.

Figure 1: Basic IACD Component Framework shows this basic component framework.

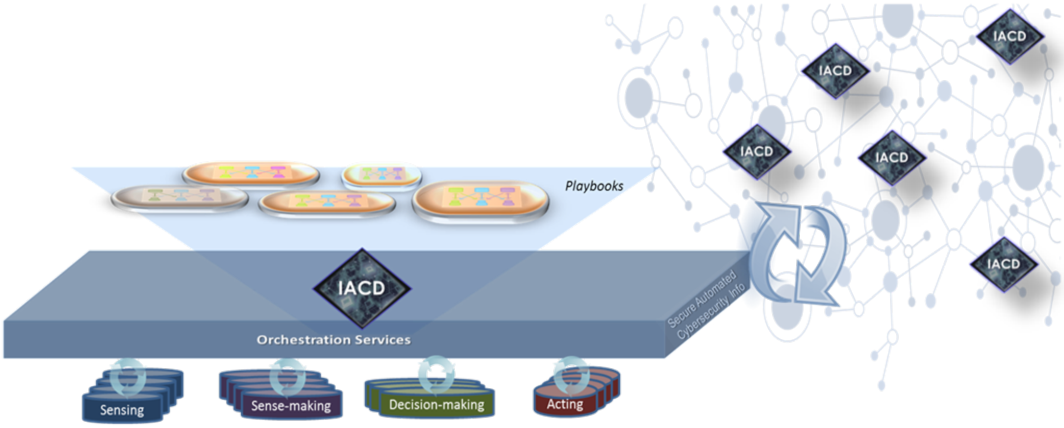

Figure 1: Basic IACD Component Framework

The Orchestration Services block in Figure 2: IACD Orchestration Services can be decomposed into a set of orchestration capabilities based on the previously described OODA Loop activities. Figure 2 illustrates the IACD vision of information sharing across these activities, and among organizations, through a common messaging system to achieve shared situational awareness.

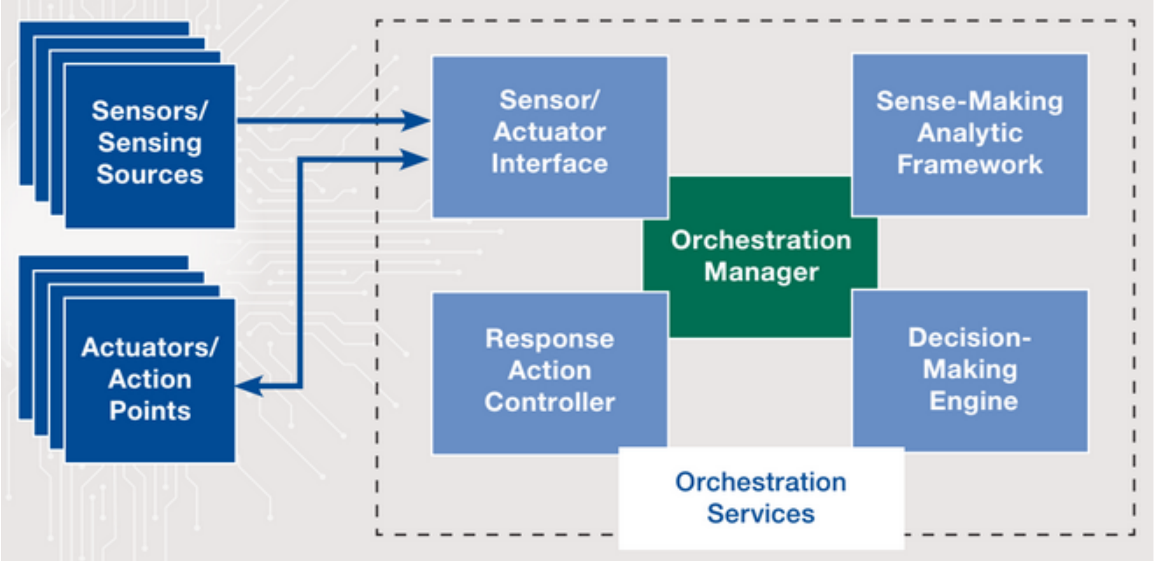

Figure 2: IACD Orchestration Services

4. THE ORCHESTRATION MODEL

The Integrated Cyber Defense (ICD) Conceptual Reference Model captures the overarching capabilities (an ability provided by a cybersecurity tool or product), functions (an action carried out by a cybersecurity tool or product), and activities (representing high-level processes that an organization undertakes to satisfy policy and governance requirements) that enable automation of cyber defense via the sharing of cyber threat information, indicators, and intelligence (CTI3). One of the five sub-models, which comprise the Conceptual Reference Model, is the Orchestration Model.

The Orchestration Model presents functions that are used to satisfy an organization's activities in response to CTI3. The orchestrator is critical as it manages the individual capabilities, rather than the function, provided by cybersecurity tools and products in an auditable, consistent, repeatable, and scalable manner to satisfy organizational policies that govern the whole process. One or more capabilities can be used in conjunction to complete an activity, while multiple capabilities can make up a function. Therefore, the link between the concepts of functions and capabilities is the orchestration of the requisite capabilities.

Additional details of the Orchestration Model are provided in a white paper located on the IACD website at **https://www.iacdautomate.org**.

5. OVERVIEW OF PLAYBOOKS, WORKFLOWS, AND LOCAL INSTANCES

Playbooks are a set of process-oriented steps that enable an organization to meet the requirements specified in its policies and procedures. They are a set of ***human understandable actions*** that document ***organizational processes***.

Workflows are the machine-understandable codification of playbooks that enable repeatable and auditable automated procedures. Orchestration services execute workflows, interfacing with other orchestration services and humans, as necessary. To ensure proper workflow execution, the orchestration services must maintain each individual task's sequence and state in relation to any component, as well as with the workflow as a whole.

A local instance of a workflow 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 machine-to-machine shareable.

Figure 3: Description for Playbooks, Workflows, and Local Instances represents the increasingly specific three levels of security automation abstraction, from the highest to lowest detail levels.

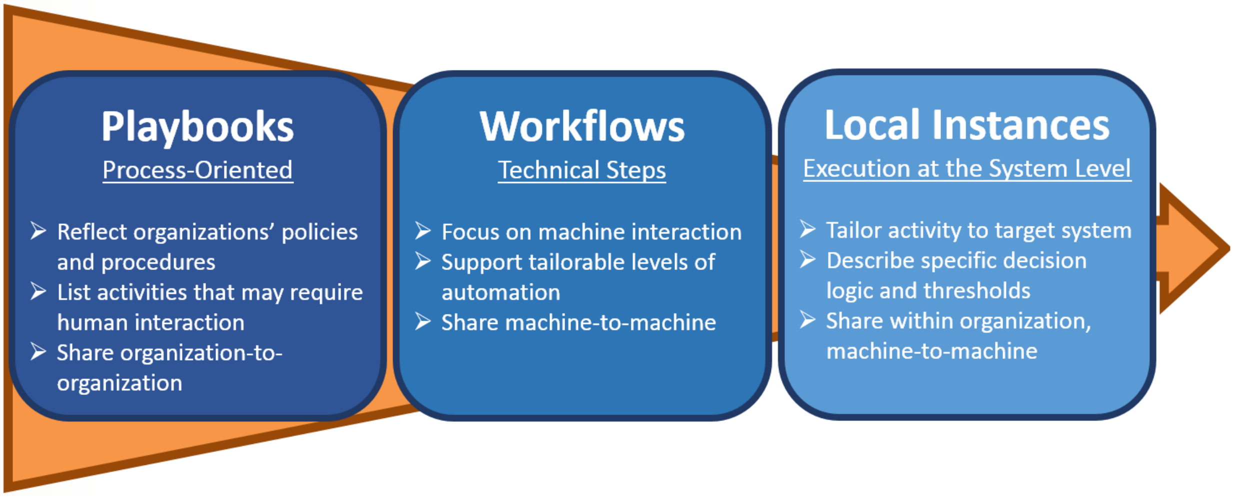
Playbooks
Process-Oriented
➢ Reflect organizations' policies and procedures
➢ List activities that may require human interaction
➢ Share organization-to-organization
Workflows
Technical Steps
➢ Focus on machine interaction
➢ Support tailorable levels of automation
➢ Share machine-to-machine
Local Instances
Execution at the System Level
➢ Tailor activity to target system
➢ Describe specific decision logic and thresholds
➢ Share within organization, machine-to-machine

Figure 3: Description for Playbooks, Workflows, and Local Instances

Simply stated, playbook execution is initiated in response to a cyber-event or other defined trigger condition (e.g., a compromised device is detected). Depending on the situation, playbooks may invoke other playbooks, operate serially or in parallel, or initiate a workflow. Workflows instantiate playbooks in IACD, and orchestration services are responsible for coordinating and executing those workflows. Workflows may be as automated as desired, allowing for optional human interaction to support organizational policies and procedures.

The IACD website at https://www.iacdautomate.org provides more information regarding playbooks.

6. MINIMUM SOAR REQUIREMENTS

The minimum SOAR product requirements are grouped by the functional categories described in Table 1: SOAR Requirement Functional Categories and captured in the following subsections.

Table 1: SOAR Requirement Functional Categories

Functional Category	Areas Addressed
General Orchestration	Backup, interconnected workflows, logging & tracking, human-in-the-loop, error handling, failover, integration, multiple indicators, batch & real-time processing, cost, performance, archiving, sharing, load balancing, etc.
Workflows	Creating, editing, conditional logic, cataloging, versioning, scheduling; including Playbooks & courses of action (COAs)
Security	Authentication & secure protocols, safe storage, confidential information (CI) regulatory compliance, access & use audits, data at rest & in motion, recovery, least privilege, etc.
Quality	Availability, reliability, consistency, usability, support, maintainability, etc.
Orchestration Management	Action thresholds, workflow component state/sequence, reversibility, etc.
Decision-Making	Policy-workflow association

Products or services intended to provide SOAR must either:

1) Fulfill these requirements, or
2) Indirectly fulfill these requirements via an interface or implementation with other products or services that meet these requirements directly.

Table 2: General Orchestration Requirements

ID	Requirement
GO-01	*Logging*. The SOAR product shall log all actions that it performs, including provenance (e.g., associated information origin and decision rationale).
GO-02	*Human Involvement*. The SOAR product shall allow users to insert manual actions at any process step.
GO-03a	*Error Monitoring*. The SOAR product shall monitor itself for error conditions.
GO-03b	*Error Reporting*. The SOAR product shall report the status of its own error conditions.
GO-03c	*Error Logging*. The SOAR product shall automatically log its own errors, if and as they occur.
GO-03d	*Error Hand-off to Operator*. The SOAR product shall automatically hand off logged errors to an operator.
GO-03e	*Failure Logging*. The SOAR product shall automatically log its own failures, if and as they occur.
GO-03f	*Failure Hand-off to Operator*. The SOAR product shall automatically hand off logged failures to an operator.
GO-04	*Record Current State*. The SOAR product shall record its current state at the time of a service interruption or system shutdown.
GO-05a	*Failover Provision*. The SOAR product shall have the ability to hand off its operations to a backup orchestration tool, in the event of failure or maintenance down time (i.e., failover provision for resiliency).
GO-05b	*Load Balancing Provision*. The SOAR product shall have the ability to spread its operational load to another orchestration tool, in the event of maxing out its processing volume (i.e., load balancing provision).
GO-06a	*Back Up Workflows*. The SOAR product shall have the ability to back up its workflows.
GO-06b	*Back Up Workflow Data*. The SOAR product shall have the ability to back up its workflow data.
GO-06c	*Back Up Interface Module Data*. The SOAR product shall have the ability to back up its interface module data.
GO-06d	*Back Up Orchestration Service Configuration*. The SOAR product shall have the ability to back up its orchestration service configuration.
GO-08a	*Enter Policies*. The SOAR product shall provide the ability for users to enter their enterprise policies and procedures.
GO-08b	*Edit Policies*. The SOAR product shall provide the ability for users to edit their previously entered enterprise policies and procedures.
GO-09a	*Performance Data Capture*. The SOAR product shall have the ability to capture its performance data.
GO-09b	*Performance Data Visibility*. The SOAR product shall have the ability to show its performance data.
GO-10a	*Batch Processing*. The SOAR product shall have the ability to execute multiple workflows concurrently (i.e., batch processing).
GO-10b	*Real-Time Processing*. The SOAR product shall have the ability to execute workflows triggered in real time (i.e., real-time processing).
GO-11a	*Archive Log Data*. The SOAR product shall provide the ability to archive historical log data.

ID	Requirement
GO-11b	*Recover Archived Log Data*. The SOAR product shall provide the ability to recover previously archived historical log data.
GO-12	*Product Interface*. The SOAR product shall have the ability to interface with *<name of specific security, information technology, or other type of orchestration platform, product, or service in an enterprise's existing or planned environment>*, or be able to support the integration through a roadmap. (Note: Enterprises should replicate this requirement and fill in a specific name for each instance.)
GO-13	*Cost*. The SOAR product shall have a combined total cost of ownership and return on investment (ROI) that justifies purchasing and incorporating it in an enterprise.

Table 3: Workflow Requirements

ID	Requirement
WF-01a	*Workflow Creation*. The SOAR product shall provide a user interface for creating workflows.
WF-01b	*Workflow Editing*. The SOAR product shall provide a user interface for editing existing workflows.
WF-01c	*Playbook Creation*. The SOAR product shall provide a user interface for creating playbooks.
WF-01d	*Playbook Editing*. The SOAR product shall provide a user interface for editing existing playbooks.
WF-01e	*Course of Action (COA) Creation*. The SOAR product shall provide a user interface for creating COAs.
WF-01f	*COA Editing*. The SOAR product shall provide a user interface for editing existing COAs.
WF-02	*Workflow Scheduling*. The SOAR product shall provide the ability to schedule workflows.
WF-03a	*Workflow Cataloging*. The SOAR product shall provide the ability to catalog workflows.
WF-03b	*Workflow Versioning*. The SOAR product shall provide the ability to control workflow versioning.
WF-03c	*COA Cataloging*. The SOAR product shall provide the ability to catalog COAs.
WF-04a	*Multiple Nested Workflows*. The SOAR product shall have the ability to execute multiple, nested workflows, which are part of one large workflow.
WF-04b	*Multiple Interconnected Workflows*. The SOAR product shall have the ability to execute multiple, interconnected workflows, which are part of one large workflow.
WF-04c	*Multiple Workflows From Same Trigger*. The SOAR product shall have the ability to execute individual workflows initiated from the same trigger event independent from any other orchestration tool within the same enterprise.
WF-04d	*Multiple Indicators For Same Workflow*. The SOAR product shall have the ability to execute the same workflow from more than one indicator.
WF-05	*Conditional Logic*. The SOAR product shall provide the ability to include conditional logic in workflows.

ID	Requirement
WF-07a	*Archive Workflows*. The SOAR product shall provide the ability to archive previous workflows.
WF-07b	*Recover Archived Workflows*. The SOAR product shall provide the ability to recover archived workflows.

Table 4: Security Requirements

ID	Requirement
S-01a	*Account Administration*. The SOAR product shall provide the ability to perform user account administration.
S-01b	*Access Audits*. The SOAR product shall provide the ability to perform user access audits.
S-01c	*Usage Audits*. The SOAR product shall provide the ability to perform platform usage audits.
S-02a	*Mutual System Authentication*. The SOAR product shall have the ability to provide mutual authentication with other systems.
S-02b	*Mutual Tool Authentication*. The SOAR product shall have the ability to provide mutual authentication with other tools.
S-02c	*Authentication Protocols Compatibility*. The SOAR product shall be compatible with existing authentication protocols within an enterprise.
S-03	*Secure Protocols Compatibility*. The SOAR product shall be compatible with existing secure protocols within an enterprise.
S-04a	*Least Privilege With Processes Interfaces*. The SOAR product shall adhere to the mutual principle of least privilege in relation to any process interfaces.
S-04b	*Least Privilege With User Interfaces*. The SOAR product shall adhere to the mutual principle of least privilege in relation to any user interfaces.
S-04c	*Least Privilege With Tool Interfaces*. The SOAR product shall adhere to the mutual principle of least privilege in relation to any tool interfaces.
S-05a	*Patch Installation*. The SOAR product shall have the ability to install authorized software patches received.
S-05b	*Patch Installation Preference*. The SOAR product shall provide the ability for users to specify either automatic or manually approved updates for installing software patches.
S-06a	*Safe Credential Storage*. The SOAR product shall have the ability to safely store credentials.
S-06b	*Safe Credential Access*. The SOAR product shall have the ability to securely access credentials.
S-07a	*Recovery From System Failure*. The SOAR product shall have the ability to recover from system failure.
S-07b	*Recovery From System Corruption*. The SOAR product shall have the ability to recover from system corruption.
S-08	*Confidential Information (CI).* The SOAR product shall have the ability protect CI when handling it, in accordance with legal and regulatory requirements.
S-09a	*Data in Motion*. The SOAR product shall have data integrity safeguards, including provenance tracking, for data in motion.
S-09b	*Data at Rest*. The SOAR product shall have data integrity safeguards, including provenance tracking, for data at rest.

Table 5: Quality Requirements

ID	Requirement
Q-01	*Availability*. The SOAR product shall function properly at least <*xx*> hours per day (Note: exact value to be supplied by enterprise).
Q-02	*Reliability*. The SOAR product shall function properly at least <*xx*> hours before any malfunction (Note: exact value to be supplied by enterprise).
Q-03	*Consistency*. The SOAR product shall perform consistently by arriving at the same COA each time for the same triggering event.
Q-04	*Usability*. The SOAR product shall use the <*name*> development language, which is already known to an enterprise's current staff. (Note: Enterprises should replicate this requirement and fill in a specific name for each instance.)
Q-05	*Graphical User Interface (GUI).* The SOAR product shall provide a GUI for building workflows.
Q-06	*Command Line Interface*. The SOAR product shall provide a command line or debug interface.
Q-07	*Vendor Support*. The SOAR product shall have 24/7 vendor help desk support available.
Q-08	*Maintainability*. The SOAR product shall receive vendor updates, such as enhancements, bug fixes, integration module developments, etc.

Table 6: Orchestration Management Requirements

ID	Requirement
OM-02	*Thresholds*. The SOAR product shall provide the ability to set thresholds for actions to occur (e.g., define a default timeout for receiving responses).
OM-03a	*Workflow State Awareness*. The SOAR product shall continually be aware of the state of any workflow.
OM-03b	*Workflow Sequence Awareness*. The SOAR product shall continually be aware of the sequence of tasks of any workflow.
OM-07	*Rollback*. The SOAR product shall provide the ability to reverse the automated actions of a previous workflow.

Table 7: Decision-Making Requirements

ID	Requirement
DM-01	*Policies and Procedures*. The SOAR product shall keep track of the association between entered policies and procedures vs. the workflows.

APPENDIX A: LIST OF ACRONYMS AND ABBREVIATIONS

AIS	Automated Indicators Sharing
CEDA	Capabilities Engineering and Data Analysis
CI	Confidential Information
COA	Course of Action
CTI3	Cyber Threat Information, Indicators, and Intelligence
DHS	Department of Homeland
GUI	Graphical User Interface
IACD	Integrated Adaptive Cyber Defense
ICD	Integrated Cyber Defense
JHU/APL	The Johns Hopkins University Applied Physics Laboratory
NSA	National Security Agency
OODA	Observe, Orient, Decide, Act
SOAR	Security Orchestration, Automation, and Response