MOSAICS

IACD Application to MOSAICS

4 November 2020

Harley Parkes (JHU APL)

Who is IACD?

Integrated Adaptive Cyber Defense is an initiative hosted by the Johns Hopkins University Applied Physics Laboratory under the sponsorship of the National Security Agency (NSA) and the Department of Homeland Security (DHS).

Our goal is to dramatically change the timeline and effectiveness of cyber defense via integration, automation, and information sharing.

What is IACD?

IACD *defines a <u>strategy</u> and <u>framework</u> to adopt an extensible, adaptive, COTS-based approach*

Plug-and-Play

Interoperability & Automation

IACD
Accelerating the Speed and Scale of Cyber Defense

Bring Your Own Enterprise

Information Sharing

Integrated Adaptive Cyber Defense:
an ecosystem because there is no single solution

Financial Sector Pilot Performance

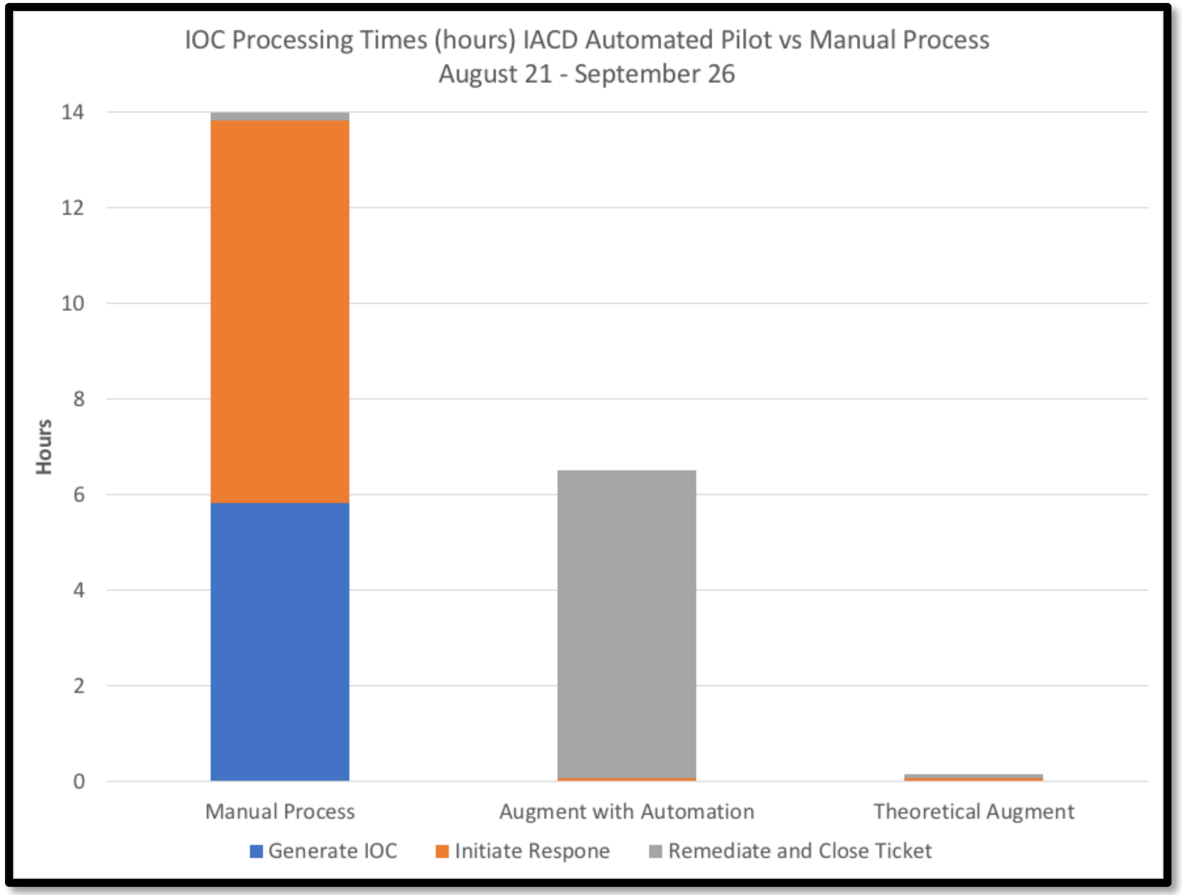
Timeline	Manual Process (Avg. per IOC)	Pilot Process (Avg. per IOC)	Theoretical Process (Avg. per IOC)
Generate IOC	5 hrs. ,49 min.	1 min.	1 min.
Initiate Response	8 hrs.	3.5 min.	3.5 min.
Remediate & Close Ticket	10 min.	6 hrs., 26 minutes	5 minutes
Total Time	13 hrs. ,59 min.	6 hrs., 30.5 min.	9.5 min.

Pilot remediation process required man in the loop for approval and closeout per IOC which creates significant delays, but still saw improvement in response times

~214% speed improvement

”Low-Regret” approach would automatically block IOCs with no prevalence on network (~99% of feed)

~8,800% speed improvement



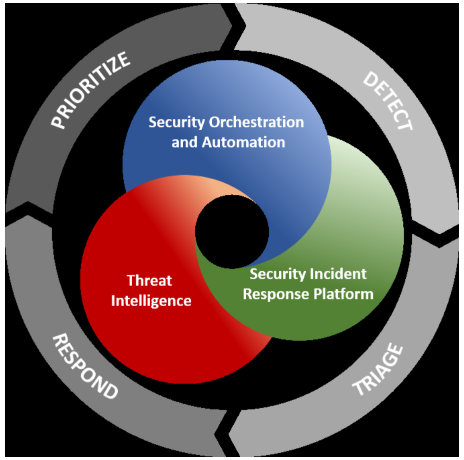
Addressing information sharing and SAO as a combined ecosystem allows for these types of improvements

Security Orchestration, Automation and Response

1. SOAR integrates security tools and disparate systems to support security automation

2. Automation provides immediate and measurable increases in efficiency and consistency of operational processes.

3. Enables collection of security event data and alerts to help investigate, prioritize and drive response actions based on a pre-defined “*workflow*”


PRIORITIZE
DETECT
TRIAGE
RESPOND
Security Orchestration and Automation
Threat Intelligence
Security Incident Response Platform

[SOAR] enables collection of security threat data and alerts from various organizational sources, where analysis and triage can be performed by both human and machine power to help define, prioritize and drive response activities according to a standard workflow

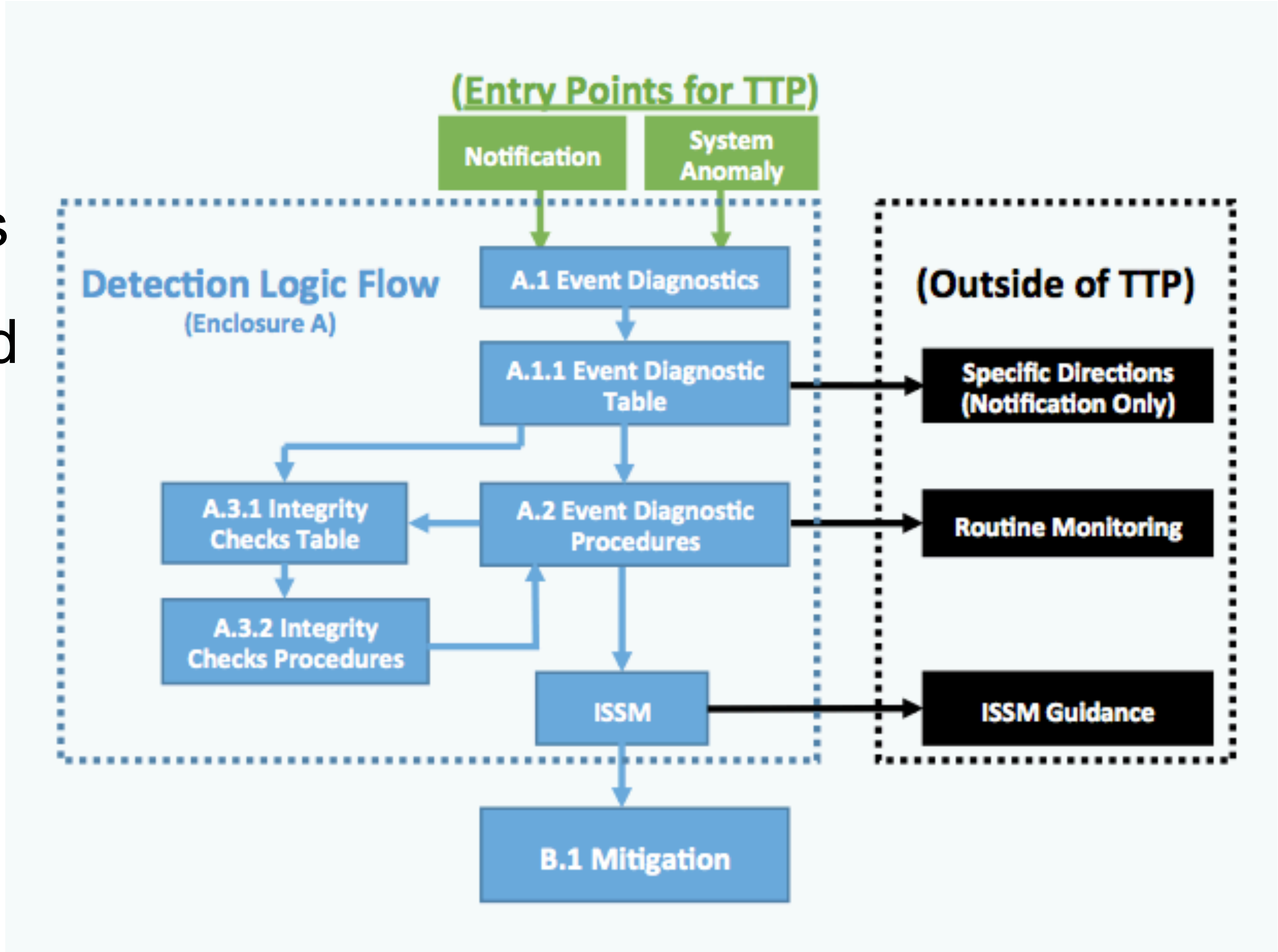
(Gartner, Inc)

Examples of SOAR vendors:

SWIMLANE
splunk> phantom
LogicHub
CYBERSPONSE ADAPTIVE SECURITY
DEMISTO A PALO ALTO NETWORKS® COMPANY

MOSAICS Use of SOAR

1. Used to automate ACI TTP process
2. Very procedurally structured around Detection, Investigation, Response
3. Lends itself well to automated implementation
4. **Important lessons learned applying SOAR to ICS**



(Entry Points for TTP)

Notification

System Anomaly

Detection Logic Flow
(Enclosure A)

A.1 Event Diagnostics

A.1.1 Event Diagnostic Table

A.2 Event Diagnostic Procedures

A.3.1 Integrity Checks Table

A.3.2 Integrity Checks Procedures

ISSM

B.1 Mitigation

(Outside of TTP)

Specific Directions (Notification Only)

Routine Monitoring

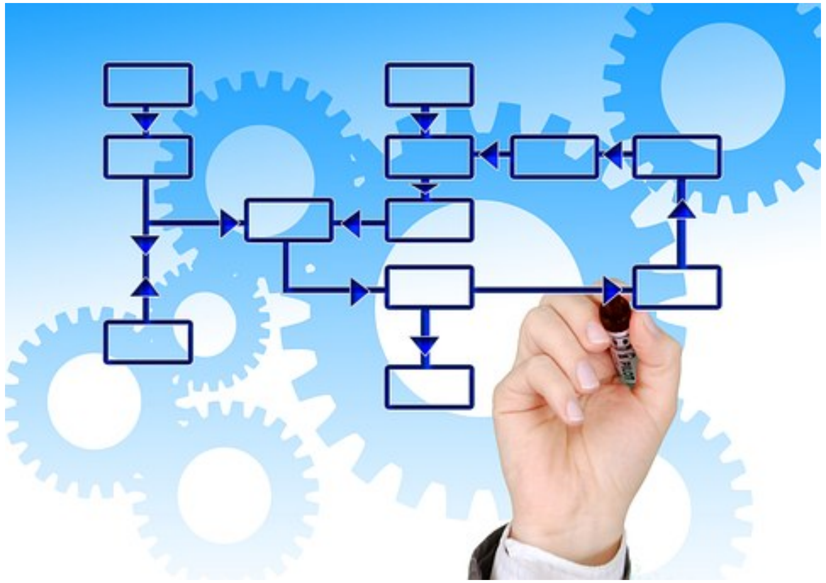
ISSM Guidance

Integration & Interoperability

1. Integrations lacking for ICS environments

2. Important implication for selection of products

3. The **right** functionality **must** be exposed through the API to:
   - Gain efficiencies via automation
   - Enable increased capabilities via integration
   - More readily leverage new functionality

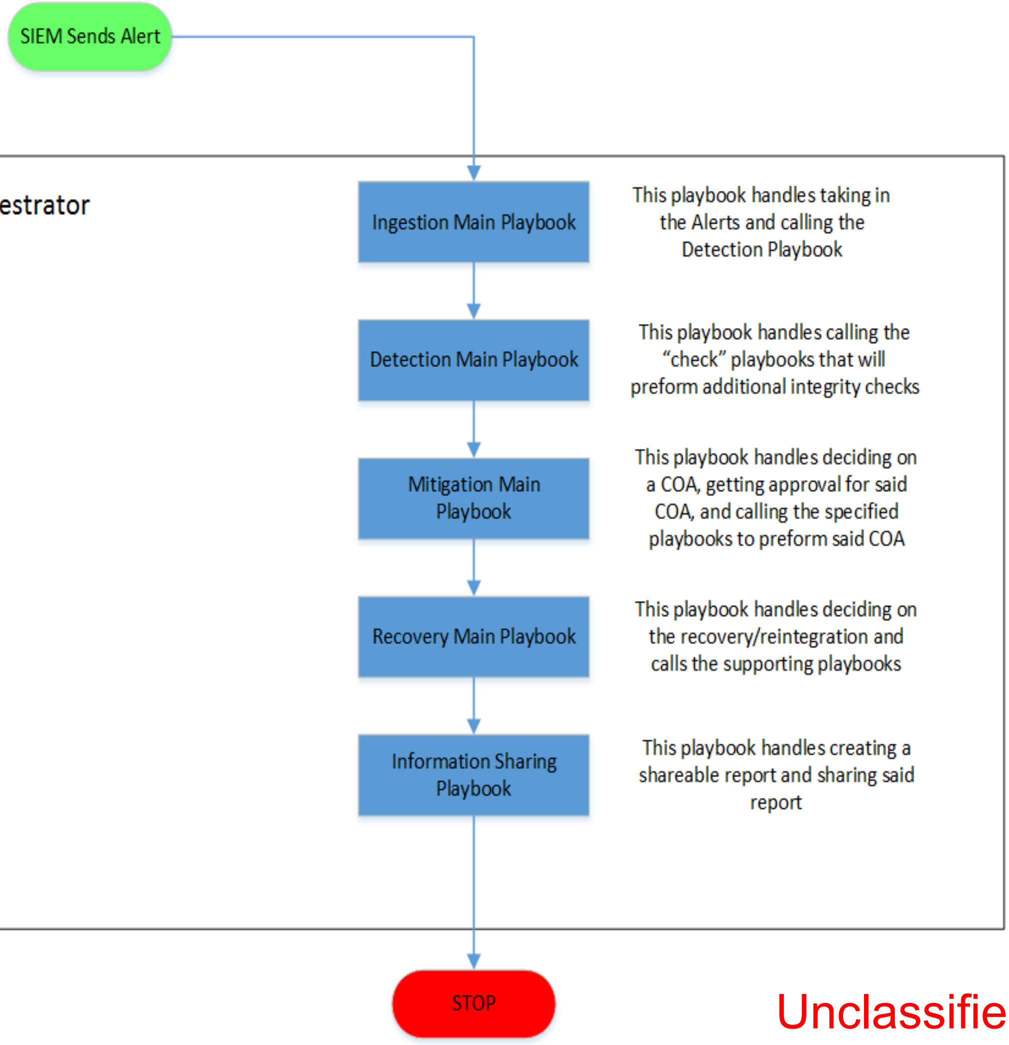


Robust, open APIs remain the single most important criteria for current and future integration

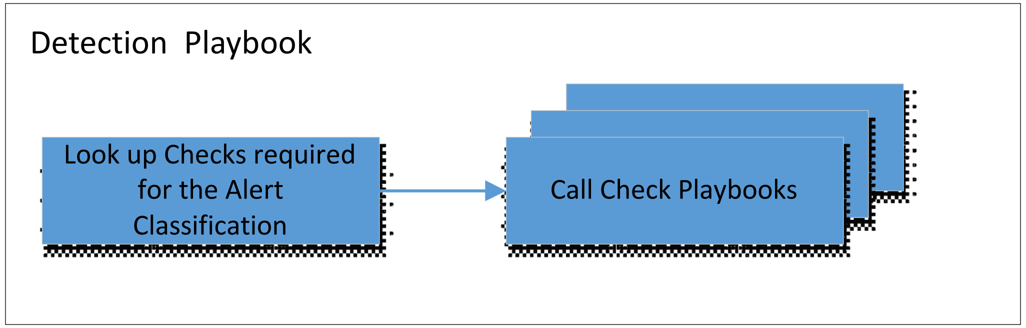
Standards Approach – OpenC2

- Open Command and Control (OpenC2)
  - Enables machine-to-machine communications for purposes of command and control of cyber defense components, subsystems and/or systems
  - Agnostic of the underlying products, technologies, transport mechanisms
  - Advantages for Interoperability:
    - Abstract actions that interface to external tools and infrastructure that differ from one organization to another
    - Playbooks with OpenC2 minimizes the changes required to incorporate shared COAs

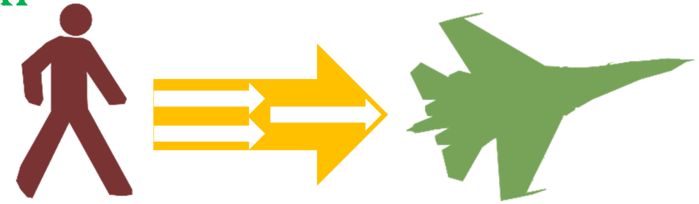
MOSAICS Playbook Hierarchy Design


SIEM Sends Alert
Orchestrator
Ingestion Main Playbook
This playbook handles taking in the Alerts and calling the Detection Playbook
Detection Main Playbook
This playbook handles calling the "check" playbooks that will preform additional integrity checks
Mitigation Main Playbook
This playbook handles deciding on a COA, getting approval for said COA, and calling the specified playbooks to preform said COA
Recovery Main Playbook
This playbook handles deciding on the recovery/reintegration and calls the supporting playbooks
Information Sharing Playbook
This playbook handles creating a shareable report and sharing said report
STOP

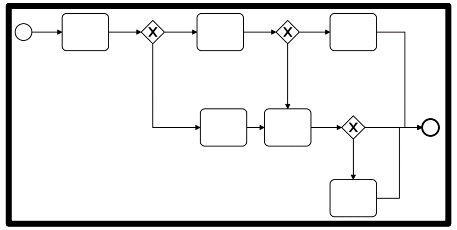
1. Modular design to isolate key functionality
2. Supports future extensibility
3. Required ability to call sub-playbooks



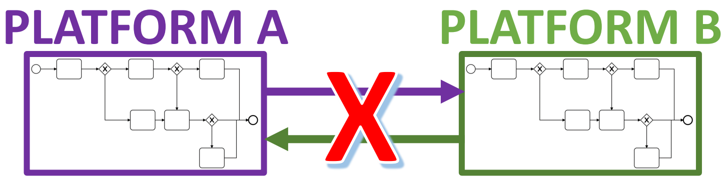
Reuse is Key to MOSAICS Success



Maturation of SOAR marketplace is increasing the speed that organizations can respond to threats and manage their environments.

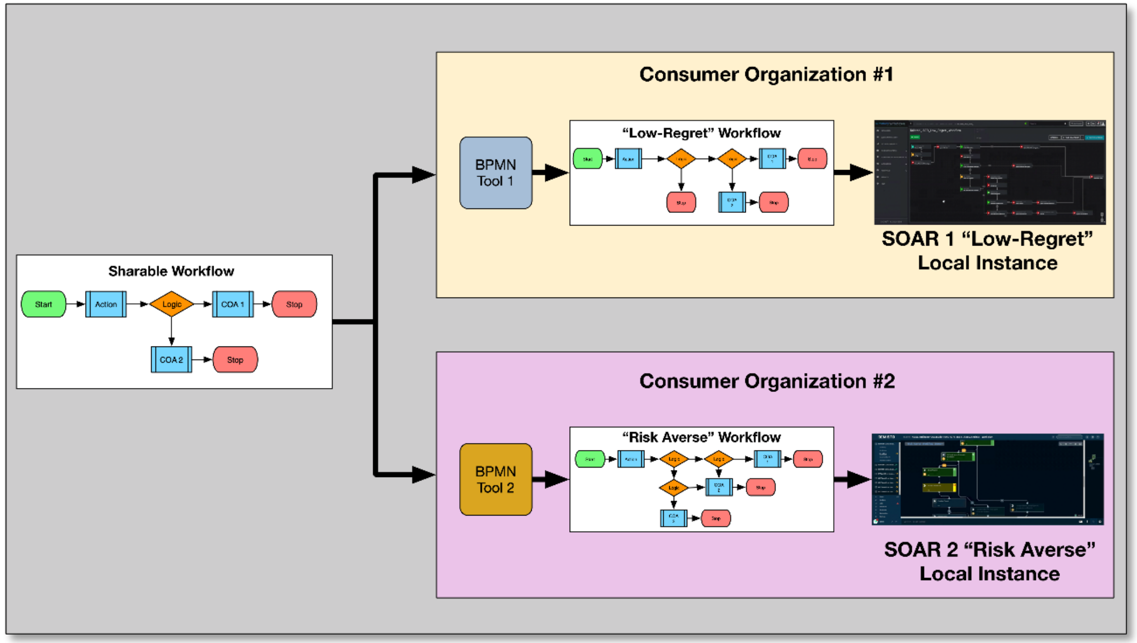


They allow for consistent and repeatable application of an organization’s policy and procedures in response to a trigger.



Many SOAR platforms utilize workflow formats that are proprietary.

Standards Approach
Business Process Model and Notation



- Graphically represents process flow
- Creates a shareable XML file
- Advantages:
  - Ability to create tool-agnostic process flows

Standard Business Process Model and Notation

BPMN

https://www.bpmn.org/

** Over 40 tools available, mostly free licenses and easy to use**

camunda

flowable

Industry Partnership

1. Interoperability / integration through robust, open APIs

2. Support modular design approach
   - Recursive sub-playbooks
   - Automations vs full Playbooks

3. Adopt evolving standards
   - OpenC2, BPMN

4. Industry support is critical to wide adoption
   - Many types of environments but…
   - COTS is a given in every ecosystem
   - Affordable scalability and sustainment

Questions??