Integrated Adaptive Cyber Defense

Introduction to Integrated Adaptive Cyber Defense (IACD) Playbooks

Purpose

The intent of this paper is to be a starting point for conversation with the Integrated Adaptive Cyber Defense (IACD) community on harmonizing the security automation playbook concept to foster agreement on amount of specificity contained within them. The results of community feedback and engagement will be a direct input to development of a playbook requirements thin-specification, which will define the minimum requirements a playbook must meet to an IACD implementation.

Background

Security Automation and Orchestration (SA&O) as a market has taken off. Organizations are increasingly interested in adopting SA&O capabilities, but barriers persist – allocation of security dollars, lack of process maturity, and determining prioritization of which process to automate first. To date, one critically important missing piece of IACD is the connection between an organization's policies and procedures with an SA&O vendor's capabilities. Playbooks can bridge this gap by showing how an SA&O vendor is able to satisfy a client's policy and procedure requirements through repeatable and auditable processes, with points where security automation can be implemented.

Playbooks, Workflows, and Local Instances

The SA&O market is forming rapidly, and terminology is not yet standardized across the IACD community. In the IACD Orchestration Services Thin Specification, initial and high level definitions of both playbook and workflow were presented. The following sections expand on those definitions as well as introduce a third level of abstraction, a "local instance" of a workflow. Community feedback on the level of specificity contained within each abstraction level is highly encouraged.

Figure 1 provides a high-level summary of these levels of orchestration abstraction, from the highest level of detail at playbooks moving towards the most granular at the local instance.

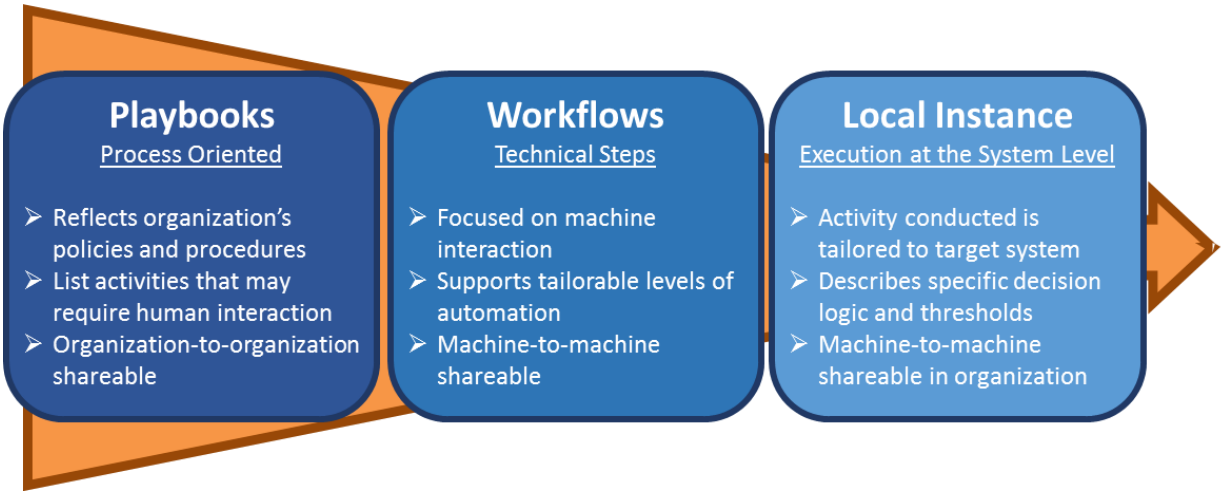

Figure 1: Detail at the Three Levels of Orchestration Abstraction

Contact Us: IACD@jhuapl.edu, https://secwww.jhuapl.edu/IACD/Contact

Playbook

At the highest level of abstraction, 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 performed in response to a cyber-event or other defined trigger condition. Playbooks are meant to be generic enough for broad applicability between organizations while detailed enough to meet specific situations. Playbooks may invoke other playbooks, operate either serially or in parallel, or initiate a workflow depending on the situation or conditions facing the system.

Purpose

The purpose of a playbook is to ***represent a general security process*** in a manner that:

1. Most organizations can associate with a process they are performing
2. Can be mapped to governance or regulatory requirements (e.g. NIST 800-53)
3. Demonstrates a path to automation of the process over time
4. Identifies industry best practices for steps in the process

Defining Characteristics

The primary characteristic of a playbook is that it is designed for a human to understand (i.e. human readable). It represents a general security process at its most basic level, so a playbook can be implemented in a completely manual fashion or increasingly automated as appropriate for the organization.

Workflow

Workflows are the machine understandable codification of playbooks to enable automation of the procedures. Orchestration services execute workflows, interfacing with the other orchestration services and humans as necessary. Workflows are meant to be machine-to-machine shareable, to include sharing between organizations.

Purpose

The purpose of a workflow is to ***implement an organizational playbook*** in a manner that:

1. Is repeatable and auditable
2. Can tailor the amount of automation depending on the needs and capabilities of the system and the desires of the organization
3. Is machine-to-machine sharable

Defining Characteristics

The primary characteristic of a workflow is that it is a structured and machine shareable representation of a security process to support automation and orchestration.

Local Instantiation of a Workflow

A local instance of a workflow is one that has been tailored for a particular environment, executing specific actions on specific devices/applications in response to specific conditions or events. Local instances are meant to be machine-to-machine shareable, although sharing is likely limited to within an organization given the tailoring done (i.e. no two organizations are exactly the same, so a local instance specific to one organization may not be compatible with another organization's environment).

Purpose

The purpose of a local instance of a workflow is to ***orchestrate and execute actions*** in a manner that:

1. Is consistent with local policies, procedures, thresholds, and decision process
2. Incorporates technologies, products, and assets deployed in the local environment
3. Responds to conditions or events that are occurring in the local environment

Defining Characteristics

The primary characteristic of a local instance of a workflow is that it is tailored to execute in a specific environment. So while organizations with different security products and policies can both implement the same workflow, the local instance will be different and likely not usable between the two.

Example Scenario of Vulnerability Mitigation

The following example is intended to show the difference between these three levels of abstraction.

A security tool or process identifies vulnerable software on a device in the enterprise. There are multiple options for mitigation ranging from uninstalling the software to updating to a non-vulnerable version of the software. The person responsible for maintaining the device decides on and then executes the appropriate mitigating actions.

Figure 2 below describes how the scenario's initiating condition, selection of mitigation, and execution of mitigation is carried out at the playbook, workflow, and local instance level of abstraction.

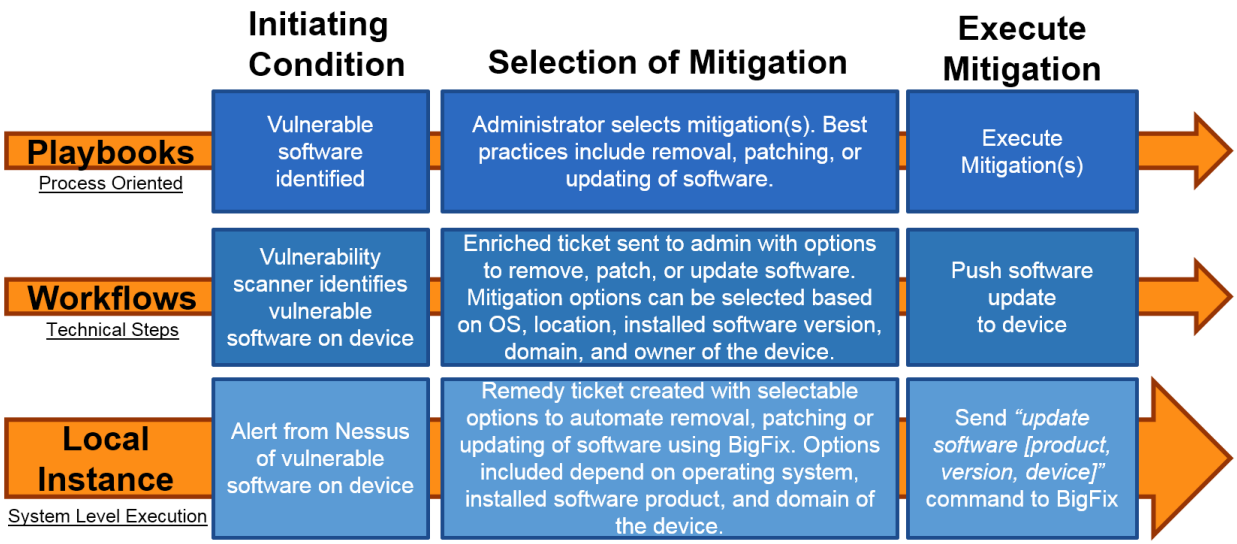

Figure 2: Levels of Orchestration Abstraction at Various Stages of Vulnerability Mitigation

Engaging the Greater Community to Advance the Art

The distinction between "playbooks," "workflows," and "local instance" presented in this paper are a product of discussion and preliminary exploration of existing industry offerings. A separate white paper will detail the various types of recommended content that should be considered included in a playbook. The section for each type contains a description, its purpose, examples of, as well as open questions and topics for discussion.

We are engaging the IACD community of interest to collaborate on playbooks and related products, which includes the Play Book Thin Specification that will begin development starting in mid-summer 2017.

Please join us at the **IACD website** and **IACD – Integrated Adaptive Cyber Defense LinkedIn page** for the latest information, developments, and discussion on the playbook initiative as well as other IACD-related products.