Integrated Adaptive Cyber Defense (IACD) Playbooks

A Specification for Defining, Building and Employing Playbooks to Enable Cybersecurity Integration and Automation

1. PURPOSE

The purpose of this document is to provide the minimum requirements necessary for current and future Integrated Adaptive Cyber Defense (IACD) participants to create security automation playbooks that are supportive of the IACD framework. This thin specification does not overly prescribe or dictate difficult-to-achieve requirements, but presents the minimum conditions of a well-conceived IACD playbook.

2. IACD BACKGROUND AND IACD PLAYBOOKS

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.

Playbooks capture the managed, repeatable cybersecurity and network operations processes in ways to enable integration, automation, and information sharing. By creating and sharing IACD playbooks, both provider and user organizations can help foster the adoption of cyber security automation. Playbooks can be used to improve cyber security operations, capture best practices, highlight local issues in policies or processes, and demonstrate a linkage between local operations/processes and regulatory/compliance requirements.

2.1 Overview of Playbooks

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

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

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, enabling a playbook to be implemented in a completely manual fashion or increasingly automated, as appropriate for the organization.

The IACD framework defines Playbooks in relation to other, increasingly-specific representations of security actions, namely, Workflows and Local Instances (See Figure 1). For additional information regarding the broader IACD framework and the decomposition of playbooks, please visit https://secwww.jhuapl.edu/iacd .

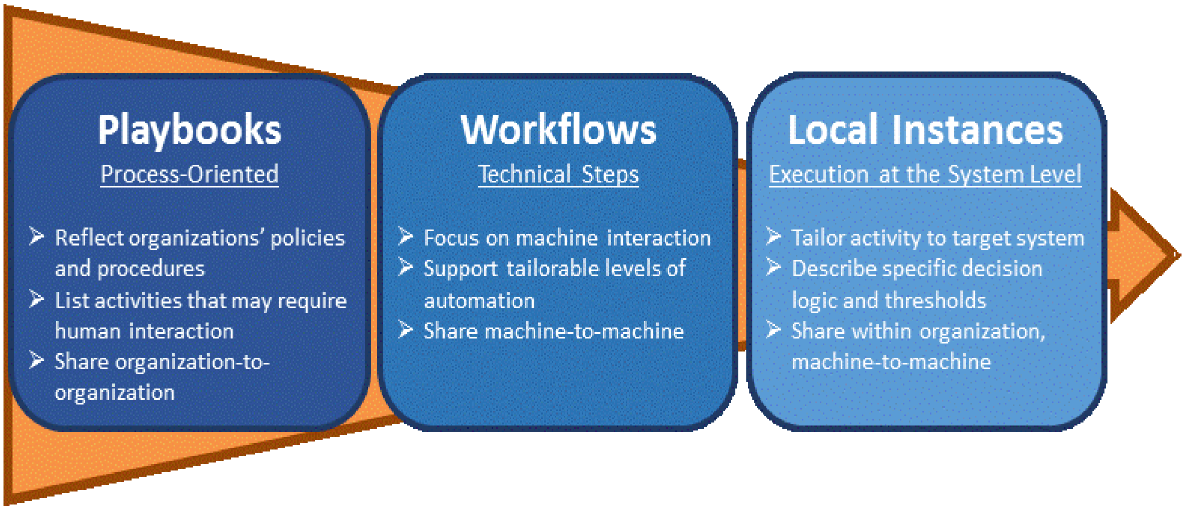

Playbooks
Process-Oriented
Reflect organizations' policies and procedures
List activities that may require human interaction
Share organization-to-organization
Workflows
Technical Steps
Focus on machine interaction
Support tailorable levels of automation
Share machine-to-machine
Local Instances
Execution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

Figure 1: Three Levels of IACD Abstraction

Refer to the **IACD Playbook White Paper – Introduction** for more detailed information about the three levels of IACD abstraction.

2.2 Overarching Tenets and Assumptions

A select set of tenets represent the core assumptions for IACD Participants creating playbooks:

- Playbooks are a ***community-driven, collaborative*** endeavor and ***readily shareable*** between organizations.
- Playbooks are ***generalized for broad applicability*** across organizations.
- Playbooks ***can be tailored*** and used to create workflows or identify existing vendor/community workflows that meet an organization's needs.
- Playbooks ***can be linked together*** to allow organizations to focus on "chunks" of a larger process, until which time organizations may choose to combine several playbooks.
- Playbooks ***can be applied*** to an organization ***regardless of its process maturity or level of automation***.
- Playbooks are not static – they ***can evolve*** with changing policy or operational and technical requirements, but should ***flexibly trace*** to the policy or requirements to ***support risk and readiness assessments***.

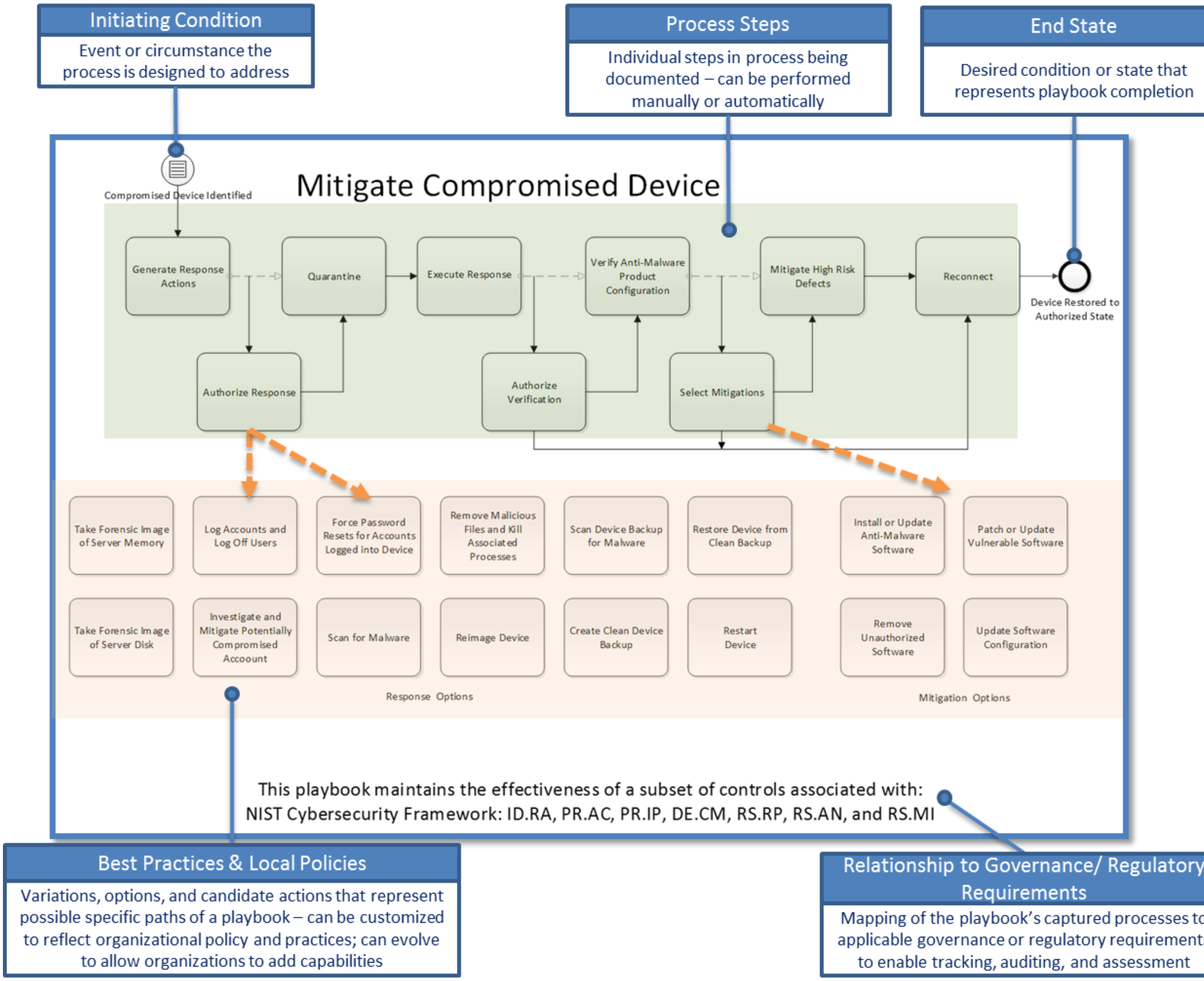
3. MINIMUM PLAYBOOK REQUIREMENTS

All IACD playbooks should contain five content types, which are necessary to address the key tenets and enable effective use and sharing of playbooks among and across organizations. These content types are described in Table 1, below:

Table 1: Content Types Contained within a Playbook

Content Type	Definition
Initiating Condition	Event or circumstance that the documented security process is designed to address
Process Steps	Sequence of steps in process being documented – can be performed manually or in an automated manner
End State	Desired condition or state that represents playbook completion
Best Practices & Local Policies	Variations, options, and candidate actions that represent possible specific paths of a playbook – can be customized to reflect organizational policies and practices; can evolve to allow organizations to add capabilities
Relationship to Governance or Regulatory Requirements	Mapping of the playbook's captured processes to applicable governance or regulatory requirements to enable tracking, auditing, and assessment

The content types are then structured together to represent an IACD Playbook, as depicted in the Figure 2 playbook example. The minimum requirements for each type are captured in the following sections.


Mitigate Compromised Device
Compromised Device Identified
Generate Response Actions
Quarantine
Execute Response
Verify Anti-Malware Product Configuration
Mitigate High Risk Defects
Reconnect
Device Restored to Authorized State
Authorize Response
Authorize Verification
Select Mitigations
Take Forensic Image of Server Memory
Log Accounts and Log Off Users
Force Password Resets for Accounts Logged into Device
Remove Malicious Files and Kill Associated Processes
Scan Device Backup for Malware
Restore Device from Clean Backup
Install or Update Anti-Malware Software
Patch or Update Vulnerable Software
Take Forensic Image of Server Disk
Investigate and Mitigate Potentially Compromised Accoount
Scan for Malware
Reimage Device
Create Clean Device Backup
Restart Device
Remove Unauthorized Software
Update Software Configuration
Response Options
Mitigation Options

Initiating Condition

Event or circumstance the process is designed to address

Process Steps

Individual steps in process being documented – can be performed manually or automatically

End State

Desired condition or state that represents playbook completion

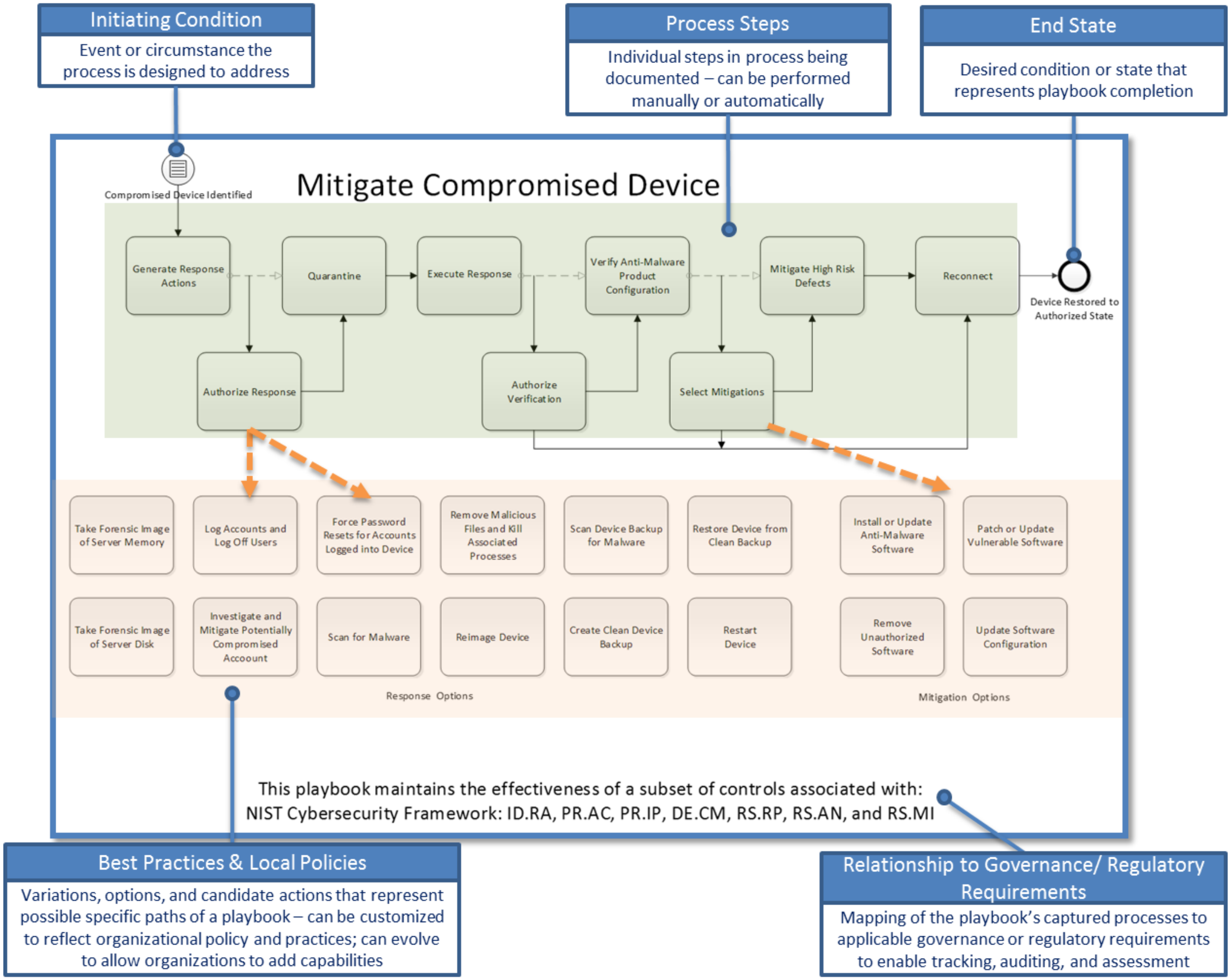
This playbook maintains the effectiveness of a subset of controls associated with:
NIST Cybersecurity Framework: ID.RA, PR.AC, PR.IP, DE.CM, RS.RP, RS.AN, and RS.MI

Best Practices & Local Policies

Variations, options, and candidate actions that represent possible specific paths of a playbook – can be customized to reflect organizational policy and practices; can evolve to allow organizations to add capabilities

Relationship to Governance/ Regulatory Requirements

Mapping of the playbook's captured processes to applicable governance or regulatory requirement to enable tracking, auditing, and assessment


Mitigate Compromised Device
Compromised Device Identified
Generate Response Actions
Quarantine
Execute Response
Verify Anti-Malware Product Configuration
Mitigate High Risk Defects
Reconnect
Device Restored to Authorized State
Authorize Response
Authorize Verification
Select Mitigations
Take Forensic Image of Server Memory
Log Accounts and Log Off Users
Force Password Resets for Accounts Logged into Device
Remove Malicious Files and Kill Associated Processes
Scan Device Backup for Malware
Restore Device from Clean Backup
Install or Update Anti-Malware Software
Patch or Update Vulnerable Software
Take Forensic Image of Server Disk
Investigate and Mitigate Potentially Compromised Accoount
Scan for Malware
Reimage Device
Create Clean Device Backup
Restart Device
Remove Unauthorized Software
Update Software Configuration
Response Options
Mitigation Options

Initiating Condition

Event or circumstance the process is designed to address

Process Steps

Individual steps in process being documented – can be performed manually or automatically

End State

Desired condition or state that represents playbook completion

This playbook maintains the effectiveness of a subset of controls associated with:
NIST Cybersecurity Framework: ID.RA, PR.AC, PR.IP, DE.CM, RS.RP, RS.AN, and RS.MI

Best Practices & Local Policies

Variations, options, and candidate actions that represent possible specific paths of a playbook – can be customized to reflect organizational policy and practices; can evolve to allow organizations to add capabilities

Relationship to Governance/ Regulatory Requirements

Mapping of the playbook's captured processes to applicable governance or regulatory requirements to enable tracking, auditing, and assessment

Figure 2: Example of an IACD Playbook and its Content Types

3.1 Initiating Condition Requirements

IC-01	Pre-defined Condition. An initiating condition shall be based on a pre-defined event or condition that is addressed by an organization's security processes and procedures.
IC-02	Excluded Mechanism. An initiating condition shall trigger the playbook, without including the mechanism that identified or created said condition.

3.2 Process Step Requirements

PS-01	Implementation-Independent. Process steps shall be implementation-independent.
PS-02	Human Involvement. Process steps shall reflect the potential for administrator or analyst involvement (e.g., decision-making oversight to authorize or approve).
PS-03	Automation. Process steps should provide an incremental path toward automation.
PS-04	Branching Paths. Process steps shall document potential branching paths, without including decision logic.
PS-05	Link to Other Playbooks. Process steps shall be able to link to other playbooks.

3.3 End State Requirements

ES-01	Desired Result. An End State shall unambiguously document the conditions, results, or state that must exist to exit the playbook (e.g., a device is compliant with an authorized state, or an enriched alert is sent to analyst).

3.4 Best Practice & Local Policy Requirements

BP-01	Differentiation. Best practices/local policies shall be differentiated from the core security automation and orchestration (SA&O) process steps, which are applicable to all users.
BP-02	Response Actions/Options. Best practices/local policies shall identify potential response actions for organizations to implement.
BP-03	Multiple Options. Best practices/local policies should include options from multiple sectors, asset types, risk tolerances, and security process maturity.

3.5 Relationship to Governance or Regulatory Requirements

GR-01	Identification. Playbooks shall identify the security controls, regulatory requirements, or other governance-related items addressed by the playbook process steps.
GR-02	Mapping. Playbooks shall allow organizations to map their governance or regulatory obligations to the process steps detailed within.