IACD

Integrated Adaptive Cyber Defense

How to Build an IACD Playbook

Purpose of a Playbook:

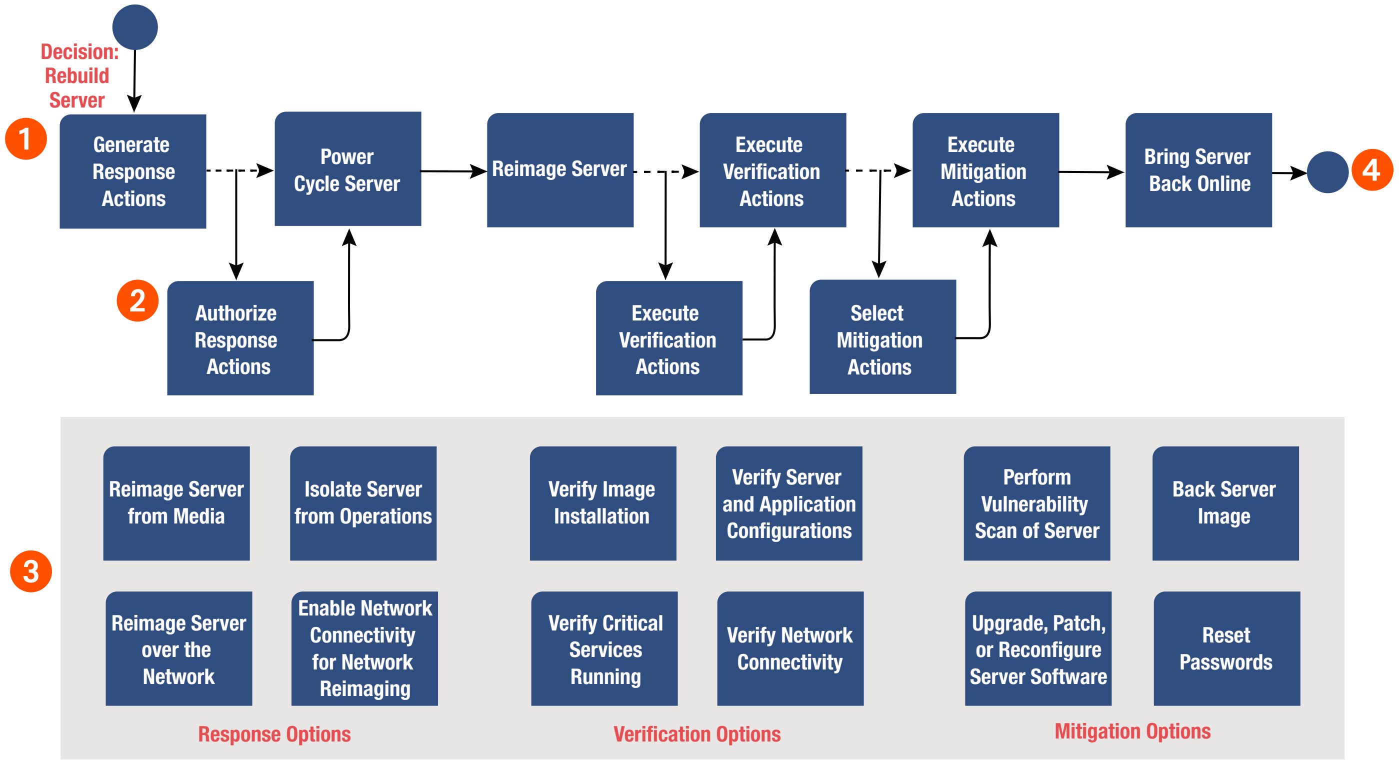
To represent a general security process *in a manner that:*

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

Playbook Content Types:

1. Initiating Condition
2. Process Steps
3. Best Practices and Local Policies
4. End State
5. Relationship to Governance or Regulatory Requirements

Example Playbook



Decision: Rebuild Server

1 Generate Response Actions

Power Cycle Server

Reimage Server

Execute Verification Actions

Execute Mitigation Actions

Bring Server Back Online

4

2 Authorize Response Actions

Execute Verification Actions

Select Mitigation Actions

3

Reimage Server from Media

Isolate Server from Operations

Reimage Server over the Network

Enable Network Connectivity for Network Reimaging

Response Options

Verify Image Installation

Verify Server and Application Configurations

Verify Critical Services Running

Verify Network Connectivity

Verification Options

Perform Vulnerability Scan of Server

Back Server Image

Upgrade, Patch, or Reconfigure Server Software

Reset Passwords

Mitigation Options

5 This playbook maintains the effectiveness of a subset of control associated with:

http:// https://secwww.jhuapl.edu/iacd @IACD_automate https://www.linkedin.com/groups/8608114 icd@jhuapl.edu

Steps to Build a Playbook

1. **Identify the initiating condition.**

   Think About: What event or condition is going to start this playbook? This could be a time-based trigger, the detection of an event, or the decision to act.

2. **List all possible actions that could occur in response to this initiating condition.**

   Think About: How could I respond to this condition? What steps would I take to mitigate this threat? Don't worry about order right now!

3. **Iterate through the actions list from Step 2 and categorize the actions based on whether they are required steps or whether they are optional.**

   Think About: Is this step necessary to mitigate or investigate this event, or is it a best practice? Some best practices have become standardized or widely implemented, while others may be considered extraneous. It's OK if it's unclear whether some actions are required or optional; it's up to you to categorize accordingly.

4. **Use the required steps from Step 3 to build the playbook process steps diagram.**

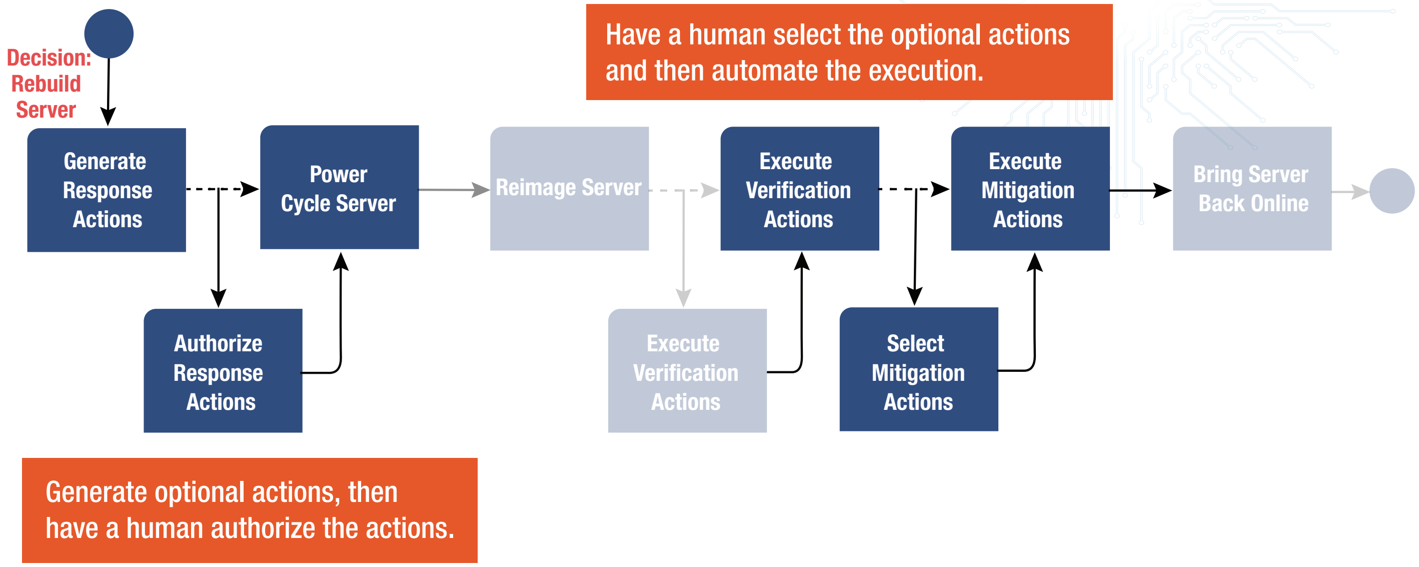
   Think About: Ordering. This is the time to think about the order in which you would perform these actions.

5. **Iterate through the optional actions and decide whether the actions can be grouped by activity or function. For example: Monitoring, Enrichment, Response, Verification, or Mitigation.**

6. ***Think About:*** **Are there possible actions that can only take place in certain parts of the playbook? This is how you would group the actions.**

7. **Modify the playbook process steps diagram from Step 4 to include the points where optional actions would be selected.**

Special Note: To indicate where optional actions would be selected, use either of the following templates:


Decision: Rebuild Server
Generate Response Actions
Power Cycle Server
Reimage Server
Execute Verification Actions
Execute Mitigation Actions
Bring Server Back Online
Authorize Response Actions
Execute Verification Actions
Select Mitigation Actions

Have a human select the optional actions and then automate the execution.

Generate optional actions, then have a human authorize the actions.

The dashed line indicates that selecting the optional actions can be authorized or performed by a human. However, on the basis of your comfort level, this process of selecting or authorizing and then executing the optional actions could be completely automated, thus putting you on the path toward full automation!

8. Use the optional actions from Step 5 to fill out the action options box below the process steps.

9. Confirm that the playbook ends in an end state or offers a new initiating condition to an appropriate playbook.

    Think About: Could this playbook initiate a different or complementary playbook? Does this playbook result in a discrete end state? The playbook should not end with ambiguity.

    Special Note: The playbook(s) that this current playbook initiates may not even exist yet. That's OK! Use this guide to make as many playbooks as you need.

10. Identify the regulatory controls and requirements that the actions in this playbook satisfies.

    Think About: Think about the relationship of this playbook to governance or regulatory requirements and whether this playbook would satisfy them.