# After Action Activities

## Overview

After a cyber incident, certain activities should take place so that an organization may respond to it appropriately with the understanding that the adversary may still be present in the organization's environment. These activities should take into account the need for long term business functions to continue. This document describes how to apply *Adaptive Response*[1], *Analytic Monitoring, Coordinated Defense,* and *Realignment* resiliency techniques.

## Applying *Adaptive Response* to Detect Adversary Impacts

*Adaptive Response* – implementing cyber courses of actions (CCoA) to manage risk – in order to respond dynamically to specific situations, using agile and alternative operational contingencies to maintain minimum operational capabilities, limit consequences and avoid destabilization. *Adaptive Response* optimizes an organization's capability to respond in a timely and appropriate manner to adversary activities, thus maximizing its capability to maintain the integrity and availability of core services. There are three approaches to applying *Adaptive Response*:

- Dynamic Reconfiguration: Make changes to an element or component while it continues operating.
- Dynamic Resource Allocation: Change the allocation of resources to tasks or functions without terminating functions or processes.
- Dynamic Composability: Replace software elements with equivalent functionality without disrupting service.

### Priorities for Immediate Action with *Adaptive Response*

The top priorities for *Adaptive Response* are:

- Update existing policies to identify when and how to respond to specific incident indicators.
    - Review the responses to indicators specified by the organization's policy.
    - Ensure that the relevant stakeholders are trained and made aware of changes to the policies.
- Implement a process for reviewing, updating, and testing manual response procedures and automated capabilities.
    - Test these elements and update processes and procedures. Consider using mission assurance and mission impact tools as part of this testing.
    - Provide guidance to stakeholders regarding the use and tradeoffs of the various manual procedures and automated capabilities (e.g., orchestrated activities such as taking input from sensors and using an automated process to make and implement actions – actions are taken much more quickly but there is a higher chance of false alarms).
    - Review elements critical to the organization to ensure that there are alternate elements that can replace the critical ones, while the organization continues operating, ensuring adequate resources are allocated for critical processes.

## Applying *Analytic Monitoring* to Detect Adversary Impacts

*Analytic Monitoring* – Continuously gather, fuse, and analyze threat intelligence data to identify vulnerabilities, find indications of potential adverse conditions, and identify potential or actual damage – Optimizes an organization's ability

[1] All italicized words are defined in the *Cyber Resiliency Terms and Concepts* document.

to detect adversary activities, thus maximizing the ability to identify and contain the adversary's impacts. There are three approaches to applying *Analytic Monitoring:*

- Monitoring and Damage Assessment: Monitor and analyze behavior and characteristics of components and resources to look for indicators of adversary activity, detect and assess damage, and watch for adversary activities during recovery and evolution.
- Sensor Fusion and Analysis: Fuse and analyze monitoring data and preliminary analysis results from different components, together with externally provided threat intelligence.
- Malware and Forensic Analysis: Analyze malware and other artifacts left behind by adversary activities.

### Priorities for Immediate Action with *Analytic Monitoring*

The top priorities for *Analytic Monitoring* are:

- Based on the after action analysis update the analytic monitoring capabilities and procedures to more quickly identify adversary presence.
    - Identify adversary behaviors and characteristics based on the incident and incorporate them into both analytic monitoring and analysis processes.
    - Identify events associated with adversary activities based on the incident and incorporate them into both analytic monitoring and analysis processes.

## Applying *Coordinated Defense* to Share Situational Awareness

*Coordinated Defense* – managing multiple, distinct mechanisms adaptively and in a coordinated way – can ensure that defender actions support both the immediate and long term needs of the enterprise. There are two major implementation approaches to *Coordinated Defense*.

- Technical Defense-in-Depth: Make use of multiple protective mechanisms, applied at different architectural layers or locations (e.g., application, endpoints, network and incident response perimeters).
- Coordination and Consistency Analysis: Apply processes, supported by analytic tools, to ensure that defenses are applied and cyber courses of action are defined and executed in a coordinated, consistent, and non-disruptive way.

### Priorities for Immediate Action with *Coordinated Defense*

The top priorities for *Coordinated Defense* are:

- Review public incident reports to identify and address potential shortcomings in the organization's own infrastructure.
    - If the organization has not joined an external incident sharing collaboration already, do so now in order to obtain more extensive information about incidents and the threat environment than is generally available in public accounts.
- Document and share the findings of the after action analysis with the appropriate stakeholders and partners.
    - Identify key findings such as vulnerabilities and risk tradeoffs and where in the cyber attack lifecycle these findings are relevant.
    - Identify all stakeholders and partners.
    - Provide a set of activities and the likely consequences of not making changes to defensive posture in a coherent manner.

## Applying *Realignment* to Limit Adversary Impacts

*Realignment* – Aligning cyber resources with core aspects of the business functions – enables defenders to reduce the attack surface of the organization by minimizing the possible attack vectors. There are four ways of implementing realignment. They are:

- Purposing: Ensure cyber resources are used consistent with critical mission purposes.
- Offloading/Outsourcing: Offload supportive but non-essential functions to a service provider that is better able to support the functions.
- Restriction: Remove or disable unneeded risky functionality or connectivity, or add mechanisms to reduce the risk.
- Replacement: Replace risky implementations with less-risky implementations.

### Priorities for Immediate Action with *Realignment*

The top priorities for *Realignment* are all dependent on knowing what functions are critical to the enterprise. Once this knowledge has been established, the following actions should be implemented:

- Review the enterprise and system architectures and remove or disable any non-essential risky component.
    - Identify which components are high risk and do not support essential functions – remove these non-essential components.
    - Test essential functions to ensure there are no hidden links to what was considered non-essential.
- Review the use of cyber resources and ensure that their use is consistent with the critical mission or business objectives.
    - Ensure that any implied access restrictions to the resources are applied explicitly.
    - Ensure that components and systems are appropriately separated (e.g., servers generally do not need web browsers on them).
    - Ensure that separation of duties required by policy are implemented in the architecture or through procedures.
    - Identify noncritical and virtual resources that can be used to support core functionality in the event of future incidents.
- Replace high-risk implementations with low risk ones.
    - Replace out of date software implementations with versions that are licensed and maintained.
    - Reconfigure software (both COTS and FOSS) to reduce functionality to only that which is required for business objectives.

## Preparing for the Future

As the adversary continues to evolve their tactics, it is important to realize the notion of “after the incident” becomes more problematic and the need to incorporate continuous evolution and resiliency enhancement becomes more critical. Unlike non-adversarial events (e.g., natural disasters) adversarial cyber events do not necessarily have a definitive endpoint nor can one be certain that the adversary or their malware is not still present in the organization’s infrastructure. This makes it more challenging to pursue and capture the necessary after action information. Understanding the cyber attack lifecycle will help an organization understand and describe the stage of the current attack and what resources may be threatened.

Some organizations are hesitant to document anything about an incident due to potential for legal discovery. In addition there are also fears with regard to collaborating with industry partners because of trade secrets and competition. These concerns must be overcome to deal effectively with the evolving threat the adversary poses.

As the organization adopts resiliency techniques it also needs to ensure consistency and avoid cascading failures across distributed systems. Dynamic resource allocation tools and adaptive management tools are continuing to develop. Tools are only useful when properly implemented, staffed, and managed, so it is critical to have staff knowledgeable in how to deploy these tools. Political issues with respect to responsibilities for ongoing and dynamic risk management must also be resolved before implementing these tools within the organization.