After Action Activities:
Continually Improving Enterprise Resilience

This paper outlines the best practices for #12 After Action Activities.

Planning and Preparation Activities	***Recovery and Reconstitution Activities***
0. Disrupting the Attack Surface	
1. Architect to Protect *2. Secure Administration* *3. Access Control* *4. Device Hardening* *5. Backup Strategies* *6. Cyber Continuity of Operations (COOP) Planning*	*7. Cyber COOP Execution* *8. Secure Communications* *9. Core Services* *10. Data Recovery Strategies* *11. Forensics* ***12. After Action Activities***

The BIG Idea

By performing After Action Activities, an organization can review the details of an incident, identify shortfalls in its security architecture, and determine where and how to enhance resilience capabilities.

Cyber Resiliency Goals & Objectives

After Action Activities support the cyber resilience *Evolve*[1] goal and the *Transform* and *Re-Architect* objectives.

Design Principles

Once an organization has discovered the extent of an incident, the design principles for After Action Activities help improve the enterprise's capability to detect, respond to, and recover from the impact of this incident by providing information on the adversary's actions and the vulnerabilities exploited as well as recommendations and prevention strategies to improve the organizations response.

- *Adaptive Response*: Improve existing response capabilities and actuator thresholds; identify and implement new approaches to enhance protection against future incidents.
- *Analytic Monitoring*: Gather, fuse and analyze data to identify adverse conditions, reveal the extent of adversary activity and identify damage.
- *Coordinated Defense*: Improve Cyber COOP procedures and define business processes to enable cyber defenders to share incident reports and collaborate on new approaches.
- *Realignment*: Identify and disable any non-essential system capabilities that might have caused or increased the severity of the incident.

What Can Be Done Now

The following resiliency techniques can help transform business processes and redesign systems to use existing technologies more effectively:

- *Adaptive Response*

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

  - Update existing policies and procedures to identify when and how to respond to specific incident indicators.
  - Implement a process for reviewing, updating, and testing manual response procedures and automated capabilities.
- *Analytic Monitoring*
  - Perform after action analysis in order to update the analytic monitoring capabilities and procedures to more quickly identify adversary presence.
- *Coordinated Defense*
  - Review public incident reports to identify and address potential shortcomings in the organization's own infrastructure.
  - Document and share the findings of the after action analysis with the appropriate stakeholders and partners.
- *Realignment*
  - Review the enterprise and system architectures and remove or disable any non-essential risky components.
  - Review the use of cyber resources and ensure that their use is consistent with the critical mission or business objectives.
  - Replace high risk implementations with lower risk ones.

The Right People & Policies

Creating a foundation of resiliency requires specific skills and policies, including:

- System administrators and cyber defenders who understand the value of collaboration and can interpret and apply findings to improve resiliency.
- Legal support who understand the value of publicizing incident details that can help defenders and exposing adversary's TTPs, and can provide counsel to maximize the benefits of "lessons learned" from the incident while protecting the organization against negative fallout.
- Strategic planning to ensure that any changes made to the enterprise architecture as a result of "lessons learned" do not create a larger, more vulnerable attack surface.

Cyber Attack Lifecycle[2]

Using the cyber resiliency techniques, *Analytic Monitoring,* as described above, defenders can detect and analyze the adversary's efforts to maintain a presence in the enterprise. The adversary's efforts to control initial victims, execute the attack plan and maintain a presence in the enterprise may be degraded or even negated by the defender's ability to implement *Adaptive Response, Coordinated Defense, and Realignment.*

Synergies and Barriers

Synergies among practices exist between the techniques discussed in this document. *Analytic Monitoring* relies on good *Coordinated Defense. Analytic Monitoring* can also be improved by having diverse sensors (both in type of sensor and in what is being sensed). Likewise, *Adaptive Response* relies on good *Analytic Monitoring,* while *Coordinated Defense* relies on both *Adaptive Response* and *Realignment.*

Barriers to adoption include the following:

[2] The Cyber Attack Lifecycle is described in the *Cyber Attack Lifecycle and Resilience* document.

- Improper incident handling or failure to collect sufficient forensic evidence.
- Fear of documenting incidents or collaborating with industry partners.
- 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.

Just Ahead

Attackers are constantly advancing their tactics to stay ahead of defenders. Organizations need to collaborate and tap into public and private channels to stay up-to-date on these new technologies and threat tactics. After action analysis is critical to this effort and can give defenders the edge they need to achieve and sustain cyber resiliency. 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. Thus, the traditional, static "after action report" may become more of a snapshot in time and give way to continual analysis and reporting.