Forensics:
Restoring Trust in the Enterprise

This paper outlines the best practices for #11 Forensics.

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

Investigating cyber incidents provides organizational assurance that an incident has been contained and that the response has identified all exploited systems, user accounts, as well as all exfiltrated data. In addition, proper forensic processes preserve evidence for use in legal venues.

Cyber Resiliency Goals & Objectives

Forensics supports the *Recover*[1] goal and the *Reconstitute* and *Understand* objectives.

Design Principles

The design principles for Forensics improve the ability to determine the entire scope of an incident and the affected assets, allowing accounts, systems, data and services to be reconstituted. Forensics also provides a means to preserve the evidence of what happened during an attack in a form that is suitable for court.

- *Analytic Monitoring*: Don't confuse absence of evidence with evidence of absence; refine organization-wide data collection to capture and retain forensics in case of future incidents; improve situational awareness and data access capabilities for efficient evidence retrieval.
- *Coordinated Defense*: Define business processes for proper incident handling, reporting, and investigation; establish partnerships to share forensic techniques and best practices.
- *Segmentation*: Ensure malware analysis takes place in an isolated environment.
- *Substantiated Integrity*: Reduce or eliminate compromises to the integrity of incident forensic evidence, such as event logs (both as they are being collected and while in storage).

What Can Be Done Now

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

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

- *Analytic Monitoring*
  - Determine suitability of event logs and data collections as incident forensics.
- *Coordinated Defense*
  - Train cyber analysts in incident response and proper handling of forensic evidence.
  - Collaborate with other entities to share best practices for incident handling.
- *Segmentation*
  - Ensure that those elements (e.g., devices, applications and databases) used to perform malware analysis on infected components are appropriately isolated to avoid further spread of the infection.
- *Substantiated Integrity*
  - Identify ways to ensure integrity of forensic evidence (e.g., integrity-verifying backup, checksums) so that attacker's attempts to falsify logs are identified.

The Right People & Policies

Creating a foundation of resiliency requires specific skills and policies:

- Systems administrators and cyber security professionals trained in
  - Proper evidence handling
  - Incident investigation procedures
  - Working with law enforcement, government agencies and legal council
- Business policies and supporting processes that ensure
  - Proper collection and storage of potential evidence
  - Proper incident response procedures, including the chain-of-command

Cyber Attack Lifecycle[2]

Using the cyber resiliency techniques, *Analytic Monitoring, Coordinated Defense*, *Segmentation*, and *Substantiated Integrity*, as described above, defenders can detect the adversary's attack on the enterprise and limit the damage the malware causes. The use of *Analytic Monitoring* with *Substantiated Integrity* can detect to which systems the adversary has delivered malware. When the adversary attempts to, employ mechanisms to manage the initial victims, and execute the attack plan, the *Coordinated Defense*, *Segmentation* and the *Substantiated Integrity* techniques impede these efforts and limit their effects.

Synergies & Barriers

Synergies among practices include *Analytic Monitoring*, *Segmentation*, and *Coordinated Defense*. *Coordinated Defense* is more effective when applying various *Analytic Monitoring* solutions in an organization; and *Coordinated Defense* and *Segmentation* are synergistic in their efforts to provide isolation and layers of defensive.

Barriers to adoption include:

- Records and data management practices that do not take forensic requirements into account
- Gaps in data collection that prevent a full investigation and allow malware to persist.
- Lack of guidance and incident response procedures that may result in contaminated evidence.

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

- Conflicts between the need to collect data, the cost of collecting and storing data and the legal requirements of records and information management.

Just Ahead

The attack surface is expanding due to the advance of embedded technology (e.g., Internet of Things, cyber-physical systems, and medical devices) and policies such as bring-your-own-device (BYOD). With more potential exploitation points and places for adversaries to hide, synergies between *Analytic Monitoring* and *Adaptive Response* and support for *Dynamic Positioning* should be explored. In addition deception environments (e.g. honey nets) are becoming more common and easier to deploy. They provide new ways to balance the benefits of forensics on an attack with the need to remove the adversary quickly and thoroughly.