Forensics

Overview

Investigating cyber incidents requires defenders identify compromised systems and data as well as try to predict what the adversary will do next. Defenders must balance the benefits of forensics with the need to remove the adversary quickly. They must also preserve forensic data in case of future incidents and as legal evidence. This document describes how to apply *Analytic Monitoring*[1], *Coordinated Defense, Segmentation* and *Substantiated Integrity* resiliency techniques.

Applying *Analytic Monitoring* to Detect Adversary Impacts

Analytic Monitoring – Continuously gathering, fusing, and analyzing threat intelligence data to identify vulnerabilities, finding indications of potential adverse conditions, and identifying potential or actual damage – Optimizes an organization's ability 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:

- Determine suitability of event logs, data collections, and policies as incident forensics.
    - Review Intrusion Detection System (IDS) logs, host and network sensors, event logs and Security Information and Event Management (SIEM) data to ensure the needed data is collected and stored for an appropriate amount of time.
    - Ensure that forensic relevant data is properly protected from modification.
    - Ensure that collection capabilities are consistent across the environment so that blind spots are eliminated (e.g., consistency in IPv4 data collection and IPv6 data collection).

Applying *Coordinated Defense* to Share Situational Awareness

Coordinated Defense – managing multiple, distinct mechanisms adaptively and in a coordinated way – can ensure that forensic efforts 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.

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

Priorities for Immediate Action with *Coordinated Defense*

The top priorities for *Coordinated Defense* are:

- Train cyber analysts in incident response and proper handling of forensic evidence.
  - Ensure defenders know where the forensic data is stored and how to use the data without destroying or modifying it.
- Collaborate with other entities to share best practices for incident handling.
  - Collaborate within the enterprise across security, legal and information areas to ensure coordination with respect to forensics information preservation and use.
  - Collaborate with government and business organizations to share relevant indications and warning information regarding possible cyber threats.
- Ensure there are detection mechanisms at various levels in order to identify inconsistencies that may be evidence of malware tampering.

Applying *Segmentation* to Limit Adversary Impacts

Segmentation – physical or logical separation or isolation of communications based on trustworthiness and criticality – enables defenders to study the adversary's action without the adversary's awareness of the scrutiny. Separation or isolation can be physical or logical, and predefined or dynamic.

- Logical Segmentation: Separate devices, networks, services, and data repositories using encryption and access control mechanisms.
- Predefined Segmentation: Define enclaves (including separate Active Directory elements), segments, or other types of resource sets based on criticality and trustworthiness, so that they can be protected separately and, if necessary, isolated.
- Dynamic Segmentation/Isolation: Change the definition of enclaves or protected segments, or isolate resources, while minimizing operational disruption.

Priorities for Immediate Action with *Segmentation*

The top priorities for *Segmentation* are:

- Ensure that those elements performing malware analysis on infected components are appropriately isolated to avoid further spread of the infection.
  - Physically isolate the compromised system or incorporate it into forensic network using techniques such as tarpitting, dynamic honeynetting depending on the needs and capabilities of the organization.
  - Isolate the Computer Network Defense (CND) enclave using firewalls, separating of inbound and outbound traffic, and separating requests from responses so that CND can study the potential effects without compromising the organization's environment.

Applying *Substantiated Integrity* to Limit the Adversary's Ability to Hide

Substantiated Integrity – ascertaining whether critical services, information stores, information streams, and components have been corrupted – can prevent an adversary from modifying forensic evidence such as logs and thereby prevents them from hiding their presence. There are three approaches to *substantiated integrity*:

- Integrity/Quality Checks: Apply and validate checks of the integrity or quality of information, components, or services.
- Provenance Tracking: Identify and track the provenance of data, software, and/or hardware elements.

- Behavior Validation: Validate the behavior of a system, service, or device against defined or emergent criteria (e.g., requirements, patterns of prior usage).

Priorities for Immediate Action with *Substantiated Integrity*

- Identify ways to ensure integrity of forensic evidence.
    - Use checksums and time stamps or store on write once, read many (WORM) storage media to ensure that forensics data has not been modified since collection.
    - Require cryptographic certificates and signatures when receiving forensics data electronically (e.g., via email).

Preparing for the Future

Organizations should consider employing an integrated analysis team of forensic/malicious code analysts, tool developers, and real-time operations personnel. Having such a team allows organizational personnel, including developers, implementers, and operators, to share relevant information and facilitates the rapid detection of intrusions, development of appropriate mitigations, and the deployment of effective defensive measures.

Deception environments and techniques (e.g., honeynets and honeytokens on valid endpoints) are maturing and becoming easier to deploy. As they do so, they make it easier to balance the benefits of forensics with the need to remove the adversary quickly. Properly configured they can also aid in identifying which types of embedded devices and non-enterprise owned systems present are the greatest risks and what risks those may be.

The increased use of virtualization makes it easier to quickly recover from an attack as well expunge (albeit temporarily) an adversary's foothold in an organization. But at the same time, the non-persistence of data via virtualization (e.g., thinly provisioned cloud environments) can make it even more difficult to analyze adversary malware and to retain a legally viable set of evidence.

In addition, the legal and regulatory environment is changing. What is admissible in court and what is considered discoverable data as well as what an enterprise is required or prohibited from collecting need to be taken into account as the rules change. In addition, the forensic response and any potential disclosure may implicate the need to contact an appropriate law enforcement or government agency (e.g., an organization should not report that a state actor was responsible for a breach, before contacting the appropriate law enforcement and government agencies).