Digital Forensics for Health

CSP012

PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)

DFIR: How to?

The DFIR Process

How To?

Organizations should establish robust incident response plans (IRPs), conduct regular training exercises, and implement proactive measures such as threat hunting and vulnerability assessments.

- Developing and documenting incident response playbooks outlining roles, responsibilities, and communication protocols during a cyber incident.
- Conducting tabletop exercises simulating various cyberattack scenarios to test the effectiveness of response procedures.

Detection and Identification: Early detection of cyber threats relies on the use of intrusion detection systems (IDS), security information and event management (SIEM) solutions, and anomaly detection tools.

- Setting up SIEM rules to trigger alerts for suspicious login attempts or abnormal network traffic patterns indicative of a potential breach.
- Deploying endpoint detection and response (EDR) agents to monitor and correlate endpoint activities for signs of compromise.

Digital Forensic Investigation

Before we begin.

Before initiating a forensic investigation in healthcare, it's crucial to ensure that the data remains unchanged throughout the investigation process.

- **Investigation Scenario:** A healthcare facility suspects unauthorized access to patient records.
- **Preservation Technique:** Forensic investigators utilize write-blocking devices to acquire digital evidence from servers hosting patient records.
- **Tool Implementation:** Hashing algorithms such as SHA-256 are applied to verify the integrity of acquired data against original records. Assurance of data integrity allows investigators to analyze evidence confidently, ensuring accurate findings for legal proceedings.

KALI Forensic Mode: Kali Linux comes pre-loaded with a comprehensive selection of open-source forensic software. This includes popular tools for disk imaging, file analysis, memory forensics, network forensics, and more. Having these tools readily available simplifies the forensic workflow and enhances productivity.

- Investigation Scenario: A healthcare facility suspects unauthorized access to patient records.
- Preservation Technique: Forensic investigators utilize write-blocking devices to acquire digital evidence from servers hosting patient records.
- Tool Implementation: Hashing algorithms such as SHA-256 are applied to verify the integrity of acquired data against original records.

Root Cause Analysis (RCA)

Definition

Root cause analysis (RCA) is the process of identifying the fundamental reason or underlying factor responsible for a problem or issue.

- Enables addressing issues at their source, leading to more sustainable solutions.
- Resolving root causes prevents the problem from reoccurring, saving time and resources.

Steps in Root Cause Analysis: 1) Identify the Problem, 2) Gather Data, 3) Analyze Data, 4) Determine Root Cause, 5) Implement Solutions, 6) Monitor and Evaluate

Example for RCA: Unauthorized access to sensitive healthcare data.

- Root Cause: Weaknesses in network security protocols and inadequate access controls.
- Digital Forensics Investigation: RCA guides digital forensics experts in uncovering evidence related to the breach, such as compromised credentials or exploited vulnerabilities.
- Incident: Malware infection leading to system compromise.
- Root Cause: Lack of endpoint security measures and outdated software patches.
- Digital Forensics Investigation: RCA helps identify the initial entry point of the malware and traces its propagation throughout the network.

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

Please send all questions to:
stylianos.karagiannis@pdmfc.com