The International Association of Computer Investigative Specialists

Enterprise – Cyber Incident Forensic Response

Core Competencies

IACIS Enterprise – Cyber Incident Forensic Response (eCIFR) Program

The eCIFR core competencies described in this document are a binding set of competencies that guide the training program to ensure that the skills and knowledge points are delivered within the training program.

IACIS Enterprise – Cyber Incident Forensic Response (eCIFR) Core Competencies
There are nine competency areas addressed in the eCIFR Program:

i. **SIEM**
ii. **Endpoint Detection & Response (EDR)**
iii. **Velociraptor – Ability to traverse networks (*velociraptor is the tool)***
iv. **TimeSketch**
v. **Azure**
vi. **AWS**
vii. **Enterprise Security Fundamentals**
viii. **Cyber Threat Intelligence (CTI)**
ix. **Capstone Exercise**

i. SEIM

a. Understand concepts related to the role of SIEMs in a network environment.
b. Ability to search and query syntax and techniques to conduct log analysis in Windows Defender/Sentinel.
c. Ability to analyze Windows logs in Sentinel.
d. Knowledge of search and query syntax and techniques to conduct log analysis in ELK.
e. Ability to use ELK to conduct analysis.

ii. Endpoint Detection & Response (EDR)

a. Understand concepts related to the role of EDR in a network environment.
b. Knowledge of search and query syntax and techniques to conduct analysis using an EDR.
c. Ability to conduct EDR analysis concepts in a Capture-The-Flag exercise.

iii. Velociraptor

a. Understand concepts related to the role of Velociraptor in a network environment.

b. Knowledge of how to build and implement Velociraptor in the network.
c. Understanding of how to integrate community hunts into Velociraptor.
d. Ability to conduct basic and advanced searches in Velociraptor.

iv. TimeSketch

a. Ability to build and implement TimeSketch in an investigation.
b. Knowledge of and ability to conduct timeline development.
c. Ability to create timelines from images, add the timeline to TimeSketch and conduct analysis.

v. Azure

a. Understanding the Azure platform.
b. Knowledge of the most common areas within Azure involved in an incident.
c. Familiarity with security capabilities within the Azure environment.
d. Familiarity with obtaining forensic images in an Azure environment.

vi. AWS

a. Understanding the AWS platform.
b. Knowledge of the most common areas within AWS involved in an incident.
c. Familiarity with security capabilities within the AWS environment.
d. Familiarity with obtaining forensic images in an AWS environment.

vii. Enterprise Security Fundamentals

a. Knowledge of the cyber Kill Chain
b. Understanding the Incident Response Lifecycle
c. Ability to use of the OODA Loop for decision making to manage a cyber incident.
d. Knowledge of the contents of Cybersecurity Incident Response Plans (CIRP) and the role of the CIRP during an incident.

viii. Cyber Threat Intelligence (CTI)

a. Understand CTI fundamental concepts.
b. Knowledge of the Intelligence Lifecycle.
c. Familiarity with the MISP VM CTI database platform.
d. Ability to use Internet sites to conduct Open-Source Intelligence (OSINT) analysis.

ix. Capstone Exercise

a. Witness a ransomware attack against multiple systems in an Azure training environment.
b. Ability to use SIEM, ELK, and EDR to conduct analysis across the Azure training environment.

Submitted by:	Felicia DiPrinzio
Membership Review Period:	NA
Draft of Policy Reviewed by Board:	August 17, 2024
Date of Policy Ratification by Board:	October 7, 2024
Effective Date *(30 days after ratification)*:	October 7, 2024
Final Version Identifier:	1.0