Incident Response

UWF Florida Cybersecurity Training Program
Offered by the University of West Florida Center for Cybersecurity

Course Overview

Course Dates: July 22 – August 2, 2024

Duration: 14 days

Estimated Time Commitment: 10 hours per week

Instructional Hours: 24 contact hours

Delivery Format: Asynchronous online

Target Audience: Courses: IT or Cybersecurity practitioners, managers, executives, and staff

Required Prerequisites / Background: Basic understanding of computers

CEUs: 2.4, **CPEs:** 28

Live Q&A with faculty: Monday, July 29, 2024 @ 5:00 pm CENTRAL (Zoom meeting information will be emailed and included on Canvas course shell).

Course Instructor(s):

Instructor	Email
Mr. Amador Avila, Jr.	aavila@uwf.edu
Dr. Guillermo Francia, III	gfranciaiii@uwf.edu

Course Description

This course serves as an introductory course on cybersecurity incident response. It focuses on the fundamentals of cybersecurity incident response, planning, detection, analysis and management. The course lectures are supplemented with hands-on exercises to reinforce the learning process. The incident handling scenarios are loosely based on those found in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61 r2 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf). Further, it addresses Florida Rule 74-2: Information Technology Security (https://www.flrules.org/gateway/ChapterHome.asp?Chapter=74-2), particularly the following high level functions: Protect, Detect, Respond, and Recover. The course aligns with specific work roles and knowledge, skills and abilities for Cyber Defense Incident Responder (Protect and Defend, PR-CIR-001), Cyber Legal Advisor (Oversee and Govern Legal Advice and Advocacy OV-LGA-001), Privacy Officer/Privacy Compliance

Manager (Oversee and Govern Legal Advice and Advocacy, OV-LGA-002), Cyber Workforce Developer and Manager (Oversee and Govern Strategic Planning and Policy, OV-SPP-001), Target Network Analyst (Analyze Targets, AN-TGT-002), Forensics Analyst (Investigate Digital Forensics, IN-FOR-001), Cyber Operator (Collect and Operate Cyber Operations, CO-OPS-001), Communications Security (COMSEC) Manager (Oversee and Govern Cybersecurity Management OV-MGT-002) work roles as identified in NIST's Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf. The course consists of 8 modules. The modules are mapped to information common to all cybersecurity work roles defined in the Framework. Each module includes a discussion segment, a test for understanding activity, or hands-on exercises as appropriate. Each student is expected to participate actively in the course. The course will culminate with the application of lessons learned on one or two case scenarios.

NIST NICE Cybersecurity Workforce Framework Mapping

The course prepares for the following cybersecurity competency areas and work roles as defined by the NICE Cybersecurity Workforce Framework.

Cybersecurity Competency Areas:

- Communications Security
- Cyber Resiliency
- DevSecOps

Cybersecurity Work Roles and Categories:

- Cyberspace Defense (Protect and Defense, PD-WRL-002)

Course Information

Materials:

No required text

Technical Specifications:

Participants need access to a computer with stable internet connection. They will be required to access the course Leaning Management System (LMS) portal, Canvas. Participants will be logging in to the Florida Cyber Range (FCR) to do all hands-on activities (logins and instructions will be provided before session starts). The course will require internet connection for logging in to FCR.

Each module will have a discussion board that participants will use to post questions and comments related to that module. Instructors will look at the questions and comments and

respond as needed. By enrolling for this course, I agree to abide by the Computing Resources Usage Agreement provided to me.

Grading:

Participants will be assigned a pass/fail grade. Participants must earn a total of 70% or higher on graded assessments to earn a passing grade.

Assessment	**Percentage**
Discussions/Test for Understanding	50%
Projects/Exercises	50%
Total:	**100%**

Course Overview / Schedule

Modules and Lessons	**Assessments**
Module 1: Incident Response Fundamentals Topics: ▪ Basic concepts ▪ Purpose and requirements ▪ IR lifecycle • Evidence handling and administration • NIST SP800-61 rev 2: Computer Security Incident Handling Guide • Controls: physical, technical, management	▪ **Discussion** ▪ **Test for understanding**
Module 2: Preparation Topics: ▪ Design and develop an IR plan ▪ Develop IR plan checklists for specific incidents ▪ Playbooks ▪ Roles and responsibilities	▪ **Discussion** ▪
Module 3: Incident detection & Analysis Topics:	▪ **Discussion** ▪ **Test for understanding**

▪ Fundamentals of incident detection ▪ Incident indicators ▪ Anomaly detection ▪ IOC ▪ Analysis	
Module 4: Incident classification/ Notification and triage Topics: ▪ Determination that an event is an incident ▪ Incident severity ▪ Initial assessment & Triage ▪ IRP execution ▪ Notification requirements	▪ **Discussion** ▪
Module 5: Containment Topics: ▪ Strategies for containment ▪ Mitigating the impact to operations ▪ Determining the COA ▪ Decision making strategies ▪ Timelines for response	▪ **Discussion** ▪ **Test for understanding**
Module 6: Eradication Topics: ▪ Strategies for eradication ▪ Determining threat is fully eradicated ▪ Remediation of vulnerability ▪ Controls to prevent further intrusion	▪ **Discussion** ▪ **Tabletop exercise**
Module 7: Recovery/Restore Topics: ▪ Defining restoring of services ▪ Restore to normal state ▪ Legal/regulatory restore requirements ▪ Updating IRdocumentation	▪ **Discussion** ▪ **Test for understanding**
Module 8: Lessons learned Topics:	▪ **Discussion** ▪ **Test for understanding**

▪ After-Action Report ▪ Lesson learned documentation ▪ Technical controls and recommendations ▪ Tabletop exercises	