CENTER FOR CYBERSECURITY
AT THE UNIVERSITY OF WEST FLORIDA

MITRE ATT&CK™ and D3FEND™

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

Course Overview

Cyber Skills Exercise Date: September 5, 2024

Cyber Skills Exercise Times: 8 am – 4 pm CT with break from 11:30 am – 12:30 pm CT (9 am – 5 pm ET with break from 12:30 – 1:30 pm ET)

Duration: 1 day

Estimated Time Commitment: 7 hours

Instructional Hours: 7 contact hours

Delivery Format: Synchronous online

Target Audience: IT or Cybersecurity practitioners

Required Prerequisites / Background: Working knowledge of IT/Cybersecurity

CEUs: 0.7, **CPEs:** 9

Course Instructor(s):

Instructor	Email
Dr. Guillermo Francia, III	gfranciaiii@uwf.edu

Course Description

The MITRE ATT&CK™ framework allows cybersecurity professionals to quickly map cyberattack tactics, techniques, and procedures (TTP) to identify relevant information, and to build analytics for the intelligent detection across the different stages of the cyber kill chain used by adversaries. This framework helps Security Operations Center (SOC) engineers and analysts to better manage cyber risks and plan what data needs to be available for the Security Incident and Event Management (SIEM) system. The MITRE D3FEND™, a knowledge base of defensive countermeasures and technical components, complements the MITRE ATT&CK™ framework. In this course, we will examine the capabilities and the utilization of both systems.

This course utilizes a combination of lecture, discussion, and hands-on exercises using a virtual Windows machine through a synchronous (live online instruction) modality via Zoom. No prerequisite required other than a working knowledge of computer systems.

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 Competencies:

- Cyber Resiliency
- DevSecOps
- Supply Chain Security

Cybersecurity Work Roles and Categories:

- Cyberspace Defend (PD-WRL-002)
- Threat Analysis (PD-WRL-006)